MATHEMATICS OF COMPUTATION
VOLUME 45, NUMBER 171
JULY 1985, PAGES 223–231

Computation of the Class Number and Class Group of a Complex Cubic Field

By G. Dueck and H. C. Williams*

Abstract. Let h and G be, respectively, the class number and the class group of a complex cubic field of discriminant Δ. A method is described which makes use of recent ideas of Lenstra and Schoof to develop fast algorithms for finding h and G. Under certain Riemann hypotheses it is shown that these algorithms will compute h in $O(|\Delta|^{1/5+\varepsilon})$ elementary operations and G in $O(|\Delta|^{1/4+\varepsilon})$ elementary operations. Finally, the results of running some computer programs to determine h and G for all pure cubic fields $\mathcal{Q}(\sqrt[3]{D})$, with $2 \leqslant D < 30{,}000$, are summarized.

1. Introduction. Let $\mathcal{K}$ be any algebraic number field of discriminant Δ; let G be the class group of $\mathcal{K}$, and $h = |G|$ be the class number of $\mathcal{K}$. Since G is a finite Abelian group, it can be written as the direct product

$$G = C(m_1) \times C(m_2) \times \cdots \times C(m_g),$$

where $C(m_i)$ is a cyclic group of order m_i $(i = 1, 2, 3, \ldots, g)$, $h = m_1 m_2 m_3 \cdots m_g$, and m_i divides m_j whenever $i > j$. If n divides m_r and n does not divide m_{r+1}, we say that $r_n = r$ is the *n-rank* of G. Clearly, G is noncyclic whenever $r_n \geqslant 2$ for some n.

Recently, Lenstra [8] and Schoof [10] have extended the ideas of Shanks [11], [12] to develop fast algorithms for computing h and G when $\mathcal{K}$ is a quadratic field.** Under certain Riemann hypotheses they show that their algorithms will compute h in $O(|\Delta|^{1/5+\varepsilon})$ elementary operations. By an elementary operation we mean a single Boolean operation on either a single binary bit or a pair of binary bits; thus, if some procedure requires the execution of $O(g(x))$ operations, then it will complete its calculations in a length of time which is $O(g(x))$.

Let $\rho(x)$ be any cubic polynomial with integer coefficients, which is irreducible over the rationals $\mathcal{Q}$. Let Δ_ρ, the discriminant of $\rho(x)$, be negative, and denote by δ the real zero of $\rho(x)$. In this paper we will show how the ideas in [8] and [10], together with those developed in Williams, Dueck and Schmid [15] and Williams [16], can be combined to produce fast algorithms for finding h and G when $\mathcal{K} = \mathcal{Q}(\delta)$. Just as in the quadratic case, these new algorithms, under certain Riemann hypotheses, will compute h in $O(|\Delta|^{1/5+\varepsilon})$ elementary operations and G in

Received March 1, 1984.
1980 *Mathematics Subject Classification*. Primary 12A30, 12A50, 12–04.
*Research supported by NSERC of Canada Grant #A7649 and the I. W. Killam Foundation.
**By computing G we mean the determination of g, m_i, and a generator of $C(m_i)$ for $i = 1, 2, 3, \ldots, g$.

0025-5718/85 $1.00 + $.25 per page

$O(|\Delta|^{1/4+\varepsilon})$ elementary operations. We also provide a brief summary of the results of running our computer programs which compute G and h for the pure cubic fields $\mathcal{K} = \mathcal{Q}(\sqrt[3]{D})$.

2. Some Observations Concerning the Ideals of $\mathcal{O}_{\mathcal{K}}$. We will assume from this point forward that $\mathcal{K} = \mathcal{Q}(\delta)$ above, and $\mathcal{O}_{\mathcal{K}}$ is the ring of all the algebraic integers of $\mathcal{K}$. We say that any ideal $\mathfrak{a}$ of $\mathcal{O}_{\mathcal{K}}$ is *primitive* if it has no rational integer divisors. It has been shown by Voronoi [13] that any primitive ideal of $\mathcal{O}_{\mathcal{K}}$ has a unique basis $\{\alpha_1, \alpha_2, \alpha_3\}$, where $\alpha_1 = P$, $\alpha_2, \alpha_3 \in \mathcal{O}_{\mathcal{K}}$, $\alpha_2 = P'(m + \delta)/\tau$, and $\alpha_3 = P''(n + n'\delta + \delta^2)/\tau\sigma^2$. Here $P, P', P'' > 0$; $\tau, \sigma, P, P', P'', m, n, n' \in \mathbf{Z}$; and $0 \leqslant m < \tau P/P'$, $0 \leqslant n' < \tau\sigma P'/P''$, $0 \leqslant n < \tau^2\sigma P/P''$. The values of σ and τ are invariant for any fixed $\mathcal{K}$, and $\tau^6\sigma^2\Delta = \Delta_\rho$. Also, $(P', P'') = 1$, $P'P''|P$, $P''|\tau^2\sigma$, and $N(\mathfrak{a})$, the norm of $\mathfrak{a}$, is $PP'P''$. P is the least positive rational integer in $\mathfrak{a}$, and we frequently denote this value by $L(\mathfrak{a})$. We will call $\{\alpha_1, \alpha_2, \alpha_3\}$ the *canonical basis* of $\mathfrak{a}$. Given any basis of $\mathfrak{a}$, it is a simple matter (see [16]) requiring $O((\sigma\tau^2 L(\mathfrak{a}))^\varepsilon)$ elementary operations to find a canonical basis of $\mathfrak{a}$.

Let the primitive ideals $\mathfrak{a}$ and $\mathfrak{b}$ have canonical bases $\{\alpha_1, \alpha_2, \alpha_3\}$, $\{\beta_1, \beta_2, \beta_3\}$, respectively. The product ideal $\mathfrak{a}\mathfrak{b}$ can be written as $(c)\mathfrak{c}$, where $c \in \mathbf{Z}$ and $\mathfrak{c}$ is a primitive ideal with canonical basis $\{\gamma_1, \gamma_2, \gamma_3\}$. Now c, γ_1, γ_2, γ_3 can be computed by using the method suggested in Section 9 of [16] together with the observation that $c^3 N(\mathfrak{c}) = N(\mathfrak{a}\mathfrak{b})$. This requires that we be able to compute a few gcd's and solve some linear Diophantine equations; hence, it is an easy matter to show that determining these values can be done in $O((\sigma\tau^2 L(\mathfrak{a})L(\mathfrak{b}))^\varepsilon)$ elementary operations.

Since $L(\mathfrak{a}) \in \mathfrak{a}$, we know that there exists an ideal $\mathfrak{a}'$ such that $\mathfrak{a}\mathfrak{a}' = (L(\mathfrak{a}))$. Further, if $\mathfrak{a}$ is primitive, then $L(\mathfrak{a}) = L(\mathfrak{a}')$. The determination of a canonical basis of $\mathfrak{a}'$, given a basis of $\mathfrak{a}$, can be done in $O((\sigma\tau^2 L(\mathfrak{a}))^\varepsilon)$ operations. When $L(\mathfrak{a})$ is a prime or prime power, the basis of $\mathfrak{a}'$ can be found by simply using the formulas in [13].

Let $\alpha \in \mathcal{K}$ and denote by α', α'' the conjugates of α. We have $|\alpha'| = |\alpha''|$. We say that a primitive ideal $\mathfrak{a}$ of $\mathcal{O}_{\mathcal{K}}$ is *reduced* if there does not exist any $\alpha \in \mathfrak{a}$ such that both $|\alpha| < L(\mathfrak{a})$, $|\alpha'| < L(\mathfrak{a})$ hold, unless $\alpha = 0$. If $\mathfrak{a}$ is any ideal of $\mathcal{O}_{\mathcal{K}}$ there always exists a reduced ideal $\mathfrak{b}$ of $\mathcal{O}_{\mathcal{K}}$ such that $\mathfrak{b} \sim \mathfrak{a}$. For a given basis of $\mathfrak{a}$, the algorithm in [14] will find a basis of a reduced $\mathfrak{b}$ such that*** $\mathfrak{b} \sim \mathfrak{a}$ in $O((\sigma\tau^2 L(\mathfrak{a}))^\varepsilon)$ elementary operations. In view of this and our preceding remarks, we are able to deduce that if we have a basis of any ideal $\mathfrak{a}$ of $\mathcal{O}_{\mathcal{K}}$, we can find a basis of a reduced ideal $\mathfrak{b}$ such that $\mathfrak{a}^n \sim \mathfrak{b}$ in $O((n\sigma\tau^2 L(\mathfrak{a}))^\varepsilon)$ operations. We need only use the reduction algorithm of [16] together with a power algorithm, such as those described in Knuth [4, p. 441ff.] (except that we multiply ideals in this case). We also point out here that if $\mathfrak{a}$ is a reduced ideal, then $\tau^3\sigma P^2/P'P'' < \sqrt{|\Delta|/3}$; hence, $\tau^2\sigma L(\mathfrak{a}) < \sqrt{|\Delta|/3}$ (see [16] or [14]).

Given any ideal (from now on this will mean that we are given a basis of the ideal) $\mathfrak{a}$, we can use the algorithm of Voronoi [14] to find all of the reduced ideals which are equivalent to $\mathfrak{a}$. This process is described in [15] and [16]. We need only note here that after finding a reduced ideal $\mathfrak{a}_1$ ($\sim \mathfrak{a}$), we then use the algorithm of

***We say, as usual, that $\mathfrak{a} \sim \mathfrak{b}$ if there exist $\alpha, \beta \in \mathcal{O}_{\mathcal{K}}$ such that $(\alpha)\mathfrak{a} = (\beta)\mathfrak{b}$.

Voronoi to produce a basis for each of the reduced ideals equivalent to $\mathfrak{a}_1$, together with a sequence of elements $\theta_g^{(1)}, \theta_g^{(2)}, \theta_g^{(3)}, \ldots$ of $\mathscr{K}$, each of which exceeds 1. These reduced ideals can be arranged in a sequence

$$\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3, \ldots, \mathfrak{a}_{k-1}, \mathfrak{a}_k, \ldots, \tag{2.1}$$

where

$$\left(L(\mathfrak{a}_{k-1})\theta_g^{(k-1)}\right)\mathfrak{a}_k = \left(L(\mathfrak{a}_k)\right)\mathfrak{a}_{k-1}.$$

Also, to compute a basis of $\mathfrak{a}_k$ from that of $\mathfrak{a}_{k-1}$ requires $O((\sigma\tau^2 L(\mathfrak{a}_{k-1}))^{\varepsilon})$ elementary operations.

If we define

$$\theta_r = \prod_{i=1}^{r-1} \theta_g^{(i)},$$

we get

$$\left(L(\mathfrak{a}_m)\theta_n\right)\mathfrak{a}_n = \left(L(\mathfrak{a}_n)\theta_m\right)\mathfrak{a}_m.$$

We say that $\log(\theta_n/\theta_m)$ is the *distance* $d(\mathfrak{a}_n, \mathfrak{a}_m)$ from $\mathfrak{a}_m$ to $\mathfrak{a}_n$. Also, there exists an absolute and computable constant c_1 such that $n < c_1 d(\mathfrak{a}_n, \mathfrak{a}_1)$ (see [16]). The number of reduced ideals in any given ideal class is finite; at some point in (2.1) we get $\mathfrak{a}_{p+1} = \mathfrak{a}_1$ and $\theta_{p+1} = \varepsilon_0 > 1$, the fundamental unit of $\mathscr{K}$. Thus $d(\mathfrak{a}_{p+1}, \mathfrak{a}_1) = R$, the *regulator* of $\mathscr{K}$. We call the sequence $\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3, \ldots, \mathfrak{a}_p$ the *cycle of reduced ideals which belongs to* $\mathfrak{a}$.

In [16] an algorithm is presented which will determine whether or not two reduced ideals $\mathfrak{b}$ and $\mathfrak{c}$ are equivalent. We give a slightly different form of this algorithm below.

ALGORITHM 2.1.

(1) Find a reduced ideal $\mathfrak{d} \sim \mathfrak{b}\mathfrak{c}'$ and select a value for the *step size* S. Put $i = 1$ and $\mathfrak{d}_1 = \mathfrak{d}$.

(2) Calculate and store the bases of $\mathfrak{a}_1 = (1), \mathfrak{a}_2, \mathfrak{a}_3, \ldots, \mathfrak{a}_s, \mathfrak{a}_{s+1}, \ldots, \mathfrak{a}_t$, where $d(\mathfrak{a}_s, \mathfrak{a}_1) < S$, $d(\mathfrak{a}_{s+1}, \mathfrak{a}_1) > S$, $d(\mathfrak{a}_t, \mathfrak{a}_1) > 3\log|\Delta/3| + S$. Sort the above ideals on their values of $L(\mathfrak{a}_j)$.

(3) If $\mathfrak{d}_i = \mathfrak{a}_j (1 \leqslant j \leqslant t)$, then we are done, and $\mathfrak{b} \sim \mathfrak{c}$. (This part of the algorithm is most expeditiously achieved by first searching in the sorted list of $L(\mathfrak{a}_j)$'s above for those which have $L(\mathfrak{d}_i) = L(\mathfrak{a}_j)$). This can also be done by using hash coding techniques (cf. [10]). Otherwise, put $\mathfrak{d}_{i+1} =$ a reduced ideal equivalent to $\mathfrak{d}_i\mathfrak{a}_s'$.

(4) Replace the value of i by that of $i + 1$ and check that

$$i < R/(S - (1/2)\log|\Delta/3|).$$

If this is so, return to step (3); if not, we know that $\mathfrak{b}$ and $\mathfrak{c}$ are not equivalent.

The number of elementary operations needed to execute step (2) of Algorithm 2.1 is $O(S|\Delta|^{\varepsilon})$; the number needed to execute steps (3) and (4) is $O(R|\Delta|^{\varepsilon}/S)$. A modified version of this algorithm can be used to compute R in $O(|\Delta|^{1/4+\varepsilon})$ elementary operations. If we assume the Generalized Riemann Hypothesis (GRH) for $\zeta_{\mathscr{L}}(s)$, where $\mathscr{L}$ is the normal closure of $\mathscr{K}$, then R can be computed in $O(|\Delta|^{1/5+\varepsilon})$ elementary operations. The method for doing this when $\mathscr{K}$ is a pure cubic field is fully described in [15]. It is not difficult to apply these same ideas to any complex cubic field.

3. Calculation of h. If $\zeta_{\mathscr{K}}(s)$ is the zeta function for $\mathscr{K}$, then

$$2\pi hR = \sqrt{|\Delta|}\,\Phi(1),$$

where $\Phi(s) = \zeta_{\mathscr{K}}(s)/\zeta(s)$. We can write $\Phi(1)$ in terms of the Euler product

$$\Phi(1) = \prod_q f(q),$$

where the product is taken over all the rational primes, and $f(q)$ is determined by how the ideal (q) splits into prime ideal factors. If we let $\mathfrak{p}$, $\mathfrak{q}$, $\mathfrak{r}$ denote prime ideals, we have

(i)	$f(q) = 1$	when $(q) = \mathfrak{q}^3$;
(ii)	$f(q) = q/(q-1)$	when $(q) = \mathfrak{p}\mathfrak{q}^2$;
(iii)	$f(q) = q^2/(q^2-1)$	when $(q) = \mathfrak{p}\mathfrak{q}$;
(iv)	$f(q) = q^2/(q-1)^2$	when $(q) = \mathfrak{p}\mathfrak{q}\mathfrak{r}$;
(v)	$f(q) = q^2/(q^2+q+1)$	when $(q) = \mathfrak{q}$.

Criteria for determining how (q) splits can be found in [13] or Delone and Faddeev [1]. It is sufficient here to note that we require q^{ϵ} elementary operations to determine the value of $f(q)$.

If we define

$$F(Q) = \prod_q^Q f(q),$$

where the product is taken over all primes up to Q, we require $O(Q^{1+\epsilon})$ elementary operations to evaluate $F(Q)$. Also,

$$F(Q) \leqslant \prod_q^Q \frac{q^2}{(q-1)^2} \sim (e^{\gamma}\log Q)^2 \tag{3.1}$$

by Mertens' Theorem. If

$$T(Q) = \prod_{q>Q} f(q),$$

where the product is taken over all primes which exceed Q, it can be shown from a result of Lagarias and Odlyzko [5] that if the GRH holds for $\zeta_{\mathscr{L}}$, then

$$|1 - T(Q)| < c_2(\log|\Delta|Q)/\sqrt{Q}\,, \tag{3.2}$$

where c_2 is an absolute, effectively computable constant. In fact, a value for this constant c_2 can be computed by using the conditional results of Oesterlé [9] and a method similar to that used in Section 10 of [15]. It is this result (3.2) that permits us to develop our $O(|\Delta|^{1/5+\epsilon})$ algorithm for determining R.

If we put $\tilde{h} = \mathrm{Ne}(\sqrt{|\Delta|}\,F(Q)/2\pi R)$, where $\mathrm{Ne}(x)$ is the nearest integer to x, we have

$$|\tilde{h} - h| < Y = |\eta| + \left(c_2\sqrt{|\Delta|}\,F(Q)\log(|\Delta|Q)/2\pi R\sqrt{Q}\right), \tag{3.3}$$

where $\eta = (\sqrt{|\Delta|}\,F(Q)/2\pi R) - \tilde{h}$.

If $Y < 1$, then $h = \tilde{h}$. If $c_2Q^{-1/2}(\log|\Delta|Q) < 1/6$, then $Y < h/5 + 1/2$; thus, $Y < h/2$ when $Y > 1$. If $Y > 1$, we attempt to find an integer h^* such that $h^*|h$ and

$Y < h^*/2$; in this case we get $h = h^*[\tilde{h}/h^* + 1/2]$. Thus, if Q is a constant multiple of $|\Delta|^{1/5}$, we see from (3.1) and (3.3) that

$$RY = O(|\Delta|^{2/5+\varepsilon}), \tag{3.4}$$

and, as a consequence, we may assume that

$$h^*R = O(|\Delta|^{2/5+\varepsilon}). \tag{3.5}$$

In order to determine h, we require an algorithm to find the order or period e of a given prime ideal $\mathfrak{p}$ of degree 1. We first point out that if we are given the value of the rational prime $p = N(\mathfrak{p})$, it is a simple matter, using the formulas of [1] or [13], to find a basis of $\mathfrak{p}$. This involves solving a cubic congruence modulo p; however, for small values of p this congruence can be solved easily by trial, and for larger values, algorithms similar to those given in Williams and Zarnke [17] can be used.

Let $\mathfrak{a}$ be a reduced ideal equivalent to $\mathfrak{p}^{\tilde{h}}$. In view of (3.3) we know that there must exist some m such that $|m| < Y$ and

$$\mathfrak{p}^{\tilde{h}} \sim \mathfrak{a} \sim \mathfrak{p}^m. \tag{3.6}$$

If $|m| = ki + j\ (0 \leqslant j < k)$, we see that (3.6) is equivalent to

$$\begin{aligned} \mathfrak{a}(\mathfrak{p}'^k)^i &\sim \mathfrak{p}^j \qquad (m \geqslant 0), \\ \mathfrak{a}'(\mathfrak{p}'^k)^i &\sim \mathfrak{p}^j \qquad (m < 0). \end{aligned} \tag{3.7}$$

We now search for values of i, j, and k for which (3.7) holds. We now make use of what is essentially the baby-step–giant-step strategy of Shanks [11].

ALGORITHM 3.1. We consider two possible cases.

Case 1 ($Y > R$).

(1) Put $k = [\sqrt{Y/R}\,]$ and compute the cycles of reduced ideals which belong to each of (1), $\mathfrak{p}$, $\mathfrak{p}^2$, $\mathfrak{p}^3, \ldots, \mathfrak{p}^{k-1}$. By the remarks in Section 2 we see that the total number of ideals produced here is $O(kR)$. We then take these ideals and sort them (on their L values) into a list $\mathcal{L}$. Altogether, this step executes in $O(\sqrt{RY}|\Delta|^{\varepsilon})$ elementary operations.

(2) Put $\mathfrak{b}_0 = \mathfrak{a}$, $\mathfrak{c}_0 = \mathfrak{a}'$, and compute reduced ideals $\mathfrak{b}_i$ and $\mathfrak{c}_i$ by using $\mathfrak{b}_{r+1} \sim \mathfrak{b}_r(\mathfrak{p}')^k$, $\mathfrak{c}_{r+1} \sim \mathfrak{c}_r(\mathfrak{p}')^k$. If any $\mathfrak{b}_r$ or $\mathfrak{c}_r \in \mathcal{L}$, from (3.7) we get $m = rk + j$ when $\mathfrak{b}_r \sim \mathfrak{p}^j$ ($\mathfrak{b}_r$ is in the cycle belonging to $\mathfrak{p}^j$) or $m = -rk - j$ when $\mathfrak{c}_r \sim \mathfrak{p}^j$. Since $|m| < Y$ and $j < k$, we see that we must find such a value for r, where $r < Y/k = O(|\Delta|^{1/5+\varepsilon})$.

Case 2 ($Y < R$). In this case we put $k = 1$ and $j = 0$ in (3.7), and we compute $\mathfrak{b}_r$ and $\mathfrak{c}_r$ as above. Put $S = \sqrt{RY}$. We now use Algorithm 2.1 with step size S to determine, as r increases, whether $\mathfrak{b}_r$ or $\mathfrak{c}_r$ is principal. In the former case, $m = r$, and in the latter, $m = -r$. Since S is fixed here, step (2) of Algorithm 2.1 need only be executed once. Since a value for r must exist such that $r < Y$, we find that we require a total of $O(S|\Delta|^{\varepsilon}) + O(YR|\Delta|^{\varepsilon}/S) = O(|\Delta|^{1/5+\varepsilon})$ elementary operations to find m in this case.

Having found m, we next factor $|\tilde{h} - m|$, a task that can certainly be done in $O(|\Delta|^{1/6+\varepsilon})$ operations (see, for example, Lehman [7]), and then find the period e of $\mathfrak{p}$ by trying the factors of $|\tilde{h} - m|$. Since $e|h$, we can use $h^* = e$ if $e > 2Y$. If this is not the case, we put $e_1 = e$, $\mathfrak{p}_1 = \mathfrak{p}$ and select another prime ideal of degree 1, $\mathfrak{p}_2$,

and find the order e_2 of the subgroup of G which contains the ideal classes $\mathfrak{p}_1 I$, $\mathfrak{p}_2 I$, where I is the *principal class*. Continue this process until we find some $e_n > 2Y$. When this occurs, put $h^* = e_n$ and find h. In the next section we show that this process will require, under certain Riemann hypotheses, only $O(|\Delta|^{1/5+\varepsilon})$ elementary operations.

4. Calculation of G. Let $\mathfrak{h}_1, \mathfrak{h}_2, \ldots, \mathfrak{h}_k$ be k reduced ideals of $\mathcal{O}_{\mathcal{K}}$, each with period a prime p, and let C_i denote the cyclic subgroup of G generated by $\mathfrak{h}_i I$. Put $E = C_1 \times C_2 \times C_3 \times \cdots \times C_k$. We will now present an algorithm which will determine whether or not any given reduced ideal $\mathfrak{j}$ is equivalent to some ideal in E. In the former case the algorithm will also determine $t_1, t_2, t_3, \ldots, t_k$ such that

$$\mathfrak{j} \sim \mathfrak{h}_1^{t_1} \mathfrak{h}_2^{t_2} \cdots \mathfrak{h}_k^{t_k}. \tag{4.1}$$

ALGORITHM 4.1. Compute $s \in \mathbf{Z}$ such that

$$p^s \leqslant \sqrt{p^{k+1}/R}, \qquad p^{s+1} > \sqrt{p^{k+1}/R}.$$

Case 1 ($s > 0$).

(1) Compute a sorted list $\mathcal{J}$ of all reduced ideals $\mathfrak{b} \sim \mathfrak{h}_1^{u_1} \mathfrak{h}_2^{u_2} \cdots \mathfrak{h}_s^{u_s}$ for $0 \leqslant u_i < p$. Since there are p^s possible ideals of the form $\prod_{i=1}^{s} \mathfrak{h}_i^{u_i}$, and each belongs to a cycle of reduced ideals containing $O(R)$ such ideals, we require $O(p^s R|\Delta|^{\varepsilon})$ elementary operations to perform this step.

(2) Compute p^{k-s} reduced ideals $\mathfrak{c}$ such that

$$\mathfrak{c} \sim \mathfrak{j} \prod_{i=s+1}^{k} \mathfrak{h}_i^{v_i} \qquad (0 \leqslant v_i < p).$$

Check whether or not any of these is in $\mathcal{J}$. If none is, then $\mathfrak{j} I \notin E$. If we find that

$$\mathfrak{j} \prod_{i=s+1}^{k} \mathfrak{h}_i^{v_i} \sim \prod_{i=1}^{s} \mathfrak{h}_i^{u_i},$$

then $t_i = u_i$ for $i \leqslant s$ and $t_i = p - v_i$ for $i \geqslant s+1$. The total number of elementary operations needed to perform steps (1) and (2) is

$$O(p^s R|\Delta|^{\varepsilon}) + O(p^{k-s}|\Delta|^{\varepsilon}) = O\big((p^{k+1}R)^{1/2}|\Delta|^{\varepsilon}\big).$$

Case 2 ($s = 0$).

(1) Find a reduced ideal equivalent to each ideal of the form

$$\mathfrak{j} \prod_{i=1}^{k} \mathfrak{h}^{u_i} \qquad (0 \leqslant u_i < p). \tag{4.2}$$

(2) Use Algorithm 2.1 with step size $S = \sqrt{p^{k+1}R}$ to determine whether any of the ideals produced in step (1) is principal. If the ideal given by (4.2) is principal, then the values of t_i in (4.1) are given by $t_i = p - u_i$. If none of these ideals is principal, then $\mathfrak{j} I \notin E$. In step (1) of this case we produce $p^k < \sqrt{Rp^{k+1}}$ ideals, and Algorithm 2.1 must be used on each of them. Since S is fixed, step (2) of Algorithm 2.1 need only be executed once; hence, the total number of elementary operations required for the execution of this case of the algorithm is

$$O(S|\Delta|^{\varepsilon}) + O(p^k R|\Delta|^{\varepsilon}/S) = O\big((p^{k+1}R)^{1/2}|\Delta|^{\varepsilon}\big).$$

We now use this algorithm in order to compute the smallest subgroup H of G which contains $\mathfrak{g}_1 I$, $\mathfrak{g}_2 I, \ldots, \mathfrak{g}_k I$, where the $\mathfrak{g}_i$ are given reduced ideals of $\mathcal{O}_{\mathcal{K}}$ with periods $e_1, e_2, \ldots, e_k$. If $e_i = p^{\kappa_i} f_i$, where p is a prime and $(p, f_i) = 1$, then $\mathfrak{g}_i^{f_i}$ has period p^{κ_i}, and some of the ideal classes $\mathfrak{g}_i^{f_i} I$ $(i = 1, 2, 3, \ldots, k)$ generate S_p, the Sylow p-subgroup of H. Since the problem of finding H is easy once all the distinct Sylow p-subgroups of H have been computed, we will assume that the periods e_i $(i = 1, 2, 3, \ldots, k)$ are all positive powers of a fixed prime p.

We first find a reduced ideal $\mathfrak{k}_i \sim \mathfrak{g}_i^{w_i}$, where $w_i = p_i^{\kappa_i - 1}$, for $i = 1, 2, 3, \ldots, k$. We then find those $\mathfrak{k}_i$'s whose corresponding ideal classes are generators of E, subject to the constraint that the sum of their corresponding κ_i's is maximal. This can be done as follows. We suppose that we have found from among the s ideals $\mathfrak{k}_1, \mathfrak{k}_2, \mathfrak{k}_3, \ldots, \mathfrak{k}_s$, v ideals $\mathfrak{h}_1, \mathfrak{h}_2, \mathfrak{h}_3, \ldots, \mathfrak{h}_v$ such that $\mathfrak{h}_i I$ $(i = 1, 2, 3, \ldots, v)$ generates C_i and $E_v = C_1 \times C_2 \times C_3 \times \cdots \times C_v$. For example, when $s = 1$, we have $v = 1$ and $\mathfrak{h}_1 = \mathfrak{k}_1$. We then use Algorithm 4.1 to determine whether or not $\mathfrak{k}_{s+1} I \in E_v$. If $\mathfrak{k}_{s+1} I \notin E_v$, then put $\mathfrak{h}_{r+1} = \mathfrak{k}_{s+1}$ and increase v by 1. If $\mathfrak{k}_{s+1} I \in E_v$, then

$$\mathfrak{k}_{s+1} \sim \mathfrak{h}_1^{t_1} \mathfrak{h}_2^{t_2} \cdots \mathfrak{h}_v^{t_v}.$$

If p^{n_i} is the period of $\mathfrak{h}_i$ and

$$n_m = \min\{n_j | t_j \neq 0; j = 1, 2, 3, \ldots, v\},$$

we replace $\mathfrak{h}_m$ by $\mathfrak{k}_{s+1}$ and increase s by 1 whenever $n_m < \kappa_{s+1}$. If $n_m \geqslant \kappa_{s+1}$, we simply increase s by 1. We repeat this process until we get a value for s which exceeds k. At this point we have found $E_r = E$ and

$$S_p = C(p^{n_1}) \times C(p^{n_2}) \times \cdots \times C(p^{n_r}).$$

Note that this entire process requires $O(k(p^{r+1}R)^{1/2}|\Delta|^{\varepsilon})$ elementary operations. If we know r in advance, then we need only find that ideal $\mathfrak{k}$, among those not previously used to determine E_{r-1}, with the largest period. We then put $\mathfrak{h}_r = \mathfrak{k}$ and p^{n_r} equal to the period of $\mathfrak{k}$. This process requires only $O(k(p^r R)^{1/2}|\Delta|^{\varepsilon})$ elementary operations. It follows that if we know an upper bound b on r $(r \leqslant b)$, then the number of elementary operations needed to compute H is $O(k(p^b R)^{1/2}|\Delta|^{\varepsilon})$.

If we make use of Corollary 1.3 of Theorem 1.2 of Lagarias, Montgomery and Odlyzko [6], we see that if extra Riemann hypotheses involving the location of the zeros of certain Hecke L-functions are assumed, then there exists an effectively computable constant c_3 such that if $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3, \ldots, \mathfrak{p}_k$ are all the prime ideals of degree 1 with norm less than $c_3(\log|\Delta|)^2$, then the smallest subgroup H of G, which contains $\mathfrak{p}_i I$ $(i = 1, 2, 3, \ldots, k)$ is G itself (see the proof of Corollary 6.2 of [10]). It follows that, under these hypotheses, we can compute a subgroup of G of order h^* in $O(\sqrt{h^* R}\,|\Delta|^{\varepsilon}) = O(|\Delta|^{1/5+\varepsilon})$ (by (3.5)) elementary operations. Also, once h is known, we can easily find the periods of any of the $\mathfrak{p}_i$ and calculate the class group in $O(\sqrt{hR}\,|\Delta|^{\varepsilon}) = O(|\Delta|^{1/4+\varepsilon})$ elementary operations.

5. Computational Results. Programs were written to find R, h, and G for the pure cubic fields $\mathcal{Q}(\sqrt[3]{D})$, where $D = ab^2$, a, b are square-free, and $a > b > 0$. These programs were written in FORTRAN with some assembler language subprograms. For the values of D which we considered, we needed no more than double-precision arithmetic. For any D, our programs, which ran on an AMDAHL 470-V8 computer,

produced the values of R and h and the invariants of G in a matter of seconds. We selected the pure cubic fields in order to make the programming easier and in the hope that we would find some interesting (noncyclic) class groups. It should be noted at this point that Eisenbeis, Frey and Ommerborn [2] had previously computed r_2 for all pure cubic fields with radicand $D < 10{,}000$.

Ennola and Turunen [3] found that there were only 35 noncyclic class groups among those for the 26,440 nonconjugate totally real cubic number fields with discriminant $< 500{,}000$. We found that 11,637 fields out of the 24,537 distinct pure cubic fields with radicand $D < 30{,}000$ have a noncyclic G. Of course, most of these have $C(3) \times C(3)$ as a subgroup of G. We summarize our results in Table 1, where we give, for each n, the frequency of occurrence of all G with $r_n \geqslant 2$.

The only case in our table where $C(p) \times C(p)$ ($p > 3$ and p prime) is a subgroup of G occurs for $D = 10{,}263$, where $G = C(90) \times C(5)$. The largest value of h in our table is 2412, which occurs when $D = 28{,}365$; here $G = C(804) \times C(3)$. The complete table, giving for each D with noncyclic G the value of R and the class group invariants $m_1, m_2, m_3, \ldots$, has been deposited in the UMT file.

TABLE 1

n \ r_n	2	3	4
2	1834	93	–
3	8614	1850	74
4	24	–	–
5	1	–	–
6	826	3	–
9	27	–	–
12	7	–	–
18	2	–	–

Department of Computer Science
University of Manitoba
Winnipeg, Manitoba, Canada R3T 2N2

1. B. N. DELONE & D. K. FADDEEV, *The Theory of Irrationalities of the Third Degree*, Transl. Math. Monographs, Vol. 10, Amer. Math. Soc., Providence, R. I., 1964.

2. H. EISENBEIS, G. FREY & B. OMMERBORN, "Computation of the 2-rank of pure cubic fields," *Math. Comp.*, v. 32, 1978, pp. 559–569.

3. V. ENNOLA & R. TURUNEN, "On totally real cubic fields," *Math. Comp.*, v. 44, 1985, pp. 495–518.

4. D. E. KNUTH, *The Art of Computer Programming*. Vol. II: *Seminumerical Algorithms*, 2nd ed., Addison-Wesley, Reading, Mass., 1981.

5. J. C. LAGARIAS & A. M. ODLYZKO, "Effective versions of the Chebotarev density theorem," *Algebraic Number Fields* (A. Fröhlich, ed.), Academic Press, London, 1977, pp. 409–464.

6. J. C. LAGARIAS, H. L. MONTGOMERY & A. M. ODLYZKO, "A bound for the least prime ideal in the Chebotarev density theorem," *Invent. Math.*, v. 54, 1979, pp. 271–296.

7. R. S. LEHMAN, "Factoring large integers," *Math. Comp.*, v. 28, 1974, pp. 637–646.

8. H. W. LENSTRA, JR., *On the Calculation of Regulators and Class Numbers of Quadratic Fields*, London Math. Soc. Lecture Note Ser., Vol. 56, 1982, pp. 123–150.

9. J. OESTERLÉ, "Versions effectives du théorème de Chebotarev sous l'hypothèse de Riemann généralisée," *Astérisque*, v. 61, 1979, pp. 165–167.

10. R. SCHOOF, "Quadratic fields and factorization," *Computational Methods in Number Theory*. Part II, Math. Centrum Tracts, No. 155, Amsterdam, 1983, pp. 235–286.

11. D. SHANKS, *Class Number, A Theory of Factorization and Genera*, Proc. Sympos. Pure Math., Vol. 20, Amer. Math. Soc., Providence, R. I., 1971, pp. 415–440.

12. D. SHANKS, *The Infrastructure of a Real Quadratic Field and Its Applications*, Proc. 1972 Number Theory Conf. (Boulder, 1972), pp. 217–224.

13. G. F. VORONOI, *Concerning Algebraic Integers Derivable from a Root of an Equation of the Third Degree*, Master's Thesis, St. Petersburg, 1894. (Russian)

14. G. F. VORONOI, *On a Generalization of the Algorithm of Continued Fractions*, Doctoral Dissertation, Warsaw, 1896. (Russian)

15. H. C. WILLIAMS, G. W. DUECK & B. K. SCHMID, "A rapid method of evaluating the regulator and class number of a pure cubic field," *Math. Comp.*, v. 41, 1983, pp. 235–286.

16. H. C. WILLIAMS, "Continued fractions and number-theoretic computations," Proc. Number Theory Conf. (Edmonton, 1983); *Rocky Mountain J. Math.* (To appear.)

17. H. C. WILLIAMS & C. R. ZARNKE, "Some algorithms for solving a cubic congruence modulo p," *Utilitas Math.*, v. 6, 1974, pp. 285–306.