MATHEMATICS OF COMPUTATION, VOLUME 35, NUMBER 152
OCTOBER 1980, PAGES 1423–1434

Improving the Speed of Calculating the Regulator of Certain Pure Cubic Fields

By H. C. Williams

Abstract. To calculate R, the regulator of a pure cubic field $Q(\sqrt[3]{D})$, a complete period of Voronoi's continued fraction algorithm over $Q(\sqrt[3]{D})$ is usually generated. In this paper it is shown how, in certain pure cubic fields, R can be determined by generating only about one third of this period. These results were used on a computer to find R and then the class number for all pure cubic fields $Q(\sqrt[3]{p})$, where p is a prime, $p \equiv -1 \pmod 3$, and $p < 2 \times 10^5$. Graphs illustrating the distribution of such cubic fields with class number one are presented.

1. Introduction. In several previous papers [3], [10], [12], [13] the problem of the distribution of pure cubic fields with class number one has been studied. The main difficulty in obtaining numerical results has always been (and still is) the amount of time needed to calculate the regulator of such a field. The regulator of $Q(\sqrt[3]{D})$ is usually much larger than that of $Q(\sqrt{D})$. For example, the largest regulator of $Q(\sqrt{D})$, for all $D < 2 \times 10^5$, occurs for $D = 196771$ [11] and is 1291.32, while, for $D = 199109$, the regulator of $Q(\sqrt[3]{D})$ is 455713.75.

The only primes p such that $Q(\sqrt[3]{p})$ can have class number one are those which have the form $3t - 1$ [5]. In [12] the case of $p \equiv 8 \pmod 9$ was investigated for all $p < 2 \times 10^5$. The problem of dealing with $Q(\sqrt[3]{p})$ for the primes $p \equiv 2, 5 \pmod 9$ is more difficult as their regulators tend to be about three times larger than those for $Q(\sqrt[3]{p})$ when $p \equiv 8 \pmod 9$ because their discriminants are nine times larger. In order to deal with this problem it was necessary to find a method which increased the speed of regulator calculation for these fields.

In quadratic fields continued fractions are used to determine the regulators; see [9], [11]. Also, instead of going through the entire period of the continued fraction for $\sqrt{D}$, it is sufficient to go no more than about one-half the period in order to calculate the regulator. In this paper we show that for certain pure cubic fields it is only necessary to go about one third of the way through the period of Voronoi's continued fraction algorithm for $\sqrt[3]{D}$ to find the regulator of $Q(\sqrt[3]{D})$. We also present some computational results concerning pure cubic fields with class number one.

2. Simple Results Concerning Pure Cubic Fields. We first summarize some well-known results on pure cubic fields. Let Z be the set of rational integers and put $D = ab^2$, where $a, b \in Z$, $(a, b) = 1$ and a, b are square-free. Let $Q(\delta)$ be the pure cubic

Received October 31, 1979; revised March 3, 1980.
1980 *Mathematics Subject Classification.* Primary 12A30, 12A45, 12A50, 12–04.

field formed by adjoining $\delta = \sqrt[3]{D}$ to the rationals Q. If $\bar{D} = a^2b$ and $\bar{\delta} = \sqrt[3]{\bar{D}}$, then $Q(\delta) = Q(\bar{\delta})$; hence, we may assume that $a > b$.

If $D \not\equiv \pm 1 \pmod 9$, then $[1, \delta, \bar{\delta}]$ is a basis of the *ring of integers* $Q[\delta]$ of $Q(\delta)$, and the *discriminant* Δ of $Q(\delta)$ is $-27a^2b^2$. If $D \equiv \pm 1 \pmod 9$, then $[1, \delta, \beta]$, where $\beta = (1 + a\delta + b\bar{\delta})/3$, is a basis of $Q[\delta]$ and $\Delta = -3a^2b^2$. Thus, if $x_1, x_2, x_3 \in Z$ and $(x_1 + x_2\delta + x_3\bar{\delta})/\sigma \in Q[\delta]$, then $\sigma = 1$ when $D \not\equiv \pm 1 \pmod 9$ (Dedekind type 1 field) and $\sigma = 3$, $x_1 \equiv ax_2 \equiv bx_3 \pmod 3$ when $D \equiv \pm 1 \pmod 9$ (Dedekind type 2 field).

If $\alpha \in Q(\delta)$, then $\alpha = (x_1 + x_2\delta + x_3\bar{\delta})/x_4$, where $x_1, x_2, x_3, x_4 \in Z$. Define the *conjugates* of α as

$$\alpha' = (x_1 + x_2\omega\delta + x_3\omega^2\bar{\delta})/x_4, \qquad \alpha'' = (x_1 + x_2\omega^2\delta + x_3\omega\bar{\delta})/x_4,$$

where ω is a fixed primitive cube root of unity. We define the *norm* of α to be $N(\alpha) = \alpha\,\alpha'\alpha''$. When $\alpha \in Q[\delta]$, $N(\alpha) \in Z$. If $\epsilon \in Q[\delta]$ and $N(\epsilon) = \pm 1$, then ϵ is a *unit* of $Q(\delta)$ and $\epsilon = \pm\epsilon_0^n$, for some $n \in Z$, where ϵ_0 is the *fundamental unit* of $Q(\delta)$. We assume $\epsilon_0 > 1$ and define the *regulator* R of $Q(\delta)$ to be $R = \log \epsilon_0$.

If $3\,|\,D$, put $S = |\Delta|/27$; otherwise, put $S = |\Delta|/3$; thus, if $D \not\equiv 1 \pmod 9$, then $9\,|\,S$. We note that if s is any rational prime divisor of S, then the ideal $[s] = \mathfrak{s}^3$, where $\mathfrak{s}$ is a prime ideal, and the norm of $\mathfrak{s}$, $N(\mathfrak{s})$, is s. From this observation we deduce

LEMMA 1. *If $\alpha \in Q[\delta]$ and $N(\alpha)\,|\,S$, then $\alpha^3/N(\alpha) \in Q[\delta]$.*

Proof. Follows easily by noting that, since $N(\alpha)\,|\,S$, we must have $[\alpha^3] = [N(\alpha)]$.

LEMMA 2. *Let $x_1, x_2, x_3 \in Z$ and $\alpha = (x_1 + x_2\delta + x_3\bar{\delta})/\sigma \in Q[\delta]$. If $t\,|\,S$ and $t^3\,|\,N(\alpha)$, then $t\,|\,(x_1, x_2, x_3)$.*

Proof. If s is a prime divisor of S and* $s^n \,|\,|\, t$, then $s^{3n}\,|\,N(\alpha)$ and $\alpha \equiv 0 \pmod{\mathfrak{s}^{3n}}$. Thus, $\alpha \equiv 0 \pmod{[t]}$ and the result follows.

LEMMA 3. *Let $d = d_1d_2$, where $d_1, d_2 \in Z$, $d_1\,|\,a$, and $d_2\,|\,b$. If $d^2\,|\,N(\alpha)$ when $\alpha = (x_1 + x_2\delta + x_3\bar{\delta})/\sigma \in Q[\delta]$, then $d\,|\,x_1$, $d_1\,|\,x_2$, $d_2\,|\,x_3$.*

Proof. Follows easily on noting that $d\,|\,ab$, d is square-free, and $\sigma^3N(\alpha) = x_1^3 + ab^2x_2^3 + a^2bx_3^3 - 3abx_1x_2x_3$.

Our final result of this section is

LEMMA 4. *Let $\alpha = (x_1 + x_2\delta + x_3\bar{\delta})/\sigma \in Q[\delta]$, where $x_1, x_2, x_3 \in Z$ and $(x_1, x_2, x_3)\,|\,\sigma$. If $27 \nmid N(\alpha)$, $r \in Z$, $|r| < N(\alpha)$, and $r\alpha = N(\alpha)\gamma$, where $\gamma \in Q[\delta]$, then $r = 0$.*

Proof. Let $\gamma = (g_1 + g_2\delta + g_3\bar{\delta})/\sigma$. We must have $rx_i = N(\alpha)g_i$ $(i = 1, 2, 3)$ and, since $(x_1, x_2, x_3)\,|\,\sigma$, we get $N(\alpha)\,|\,\sigma r$. If $\sigma = 1$, we have $N(\alpha)\,|\,r$; hence, $r = 0$.

*We denote by $p^\alpha \,|\,|\, a$ the fact that $p^\alpha\,|\,a$ and $p^{\alpha+1} \nmid a$.

If $\sigma = 3$ and $N(\alpha)\nmid r$, then $3\,|\,N(\alpha)$ and $r = kN(\alpha)/3$ with $k \in Z$ and $(k, 3) = 1$. Since $r^3 = N(\alpha)^2 N(\gamma)$, it follows that $27\,|\,N(\alpha)$, which is not possible.

3. Relative Minima. Let $\alpha \in Q(\delta)$ and consider the ordered triple

$$A = \left(\alpha, \frac{\alpha' - \alpha''}{2i}, \frac{\alpha' + \alpha''}{2}\right),$$

where $i^2 = -1$. Since A is uniquely determined once α is known, we often identify A with α and write $A \approx \alpha$ or $\alpha \approx A$, where the lower case letter refers to the element of $Q(\delta)$ and the upper case letter to the corresponding ordered triple. Let $\mu, \nu \in Q(\delta)$ and let

$$\mathcal{R} = \{A\,|\,A \approx x + y\mu + z\nu,\ x, y, z \in Z\}.$$

$\mathcal{R}$ is a *lattice* with *basis* $[1, \mu, \nu]$.

We say that $\Theta \approx \theta \in Q(\delta)$ is a *relative minimum* of $\mathcal{R}$ if $\Theta \in \mathcal{R}$ and there does not exist $\Phi \in \mathcal{R}$ such that $\phi \neq 0$, $|\phi| < |\theta|$ and $\phi'\phi'' < \theta'\theta''$. If Θ and Φ are relative minima of $\mathcal{R}$ with $\theta > \phi$, we say they are *adjacent* relative minima of $\mathcal{R}$ when there does not exist $\Psi \in \mathcal{R}$ such that $\psi \neq 0$, $|\psi| < |\theta|$ and $\psi'\psi'' < \phi'\phi''$. If $\theta_i \approx \Theta_i \in \mathcal{R}$ $(i = 1, 2, 3, \ldots, n, \ldots)$, $\theta_{i+1} > \theta_i$, and Θ_i, Θ_{i+1} are adjacent relative minima, we call the sequence

$$\Theta_1, \Theta_2, \Theta_3, \ldots, \Theta_n, \ldots,$$

a *chain* of relative minima. If Θ_i precedes Θ_j in such a chain we say that Θ_i is less than Θ_j. If Φ is any relative minimum of $\mathcal{R}$ and $\phi > \theta_1$, then $\Phi = \Theta_k$ for some k. For a more detailed description of these ideas see [4], [7], [13].

In [8] Voronoi presented a method of finding a chain of relative minima when $\Theta_1 = (1, 0, 1)$ is a relative minimum of $\mathcal{R}$. This technique is simply a means of finding in any such lattice a relative minimum Θ_g adjacent to $(1, 0, 1)$. Here we shall concern ourselves with finding $\Theta_g \approx \theta_g$ such that $\theta_g > 1$. Let $\mathcal{R}_1 = \mathcal{R}$ and let $\Theta_g^{(1)} \approx \theta_g^{(1)}$ be the relative minimum adjacent to $(1, 0, 1)$ in $\mathcal{R}_1$ with $\theta_g^{(1)} > 1$. Embed $1, \theta_g^{(1)}$ in a basis of $\mathcal{R}_1$ and let this basis be $[1, \theta_g^{(1)}, \theta_h^{(1)}]$. Let $\mathcal{R}_2$ have basis $[1, 1/\theta_g^{(1)}, \theta_h^{(1)}/\theta_g^{(1)}]$. We see that $(1, 0, 1)$ is a relative minimum of $\mathcal{R}_2$ and find the relative minimum $\Theta_g^{(2)} \approx \theta_g^{(2)} > 1$ adjacent to $(1, 0, 1)$ in $\mathcal{R}_2$. We continue this process by defining $\mathcal{R}_{i+1}$ to be the lattice with basis $[1, 1/\theta_g^{(i)}, \theta_h^{(i)}/\theta_g^{(i)}]$, where $\Theta_g^{(i)} \approx \theta_g^{(i)} > 1$ is the relative minimum adjacent to $(1, 0, 1)$ in $\mathcal{R}_i$ and $[1, \theta_g^{(i)}, \theta_h^{(i)}]$ is a basis of $\mathcal{R}_i$. It follows that $\Theta_n \approx \theta_n$, where

$$\theta_n = \prod_{i=1}^{n-1} \theta_g^{(i)}.$$

If $[1, \mu, \nu]$ is an integral basis of $Q[\delta]$, then we see that $(1, 0, 1)$ is a relative minimum of $\mathcal{R}$ and so is $E \approx \epsilon$, where ϵ is any unit of $Q(\delta)$. Thus, since this algorithm gives us a method of finding all relative minima Θ such that $\theta > 1$, we see that it can be used to find ϵ_0. Let

$$\theta_g^{(r)} = (m_1 + m_2\delta + m_3\bar{\delta})/\sigma_r, \qquad \theta_h^{(r)} = (n_1 + n_2\delta + n_3\bar{\delta})/\sigma_r,$$

where $m_1, m_2, m_3, n_1, n_2, n_3, \sigma_r \in Z$, $\sigma_r > 0$ and g.c.d. $(\sigma_r, m_1, m_2, m_3, n_1, n_2, n_3) = 1$. If we put $e_r = m_2n_3 - n_2m_3$, by Theorem 3.1 of [13], we have $N(\theta_r) = \sigma_r^2/|e_r|\sigma$. Thus, if r (>1) is the least integer such that $\sigma_r^2 = |e_r|\sigma$, then $\epsilon_0 = \theta_r$.

However, in many cases we need not go so far as the point where $N(\theta_r) = 1$ in the calculation of the θ_n's in order to find ϵ_0. In fact, for $D = p, 3p, 9p$ ($p \equiv 2, 5 \pmod 9$)), we will show that we can find ϵ_0 by using a certain special relative minimum of R. This relative minimum is the first relative minimum $\Theta_k \approx \theta_k$ in the chain starting with $\Theta_1 = (1, 0, 1)$ such that $N(\theta_k) = 3$ or 9; that is, such that $\sigma_k^2 = 3|e_k|$ or $\sigma_k^2 = 9|e_k|$. In the next section we will show how this can be done, but we first require the following simple results concerning relative minima.

LEMMA 5. *If $\Theta \approx \theta$ and $\Phi \approx \phi$ are relative minima of $\mathcal{R}$ and $\theta > \phi > 0$, then*

$$\theta^3/N(\theta) > \phi^3/N(\phi).$$

Proof. Since Θ is a relative minimum of $\mathcal{R}$ and $\phi < \theta$, we must have $\theta'\theta'' < \phi'\phi''$. (If $\theta'\theta'' = \phi'\phi''$, then $\theta = \pm\phi$ [4, p. 274].) Thus, $(\theta'\theta'')^{-1} > (\phi'\phi'')^{-1}$ and

$$\theta^2/\theta'\theta'' > \theta^2/\phi'\phi'' > \phi^2/\phi'\phi''.$$

LEMMA 6. *Let $\mathcal{R}$ have as its basis an integral basis of $Q[\delta]$ and let $\Theta \approx \theta$, $\Phi \approx \phi$ be relative minima of $\mathcal{R}$ such that $N(\phi), N(\theta) \neq 1, N(\theta) \neq N(\phi)$. If $\theta > \phi$, $N(\theta)|S$, and Φ is the least relative minimum such that $\phi > 1$ and $N(\phi)\,|\,S$, then $\phi^3/N(\phi) = \epsilon_0$.*

Proof. Since $\phi > 1$, there must be some nonnegative integer n such that

$$\epsilon_0^n < \phi < \epsilon_0^{n+1}.$$

If we put $\psi = \epsilon_0^{-n}\phi$, we have $1 < \psi < \epsilon_0$ and $N(\psi) = N(\phi)$. By definition of ϕ, we must have $\phi \leqslant \psi$; hence, $n = 0$ and $\phi < \epsilon_0$.

By Lemma 1, $\phi^3/N(\phi) \in Q[\delta]$ and $N(\phi^3/N(\phi)) = 1$; hence, $\epsilon_0^n = \phi^3/N(\phi)$ for some n. Since $\phi'\phi'' < 1$, we have $\phi > N(\phi)$ and $\phi^3/N(\phi) > 1$; thus, $n > 0$. Since $N(\phi) > 1$ and $\phi^3/N(\phi) < \epsilon_0^3$, we can only have $n = 1$ or 2. If $\chi = \epsilon_0^{-m}\theta$, where $1 < \chi < \epsilon_0$, then $N(\chi)\,|\,S$ and $\epsilon_0^r = \chi^3/N(\chi)$. Since r can only be 1 or 2 and $\phi < \chi$ by definition of ϕ, by Lemma 5 we must have $n = 1$.

4. The Main Results.

In order to prove the results given in this section we require

LEMMA 7. *If $x_1, x_2, x_3 \in Z$, $\alpha = x_1 + x_2\delta + x_3\bar{\delta}$, $|\alpha| < t_1$, $|\alpha'| < t_2$, then $3|x_1|, 3\delta|x_2|, 3\bar{\delta}|x_3| < t_1 + 2t_2$.*

Proof. Since

$$3x_1 = \alpha + \alpha' + \alpha'', \quad 3\delta x_2 = \alpha + \omega^2\alpha' + \omega\alpha'', \quad 3\bar{\delta}x_3 = \alpha + \omega\alpha' + \omega^2\alpha'',$$

we have

$$3|x_1|, 3\delta|x_2|, 3\bar{\delta}|x_3| < |\alpha| + |\alpha'| + |\alpha''| = |\alpha| + 2|\alpha'| < t_1 + 2t_2.$$

We now give a theorem which is analogous to the well-known result that if $(x, y) = 1$ and $x^2 - Dy^2 = N$, where $|N| < \sqrt{D}$, then x/y must be a convergent in the continued fraction expansion of $\sqrt{D}$.

THEOREM 1. *Let $\mathcal{R}$ have $[1, \delta, \bar{\delta}]$ as a basis and suppose $\alpha = x_1 + x_2\delta + x_3\bar{\delta} > 0$, where $x_1, x_2, x_3 \in Z$ and $(x_1, x_2, x_3) = 1$. If $N(\alpha) < \sqrt[3]{D}$, then A $(\approx \alpha)$ must be a relative minimum of $\mathcal{R}$.*

Proof. If A is not a relative minimum of $\mathcal{R}$ there must exist $\Gamma \in \mathcal{R}$ such that if $\gamma \approx \Gamma$, then $0 < \gamma < \alpha$ and $\gamma'\gamma'' < \alpha'\alpha''$. Let $\rho = N(\alpha)\gamma/\alpha$. If $P \approx \rho$, then $P \in \mathcal{R}$. Further, $0 < \rho < N(\alpha)$ and $\rho'\rho'' = |\rho'|^2 < N(\alpha)^2$; thus, if $\rho = r_1 + r_2\delta + r_3\bar{\delta}$ $(r_1, r_2, r_3 \in Z)$, by Lemma 7, we have $|r_1| < N(\alpha)$, $\delta|r_2| < N(\alpha)$, $\bar{\delta}|r_3| < N(\alpha)$. Now $\bar{\delta} > \delta > N(\alpha)$ and therefore $r_3 = r_2 = 0$. By Lemma 4, it follows that $\rho = 0$, which contradicts the assumption that $\gamma \neq 0$; hence, A is a relative minimum of $\mathcal{R}$.

COROLLARY *If $D \not\equiv \pm 1 \pmod 9$, $D > 9^3 = 729$ and $\Theta_k \approx \theta_k$ is the least relative minimum such that $\theta_k > 1$, $N(\theta_k) \neq 1$, and $N(\theta_k) | 9$, then $\epsilon_0 = \theta_k^3/N(\theta_k)$.*

Proof. Put $\phi = \theta_k^2$ when $N(\theta_k) = 3$; otherwise, put $\phi = \theta_k^2/3$. By Lemma 2, $\phi \in Q[\delta]$; hence, if $\Phi \approx \phi$, then $\Phi \in \mathcal{R}$ and $N(\phi) < \sqrt[3]{D}$. Thus, Φ is a relative minimum of $\mathcal{R}$. The corollary follows from Lemma 6.

Note that the above theorem gives us a method for finding all of the solutions of the Diophantine equation

$$N(\alpha) = x_1^3 + ab^2x_2^3 + a^2bx_3^3 - 3abx_1x_2x_3 = N,$$

when $N < \sqrt[3]{ab^2}$. We need only use Voronoi's algorithm to find all θ_r such that $N(\theta_r) = N$. It is necessary to check this only through the first period of the algorithm; for, if $N(\theta_r) = N$ and $\theta_r > \epsilon_0$, then $N(\epsilon_0^t\theta_r) = N$ and $1 < \epsilon_0^t\theta_r < \epsilon_0$ for some integer t.

We can improve the result of the corollary of Theorem 1 by using the corollary of

THEOREM 2. *Let $\mathcal{R}$ have as basis an integral basis of $Q[\delta]$ and suppose $\alpha = (x_1 + x_2\delta + x_3\bar{\delta})/\sigma \in Q[\delta]$, where $x_1, x_2, x_3 \in Z$ and $(x_1, x_2, x_3) | \sigma$. If $N(\alpha) | S$, $N(\alpha) = 3^\tau mn^2$, $m = m_1m_2$, $m_1 | a$ and $m_2 | b$, then A $(\approx \alpha)$ is a relative minimum of $\mathcal{R}$ when $\delta > 3^\eta m_2 n$ and $\bar{\delta} > 3^\eta m_1 n$. Here*

$$\eta = \begin{cases} 0, & D \not\equiv \pm 1 \pmod 9 \text{ and } \tau = 0, \\ 1, & \text{otherwise.} \end{cases}$$

Proof. As in Theorem 1, if A is not a relative minimum of $\mathcal{R}$, there must exist $\gamma \in Q[\delta]$ such that $0 < \gamma < \alpha$ and $\gamma'\gamma'' < \alpha'\alpha''$. Put $\rho = N(\alpha)\gamma/\alpha \in Q[\delta]$. If $\rho = (r_1 + r_2\delta + r_3\bar{\delta})/\sigma$, then, since $0 < \rho < N(\alpha)$ and $|\rho'| < N(\alpha)$, we have $|r_1|$, $\delta|r_2|$, $\bar{\delta}|r_3| < \sigma N(\alpha)$. Since $N(\rho) = N(\alpha)^2N(\gamma)$, we see by Lemma 2, that $n | (r_1, r_2, r_3)$; also, $N(\rho/n) = 3^{2\tau}m^2nN(\gamma)$ and $m | r_1$, $m_1 | r_2$, $m_2 | r_3$, by Lemma 3. Put $r_1 = mnt_1$, $r_2 = m_1nt_2$, $r_3 = m_2nt_3$; we have $\delta|t_2| < \sigma 3^\tau m_2 n$, $\bar{\delta}|t_3| < \sigma 3^\tau m_1 n$.

Case 1. $\tau > 0$. If $\sigma = 3$, then $3 \nmid S$; thus, since $3 | S$ here, we must have $D \not\equiv \pm 1 \pmod 9$ and $\sigma = 1$. If $\tau = 1$, we have $t_2 = t_3 = 0$; if $\tau = 2$, then $3 | (t_1, t_2, t_3)$ (Lemma 2) and $t_2/3 = t_3/3 = 0$. In either case we have $r_2 = r_3 = 0$ and $|r_1| < N(\alpha)$.

Case 2. $\tau = 0, D \not\equiv \pm 1 \pmod 9$. Again $\sigma = 1$ and $r_2 = r_3 = 0$.

Case 3. $\tau = 0, D \equiv \pm 1 \pmod 9$. Here $\sigma = 3$ and $r_2 = r_3 = 0$. Since $\rho \in Q[\delta]$ and $r_2 \equiv r_3 \equiv 0 \pmod 3$, we must have $r_1 \equiv 0 \pmod 3$; hence, $\rho \in Z$ and $\rho < N(\alpha)$.

The theorem now follows from Lemma 4.

COROLLARY. *Let Θ_k ($\approx \theta_k$) be the least relative minimum of $\mathcal{R}$ such that $\theta_k > 1$, $N(\theta_k) \neq 1$ and $N(\theta_k) \mid S$. Write $N(\theta_k) = 3^\tau mn^2$, where $n = n_1 n_2$ and $n_1 \mid a$, $n_2 \mid b$. Suppose that $\delta > 3^\eta n_2 m$, $\overline{\delta} > 3^\eta n_1 m$. Then $\epsilon_0 = \theta_k^3/N(\theta_k)$.*

Proof. Put $\psi = \theta_k^2/n$ when $\tau = 0, 1$ and put $\psi = \theta_k^2/3n$ when $\tau = 2$. By Lemma 2, $\psi \in Q[\delta]$; also, $N(\psi) = 3^\nu m^2 n$ ($\nu = 0, 2, 1$ when $\tau = 0, 1, 2$ respectively). If $\psi = (f_1 + f_2\delta + f_2\overline{\delta})/\sigma$, $p^\beta \mid (f_1, f_2, f_3)$ and $p^\beta \nmid \sigma$, then $p^3 \mid S$, which is not possible as S is cube-free; thus, by the theorem $\Psi \approx \psi$ is a relative minimum of $\mathcal{R}$.

Since $\theta_k' \theta_k'' < 1$, we have $N(\theta_k) < \theta_k$ and, consequently, $\psi > 1$. Further, $N(\psi) \mid S$ and $N(\psi) \neq 1$; thus, $\theta_k < \psi$ by definition of θ_k. By Lemma 6, it follows that $\epsilon_0 = \theta_k^3/N(\theta_k)$.

We see now that the restriction that D exceed 729 in the corollary of Theorem 1 can be replaced by the restriction that $D > 27$. Barrucand and Cohn [1], [2] have shown that if $D = p, 3p, 9p$, where $p \equiv 2, 5 \pmod 9$ and p is a prime, then $N(\alpha) = 3$ always has a solution with $\alpha \in Q[\delta]$. Thus, from Theorem 2, we see that if $D > 27$, then A ($\approx \alpha$) must be a relative minimum of $\mathcal{R}$ and this means that there must exist $\Theta_k \in \mathcal{R}$ as specified in the corollary. Hence, in the above cases, we can use Voronoi's algorithm to search for the least θ_k such that $N(\theta_k) = \sigma_k^2/|e_k|$ is 3 or 9. We then have $\epsilon = \theta_k^3/N(\theta_k)$ or

$$R = \log \epsilon_0 = 3 \log \theta_k - \log N(\theta_k) = 3 \sum_{i=1}^{k-1} \log \theta_g^{(i)} - \log(\sigma_k^2/|e_k|).$$

5. **Computational Results.** In [13] Voronoi's algorithm was modified for implementation on a computer. The amount of time needed to find the basis $[1, \theta_g^{(i+1)}, \theta_h^{(i+1)}]$ of $\mathcal{R}_{i+1}$, once the basis $[1, \theta_g^{(i)}, \theta_h^{(i)}]$ of $\mathcal{R}_i$ has been determined, is about 200 μ seconds on an AMDAHL 470/V7 computer. In spite of this speed, however, it is still very expensive to calculate R when $D = p, 3p, 9p$ and $p \equiv 2, 5 \pmod 9$. This is simply because, for such values of D, we have $D \not\equiv \pm 1 \pmod 9$ and the fairly likely possibility that the class number h of $Q(\delta)$ is one. Since

$$h = \frac{\Phi(1)\sqrt{|\Delta|}}{2\pi R},$$

where $\Phi(s)$ is the Artin L-function given by $\zeta_K(s)/\zeta(s)$, where $K = Q(\delta)$ (see [3]) and $\Phi(1) = O(\log|\Delta|)$ (Barrucand, private communication), we have $R = O(\sqrt{|\Delta|}\log|\Delta|)$ when $h = 1$. Also for two D values D_1, D_2 of about the same size such that $D_1 \equiv \pm 1 \pmod 9$ and $D_2 \not\equiv \pm 1 \pmod 9$, we expect that $\Delta_2 \gtrsim 9\Delta_1$ and the regulator tends to be 3 times longer for D_2 than for D_1.

In Table 1 we show how large the values of R can get to be. If D appears in the table, the regulator $R(D) > R(d)$ for all d such that $10^5 < d < D$, $d = p, 3p, 9p$, and $p \equiv 2, 5 \pmod 9$. Also, the value of k comes from $\epsilon_0 = \theta_k^3/N(\theta_k)$.

TABLE 1

D	R(D)	k
104369	227943.625	67135
105981	229038.437	67653
107717	230024.187	68201
107843	233824.437	68930
108347	234699.062	69339
112601	248248.875	73172
116507	259221.500	76585
117389	273369.250	80591
119783	280993.375	82874
127301	286446.812	84377
129011	287450.687	84996
141387	299283.437	88025
141653	306025.437	90313
143291	315992.125	92996
143879	361610.312	106989
161043	384876.562	114190
173139	394103.250	116390
184631	422310.000	124385
192317	431283.062	127155
195161	450992.375	132909
199109	455713.750	134645

By making use of the results of Section 4 we were able to triple the speed of our regulator program when $D = p, 3p, 9p$ ($p \equiv 2, 5 \pmod 9$). This program was used to calculate the regulator for $Q(\sqrt[3]{p})$ when $p \equiv 2, 5 \pmod 9$ and $p < 2 \times 10^5$. The class numbers of all these fields were subsequently calculated by making use of the Euler product method mentioned in [3].

Denote by $S_{a,b}(x)$ the set of all rational primes of the form $a + bt$ which are less than or equal to x, and denote by $H_1(a, b; x)$ ($H_2(a, b; x)$) the number of primes in $S_{a,b}(x)$ such that the class number of $Q(\sqrt{p})$ ($Q(\sqrt[3]{p})$) for $p \in S_{a,b}(x)$ is one. Let $\pi(a, b; x) = |S_{a,b}(x)|$. In Table 2 we present some values of $\pi(a, b; x)$, $H_2(a, b; x)$, and $H_2(a, b; x)/\pi(a, b; x)$ for $b = 9$ and $a = 2,5$. For some numerical results and references concerning $H_1(a, b; x)$ see Lakein [6]. Further references can be found in [10].

In Figures 1, 2, 3 below we show how the ratio $H_2(a, b; x)/\pi(a, b; x)$ varies as x increases to 2×10^5. The results illustrated in Figure 3 have been discussed in [12]. Figures 1 and 2 seem to reveal a difference between the behavior of $H_2(2, 9; x)$ and that of $H_2(5, 9; x)$. Why this difference should exist is not understood. It may be that $H_2(2, 9; x)/\pi(2, 9; x)$ is slowly increasing in the mean and that $H_2(5, 9; x)/\pi(5, 9; x)$ is slowly decreasing so that ultimately this initial distinction will disappear for very large x. In any event it would certainly appear that both of these ratios are decreasing sufficiently slowly to be consistent with the belief that there exists an infinitude of each type of field having class number one.

Table 2

x	$\pi(2,9;x)$	$H_2(2,9;x)$	$H_2(2,9;x)/\pi(2,9;x)$	$\pi(5,9;x)$	$H_2(5,9;x)$	$H_2(5,9;x)/\pi(5,9;x)$
2000	51	21	.4118	53	22	.4151
4000	95	37	.3895	93	34	.3656
6000	131	53	.4046	135	54	.4000
8000	169	69	.4083	170	71	.4176
10000	207	81	.3913	209	87	.4163
12000	243	95	.3909	242	96	.3967
14000	281	108	.3843	277	115	.4152
16000	319	130	.4075	312	131	.4199
18000	349	136	.3897	345	146	.4232
20000	382	150	.3927	380	160	.4211
22000	418	158	.3780	411	174	.4234
24000	449	172	.3831	450	196	.4356
26000	480	181	.3771	479	209	.4363
28000	515	195	.3786	513	225	.4386
30000	546	208	.3810	545	242	.4440
32000	576	222	.3854	577	257	.4454
34000	610	235	.3852	614	266	.4332
36000	638	243	.3809	647	281	.4343
38000	672	251	.3735	673	291	.4324
40000	705	263	.3730	709	314	.4429
50000	855	329	.3848	866	381	.4400
60000	1016	392	.3858	1012	441	.4358
70000	1154	437	.3787	1157	502	.4339
80000	1301	495	.3805	1308	568	.4343
90000	1447	555	.3836	1455	631	.4337
100000	1596	618	.3872	1597	683	.4277
110000	1742	683	.3921	1734	750	.4325
120000	1881	734	.3902	1882	816	.4336
130000	2022	786	.3887	2026	888	.4383
140000	2176	860	.3952	2169	943	.4348
150000	2318	918	.3960	2304	1000	.4340
160000	2462	986	.4005	2440	1067	.4373
170000	2601	1042	.4006	2572	1127	.4382
180000	2737	1095	.4001	2720	1185	.4357
190000	2867	1150	.4011	2861	1245	.4352
200000	2994	1200	.4008	2988	1293	.4327

FIGURE 1

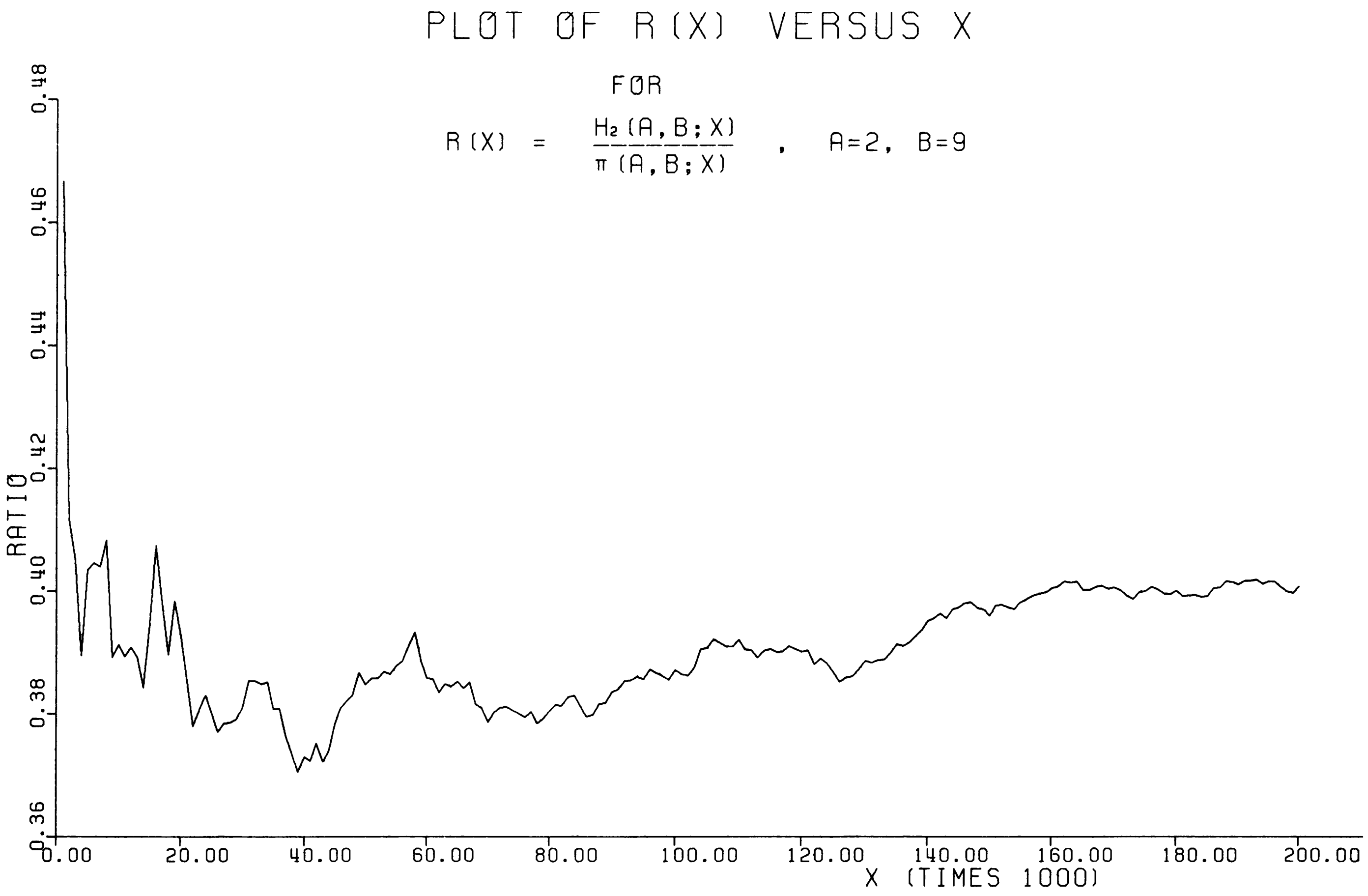

PLOT OF R(X) VERSUS X
FOR
$R(X) = \frac{H_2(A,B;X)}{\pi(A,B;X)}$, A=2, B=9
RATIO
0.36
0.38
0.40
0.42
0.44
0.46
0.48
0.00
20.00
40.00
60.00
80.00
100.00
120.00
140.00
160.00
180.00
200.00
X (TIMES 1000)

Figure 2

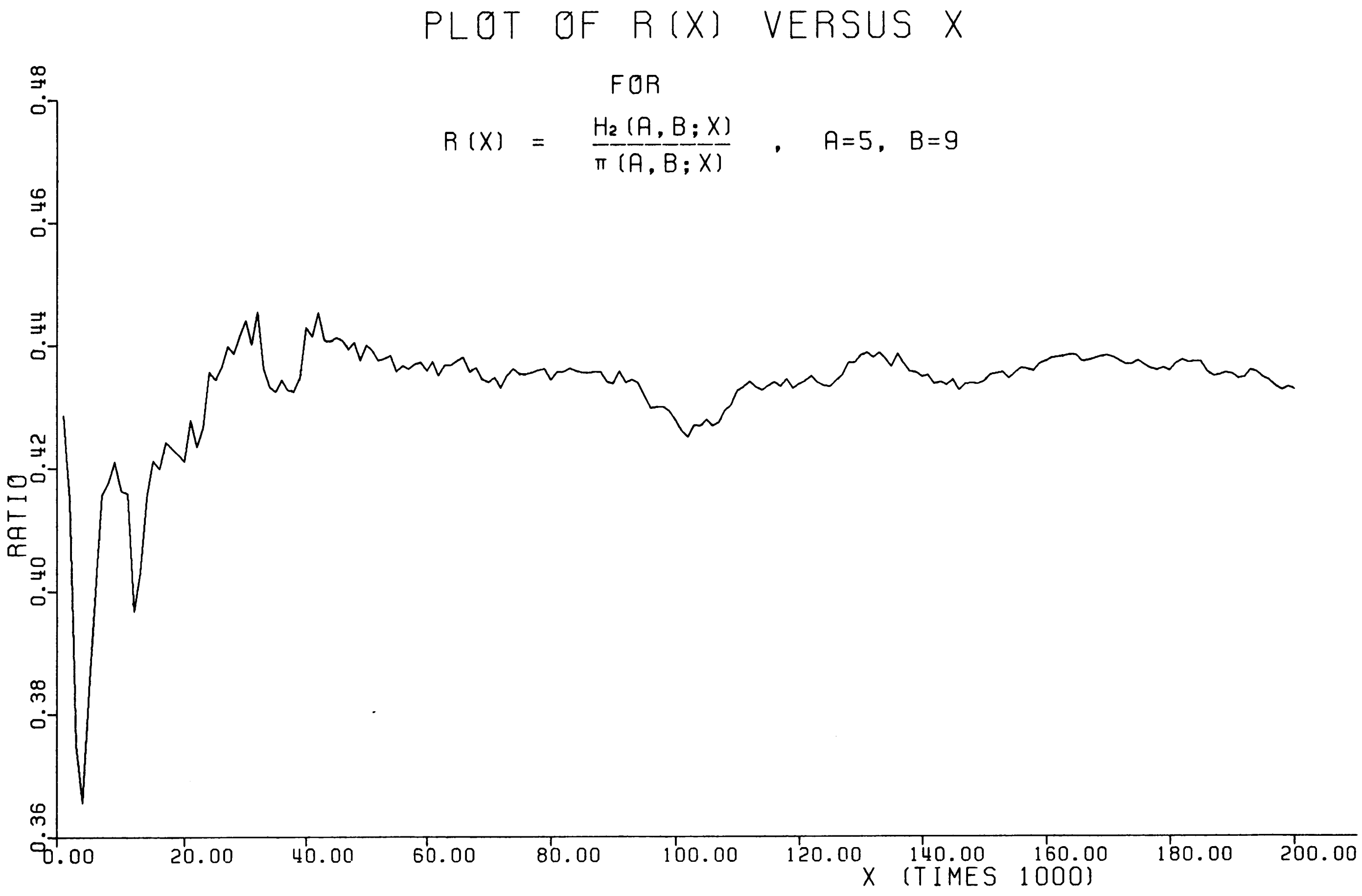
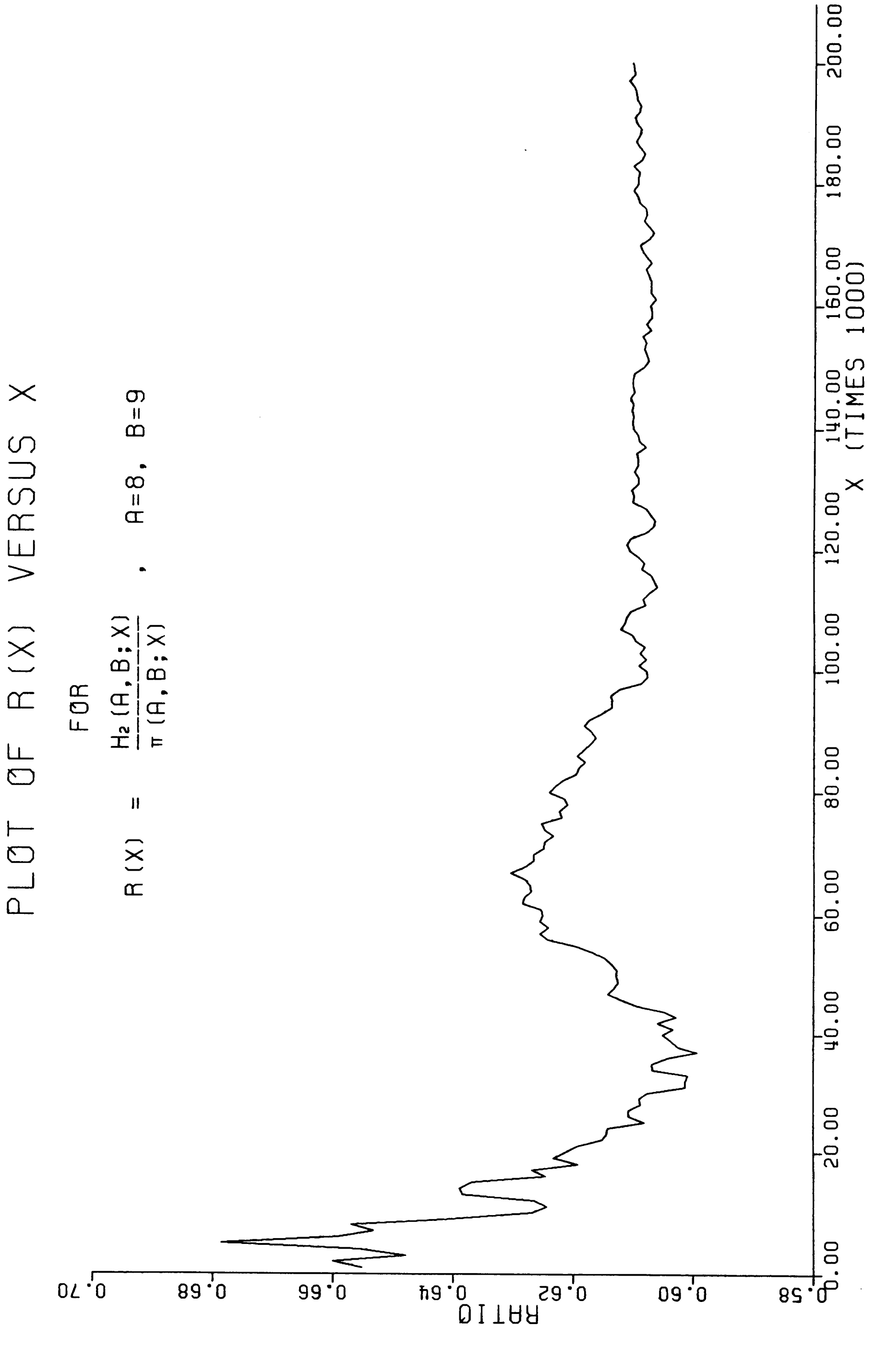

PLOT ØF R(X) VERSUS X
FØR
R(X) = H₂(A,B;X) / π(A,B;X) , A=5, B=9
RATIO
0.36
0.38
0.40
0.42
0.44
0.46
0.48
0.00
20.00
40.00
60.00
80.00
100.00
120.00
140.00
160.00
180.00
200.00
X (TIMES 1000)

FIGURE 3


PLOT OF R(X) VERSUS X
FOR
R(X) = H₂(A,B;X) / π(A,B;X) , A=8, B=9
RATIO
0.58
0.60
0.62
0.64
0.66
0.68
0.70
0.00
20.00
40.00
60.00
80.00
100.00
120.00
140.00
160.00
180.00
200.00
X (TIMES 1000)

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

1. PIERRE BARRUCAND & HARVEY COHN, "A rational genus, class number divisibility, and unit theory for pure cubic fields," *J. Number Theory*, v. 2, 1970, pp. 7–21.

2. PIERRE BARRUCAND & HARVEY COHN, "Remarks on principal factors in a relative cubic field," *J. Number Theory*, v. 3, 1971, pp. 226–239.

3. PIERRE BARRUCAND, H. C. WILLIAMS & L. BANIUK, "A computational technique for determining the class number of a pure cubic field," *Math. Comp.*, v. 30, 1976, pp. 312–323.

4. 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.

5. TAIRA HONDA, "Pure cubic fields whose class numbers are multiples of three," *J. Number Theory*, v. 3, 1971, pp. 7–12.

6. R. B. LAKEIN, "Review of UMT File: *Table of Class Numbers* $h(p)$ *Greater than* 1, *for Fields* $Q(\sqrt{p})$, $p \equiv 1 \pmod 4) \leqslant 2776817$," *Math.Comp.*, v. 29, 1975, pp. 335–336.

7. R. STEINER, "On the units in algebraic number fields," *Proc. 6th Manitoba Conf. on Numerical Math.*, Winnipeg, 1976, pp. 413–435.

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

9. H. C. WILLIAMS & J. BROERE, "A computational technique for evaluating $L(1, \chi)$ and the class number of a real quadratic field," *Math. Comp.*, v. 30, 1976, pp. 887–893.

10. H. C. WILLIAMS, "Certain pure cubic fields with class number one," *Math. Comp.*, v. 31, 1977, pp. 578–580; "Corrigendum", *Math. Comp.*, v. 33, 1979, pp. 847–848.

11. H. C. WILLIAMS & P. A. BUHR, "Calculation of the regulator of $Q(\sqrt{D})$ by use of the nearest integer continued fraction algorithm," *Math. Comp.*, v. 33, 1979, pp. 364–381.

12. H. C. WILLIAMS & DANIEL SHANKS, "A note on class number one in pure cubic fields," *Math. Comp.*, v. 33, 1979, pp. 1317–1320.

13. H. C. WILLIAMS, G. CORMACK & E. SEAH, "Calculation of the regulator of a pure cubic field," *Math. Comp.*, v. 34, 1980, pp. 567–611.