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 $\mathbb{Q}(\sqrt[3]{D})$, a complete period of Voronoi's continued fraction algorithm over $\mathbb{Q}(\sqrt[3]{D})$ 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 $\mathbb{Q}(\sqrt[3]{p})$, 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 $\mathbb{Q}(\sqrt[3]{D})$ is usually much larger than that of $\mathbb{Q}(\sqrt{D})$. For example, the largest regulator of $\mathbb{Q}(\sqrt{D})$, for all $D < 2 \times 10^5$, occurs for $D = 196771$ [11] and is 1291.32, while, for $D = 199109$, the regulator of $\mathbb{Q}(\sqrt[3]{D})$ is 455713.75.

The only primes $p$ such that $\mathbb{Q}(\sqrt[3]{p})$ can have class number one are those which have the form $3r - 1$ [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 $\mathbb{Q}(\sqrt[3]{p})$ 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 $\mathbb{Q}(\sqrt[3]{p})$ 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 $\mathbb{Q}(\sqrt[3]{D})$. 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
field formed by adjoining $\delta = \sqrt[3]{D}$ to the rationals $Q$. If $\overline{D} = a^2b$ and $\overline{\delta} = \sqrt[3]{D}$, then $Q(\delta) = Q(\overline{\delta})$; hence, we may assume that $a > b$.

If $D \not\equiv \pm 1 \pmod{9}$, then $[1, \delta, \overline{\delta}]$ is a basis of the ring of integers $Q[\delta]$ of $Q(\delta)$, and the discriminant $\Delta$ of $Q(\delta)$ is $-27a^2b^2$. If $D \equiv \pm 1 \pmod{9}$, then $[1, \delta, \beta]$, where $\beta = (1 + a\delta + b\overline{\delta})/3$, is a basis of $Q[\delta]$ and $\Delta = -3a^2b^2$. Thus, if $x_1, x_2, x_3 \in Z$ and $(x_1 + x_2\delta + x_3\overline{\delta})/\sigma \in Q[\delta]$, 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 $\alpha = (x_1 + x_2\delta + x_3\overline{\delta})/x_4$, where $x_1, x_2, x_3, x_4 \in Z$. Define the conjugates of $\alpha$ as

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

where $\omega$ is a fixed primitive cube root of unity. We define the norm of $\alpha$ 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 $\epsilon$ is a unit of $Q(\delta)$ and $\epsilon = \pm \epsilon_0^n$, for some $n \in Z$, where $\epsilon_0$ 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 $S = |A|/27$; otherwise, put $S = |A|/3$; thus, if $D \equiv \pm 1 \pmod{9}$, then $9|S$. We note that if $s$ is any rational prime divisor of $S$, then the ideal $[s] = \mathfrak{g}$, where $\mathfrak{g}$ is a prime ideal, and the norm of $\mathfrak{g}, N(\mathfrak{g})$, 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 $\alpha = (x_1 + x_2\delta + x_3\overline{\delta})/\sigma \in Q[\delta]$. If $t \mid S$ and $t^3 \mid N(\alpha)$, then $t|(x_1, x_2, x_3)$.

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

**Lemma 3.** Let $d = d_1d_2$, where $d_1, d_2 \in Z$, $d_1 \mid a$, and $d_2 \mid b$. If $d^2 \mid N(\alpha)$ when $\alpha = (x_1 + x_2\delta + x_3\overline{\delta})/\sigma \in Q[\delta]$, then $d|(x_1, d_1x_2, d_2x_3)$.

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

Our final result of this section is

**Lemma 4.** Let $\alpha = (x_1 + x_2\delta + x_3\overline{\delta})/\sigma \in Q[\delta]$, where $x_1, x_2, x_3 \in Z$ and $(x_1, x_2, x_3)|\sigma$. If $27\not|N(\alpha)$, $r \in Z$, $|r| < N(\alpha)$, and $ra = N(\alpha)\gamma$, where $\gamma \in Q[\delta]$, then $r = 0$.

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

*We denote by $p^\alpha|a$ the fact that $p^\alpha\mid a$ and $p^{\alpha+1}\not|a$. License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use*
If \( \sigma = 3 \) and \( N(\alpha)r \), then \( 3 | N(\alpha) \) and \( r = kN(\alpha)/3 \) with \( k \in \mathbb{Z} \) and \( (k, 3) = 1 \). Since \( r^3 = N(\alpha)^2N(\gamma) \), 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 \( \alpha \) is known, we often identify \( A \) with \( \alpha \) 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
\[
R = \{ A | A \approx x + y\mu + z\nu, x, y, z \in \mathbb{Z} \}.
\]

\( R \) is a lattice with basis \( \{1, \mu, \nu\} \).

We say that \( \Theta \approx \theta \in Q(\delta) \) is a relative minimum of \( R \) if \( \Theta \in R \) and there does not exist \( \Phi \in R \) such that \( \phi \neq 0 \), \( |\phi| < |\theta| \) and \( \phi'\phi'' < \theta'\theta'' \). If \( \Theta \) and \( \Phi \) are relative minima of \( R \) with \( \theta > \phi \), we say they are adjacent relative minima of \( R \) when there does not exist \( \Psi \in R \) such that \( \psi \neq 0 \), \( |\psi| < |\theta| \) and \( \psi'\psi'' < \phi'\phi'' \). If \( \theta_i \approx \Theta_i \in R \) \( (i = 1, 2, 3, \ldots, n, \ldots) \), \( \theta_{i+1} > \theta_i \), and \( \Theta_1, \Theta_{i+1} \) are adjacent relative minima, we call the sequence
\[
\Theta_1, \Theta_2, \Theta_3, \ldots, \Theta_n, \ldots,
\]
a chain of relative minima. If \( \Theta_j \) precedes \( \Theta_j \) in such a chain we say that \( \Theta_j \) is less than \( \Theta_j \). If \( \Phi \) is any relative minimum of \( R \) 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 \( R \). This technique is simply a means of finding in any such lattice a relative minimum \( \Theta_g \approx \theta_g \) adjacent to \( (1, 0, 1) \). Here we shall concern ourselves with finding \( \Theta_g \approx \theta_g \) such that \( \theta_g > 1 \). Let \( R_1 = R \) and let \( \Theta_g^{(1)} \approx \theta_g^{(1)} \) be the relative minimum adjacent to \( (1, 0, 1) \) in \( R_1 \) with \( \theta_g^{(1)} > 1 \). Embed \( 1, \theta_g^{(1)} \) in a basis of \( R_1 \) and let this basis be \( \{1, \theta_g^{(1)}, \theta_h^{(1)}\} \). Let \( R_2 \) have basis \( \{1, 1/\theta_g^{(1)}, \theta_h^{(1)}/\theta_g^{(1)}\} \).

We see that \( (1, 0, 1) \) is a relative minimum of \( R_2 \) and find the relative minimum \( \Theta_g^{(2)} \approx \theta_g^{(2)} \approx 1 \) adjacent to \( (1, 0, 1) \) in \( R_2 \). We continue this process by defining \( R_{i+1} \) 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 \( R_i \) and \( \{1, \theta_g^{(i)}, \theta_h^{(i)}\} \) is a basis of \( R_i \). It follows that \( \Theta_n \approx \theta_n \), where
\[
\theta_n = \prod_{i=1}^{\infty} \theta_g^{(i)}.
\]

If \( \{1, \mu, \nu\} \) is an integral basis of \( Q(\delta) \), then we see that \( (1, 0, 1) \) is a relative minimum of \( R \) and so is \( E \approx e \), where \( e \) is any unit of \( Q(\delta) \). Thus, since this algorithm gives us a method of finding all relative minima \( \Theta \) such that \( \theta > 1 \), we see that it can be used to find \( e_0 \). Let
\[
\theta_g^{(r)} = (m_1 + m_2\delta + m_3\delta)/\sigma_r, \quad \theta_h^{(r)} = (n_1 + n_2\delta + n_3\delta)/\sigma_r,
\]
where \(m_1, m_2, m_3, n_1, n_2, n_3, \sigma_r \in \mathbb{Z}, \sigma_r > 0\) and \(\gcd(\sigma_r, m_1, m_2, m_3, n_1, n_2, n_3) = 1\). If we put \(\varepsilon_r = m_2n_3 - n_2m_3\), by Theorem 3.1 of [13], we have \(N(\theta_r) = \sigma_r^2/|\varepsilon_r|\). Thus, if \(r (> 1)\) is the least integer such that \(\sigma_r^2 = |\varepsilon_r|\sigma\), then \(\varepsilon_0 = \theta_r\).

However, in many cases we need not go so far as the point where \(N(\theta_r) = 1\) in the calculation of the \(\theta_r\)'s in order to find \(\varepsilon_0\). In fact, for \(D = p, 3p, 9p (p = 2, 5 \pmod{9})\), we will show that we can find \(\varepsilon_0\) 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 \(\sigma_k^2 = \pm 3|e_k|\) or \(\sigma_k^2 = \pm 9|e_k|\). 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 \(R\) and \(\theta > \phi > 0\), then

\[
\theta^2/N(\theta) > \phi^2/N(\phi).
\]

**Proof.** Since \(\Theta\) is a relative minimum of \(R\) 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

\[
\theta^2/\theta'' > \phi^2/\phi'' > \phi^2/\phi'\phi''.
\]

**Lemma 6.** Let \(R\) have as its basis an integral basis of \(Q[\delta]\) and let \(\Theta \approx \theta, \Phi \approx \phi\) be relative minima of \(R\) such that \(N(\phi), N(\theta) \neq 1\), \(N(\theta) \neq N(\phi)\). If \(\theta > \phi, N(\theta) | S, \) and \(\Phi\) is the least relative minimum such that \(\phi > 1\) and \(N(\phi) | S\), then \(\phi^3/N(\phi) = \varepsilon_0\).

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

\[
\varepsilon_0^n < \phi < \varepsilon_0^{n+1}.
\]

If we put \(\psi = \varepsilon_0^n\phi\), we have \(1 < \psi < \varepsilon_0\) and \(N(\psi) = N(\phi)\). By definition of \(\phi\), we must have \(\phi < \psi\); hence, \(n = 0\) and \(\phi < \varepsilon_0\).

By Lemma 1, \(\phi^3/N(\phi) \in Q[\delta]\) and \(N(\phi^3/N(\phi)) = 1\); hence, \(\varepsilon_0^n = \phi^3/N(\phi)\) 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 \(\phi^3/N(\phi) < \varepsilon_0^3\), we can only have \(n = 1\) or 2. If \(x = \varepsilon_0^n\theta, \) where \(1 < x < \varepsilon_0, \) then \(N(\chi) | S\) and \(\varepsilon_0^r = \chi^3/N(\chi)\). Since \(r\) can only be 1 or 2 and \(\phi < \chi\) by definition of \(\phi\), 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 \(x_1, x_2, x_3 \in \mathbb{Z}, \alpha = x_1 + x_2\delta + x_3\bar{\delta}, |\alpha| < t_1, |\alpha'| < t_2, \) then

\[
3|\alpha|x_1, 3\delta|\alpha|x_2, 3\bar{\delta}|\alpha|x_3 < t_1 + 2t_2.
\]

**Proof.** Since

\[
3\alpha = \alpha + \alpha' + \alpha'', \quad 3\delta\alpha = \alpha + \omega^2\alpha' + \omega\alpha'', \quad 3\bar{\delta}\alpha = \alpha + \omega\alpha' + \omega^2\alpha'',
\]

we have

\[
3|\alpha|x_1, 3\delta|\alpha|x_2, 3\bar{\delta}|\alpha|x_3 < |\alpha| + |\alpha'| + |\alpha''| = |\alpha| + 2|\alpha'| < t_1 + 2t_2.
\]
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 \(R\) have \([1, \delta, \delta]\) as a basis and suppose \(\alpha = x_1 + x_2\delta + x_3\delta > 0\), where \(x_1, x_2, x_3 \in \mathbb{Z}\) and \((x_1, x_2, x_3) = 1\). If \(N(\alpha) < \sqrt[3]{D}\), then \(\alpha\) must be a relative minimum of \(R\).

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

**Corollary** If \(D \not\equiv \pm 1 (\mod 9)\), \(D > 93 = 729\) and \(\Theta_k \approx \theta_k\) is the least relative minimum such that \(\theta_k > 1\), \(N(\theta_k) \neq 1\), and \(N(\theta_k) \mid 9\), then \(e_0 = \theta_k^3/N(\theta_k)\).

**Proof.** Put \(\phi = \theta_k^3\) 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 \(\Phi \in R\) and \(N(\phi) < \sqrt[3]{D}\). Thus, \(\Phi\) is a relative minimum of \(R\). 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 \(\gamma_r\) such that \(N(\gamma_r) = N\). It is necessary to check this only through the first period of the algorithm; for, if \(N(\gamma_r) = N\) and \(\gamma_r > e_0\), then \(N(e_0\gamma_r) = N\) and \(1 < e_0\gamma_r < e_0\) for some integer \(t\).

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

**Theorem 2.** Let \(R\) have as basis an integral basis of \(Q[\delta]\) and suppose \(\alpha = (x_1 + x_2\delta + x_3\delta)/\sigma \in Q[\delta]\), where \(x_1, x_2, x_3 \in \mathbb{Z}\) and \((x_1, x_2, x_3) \mid \sigma\). If \(N(\alpha) \mid S\), \(N(\alpha) = 3^3m_1^2m_2\), \(m = m_1m_2\), \(m_1 \mid a\) and \(m_2 \mid b\), then \(A (\approx \alpha)\) is a relative minimum of \(R\) when \(\delta > 3^3m_2n\) and \(\delta > 3^3m_1n\). Here
\[\eta = \begin{cases} 0, & D \not\equiv \pm 1 (\mod 9) \text{ and } \tau = 0, \\ 1, & \text{otherwise.} \end{cases}\]

**Proof.** As in Theorem 1, if \(\alpha\) is not a relative minimum of \(R\), 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 \(\rho = (r_1 + r_2\delta + r_3\delta)/\sigma\), then, since \(0 < \rho < N(\alpha)\) and \(|\rho'| < N(\alpha)\), we have \(|r_1|, \delta|r_2|, \delta|r_3| < \sigma N(\alpha)\). Since \(N(\rho) = N(\alpha)^2N(\gamma)\), we see by Lemma 2, that \(n \mid (r_1, r_2, r_3)\); also, \(N(\rho/m) = 3^3m_2^2N(\gamma)\) and \(m_1r_1, m_2r_1, m_1r_2, m_2r_2, m_1r_3, m_2r_3\), by Lemma 3. Put \(r_1 = mnt_1, r_2 = m_1nt_2, r_3 = m_2nt_3\); we have \(\delta|t_2| < \sigma 3^3m_2n, \delta|t_3| < \sigma 3^3m_1n\).

**Case 1.** \(\tau > 0\). If \(\sigma = 3\), then \(3 \nmid S\); thus, since \(3 \mid \delta\), we must have \(D \equiv \pm 1 (\mod 9)\) and \(\sigma = 1\). If \(\tau = 1\), we have \(t_2 = t_3 = 0\); if \(\tau = 2\), then \(3 \mid (t_1, t_2, t_3)\) (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. \( \tau = 0, D \equiv \pm 1 \pmod{9} \). 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 \( \rho \in \mathbb{Q}[\delta] \) and \( r_2 \equiv r_3 \equiv 0 \pmod{3} \), we must have \( r_1 \equiv 0 \pmod{3} \); hence, \( \rho \in \mathbb{Z} \) and \( \rho < N(\alpha) \).

The theorem now follows from Lemma 4.

**Corollary.** Let \( \Theta_k (\approx \theta_k) \) be the least relative minimum of \( R \) such that \( \theta_k > 1, N(\Theta_k) \neq 1 \) and \( N(\theta_k) \mid S \). Write \( N(\Theta_k) = 3^r m^2 n \), where \( n = n_1 n_2 \) and \( n_1 \mid a, n_2 \mid b \). Suppose that \( \delta > 3^r n_2 m, \delta > 3^r n_1 m \). Then \( \epsilon_0 = \theta_k^3 / N(\Theta_k) \).

**Proof.** Put \( \psi = \theta_k^3 / n \) when \( \tau = 0, 1 \) and put \( \psi = \theta_k^3 / 3n \) when \( \tau = 2 \). By Lemma 2, \( \psi \in \mathbb{Q}[\delta] \); also, \( N(\psi) = 3^{2\nu} m^2 n \) (\( \nu = 0, 2, 1 \) when \( \tau = 0, 1, 2 \) respectively).

If \( \psi = (f_1 + f_2 \delta + f_3 \delta^2) / \sigma, p^\beta \mid (f_1, f_2, f_3) \) and \( p^3 \mid S \), 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 \( R \).

Since \( \theta_k^3 / \theta_k^6 < 1 \), 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 \( \theta_k \). 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 \( \alpha \in \mathbb{Q}[\delta] \). Thus, from Theorem 2, we see that if \( D > 27 \), then \( A \approx \alpha \) must be a relative minimum of \( R \) and this means that there must exist \( \Theta_k \in R \) as specified in the corollary. Hence, in the above cases, we can use Voronoi's algorithm to search for the least \( \theta_k \) 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

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

5. **Computational Results.** In [13] Voronoi's algorithm was modified for implementation on a computer. The amount of time needed to find the basis \( [1, \Theta_1^{(i+1)}, \Theta_2^{(i+1)}] \) of \( R_{i+1} \), once the basis \( [1, \Theta_1^{(i)}, \Theta_2^{(i)}] \) of \( R_i \) has been determined, is about 200 \( \mu \) 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 \( D \equiv \pm 1 \pmod{9} \) and the fairly likely possibility that the class number \( h \) of \( \mathbb{Q}[\delta] \) is one. Since

\[
h = \frac{\Phi(1) \sqrt{|\Delta|}}{2nR},
\]

where \( \Phi(s) \) is the Artin \( L \)-function given by \( \zeta_K(s) / \zeta(s) \), where \( K = \mathbb{Q}[\delta] \) (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 \( D_2 \equiv \pm 1 \pmod{9} \), 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

<table>
<thead>
<tr>
<th>$D$</th>
<th>$R(D)$</th>
<th>$k$</th>
</tr>
</thead>
<tbody>
<tr>
<td>104369</td>
<td>227943.625</td>
<td>67135</td>
</tr>
<tr>
<td>105981</td>
<td>229038.437</td>
<td>67653</td>
</tr>
<tr>
<td>107717</td>
<td>230024.187</td>
<td>68201</td>
</tr>
<tr>
<td>107843</td>
<td>233824.437</td>
<td>68930</td>
</tr>
<tr>
<td>108347</td>
<td>234699.062</td>
<td>69339</td>
</tr>
<tr>
<td>112601</td>
<td>248248.875</td>
<td>73172</td>
</tr>
<tr>
<td>116507</td>
<td>259221.500</td>
<td>76585</td>
</tr>
<tr>
<td>117389</td>
<td>273369.250</td>
<td>80591</td>
</tr>
<tr>
<td>119783</td>
<td>280993.375</td>
<td>82874</td>
</tr>
<tr>
<td>127301</td>
<td>286446.812</td>
<td>84377</td>
</tr>
<tr>
<td>129011</td>
<td>287450.687</td>
<td>84996</td>
</tr>
<tr>
<td>141387</td>
<td>299283.437</td>
<td>88025</td>
</tr>
<tr>
<td>141653</td>
<td>306025.437</td>
<td>90313</td>
</tr>
<tr>
<td>143291</td>
<td>315992.125</td>
<td>92996</td>
</tr>
<tr>
<td>143879</td>
<td>361610.312</td>
<td>106989</td>
</tr>
<tr>
<td>161043</td>
<td>384876.562</td>
<td>114190</td>
</tr>
<tr>
<td>173139</td>
<td>394103.250</td>
<td>116390</td>
</tr>
<tr>
<td>184631</td>
<td>422310.000</td>
<td>124385</td>
</tr>
<tr>
<td>192317</td>
<td>431283.062</td>
<td>127155</td>
</tr>
<tr>
<td>195161</td>
<td>450992.375</td>
<td>132909</td>
</tr>
<tr>
<td>199109</td>
<td>487113.750</td>
<td>136465</td>
</tr>
</tbody>
</table>

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 $Q(3\sqrt{p})$ 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 $Q(3\sqrt{p})$ ($Q(3\sqrt{p})$) 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 $\pi(a, b; x)$, $H_1(a, b; x)$, 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 $2 \times 10^5$. 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

<table>
<thead>
<tr>
<th>x</th>
<th>( r(2,9;x) )</th>
<th>( H_2(2,9;x) )</th>
<th>( H_2(2,9;x)/r(2,9;x) )</th>
<th>( \pi(5,9;x) )</th>
<th>( H_2(5,9;x) )</th>
<th>( H_2(5,9;x)/\pi(5,9;x) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>2000</td>
<td>51</td>
<td>21</td>
<td>.4118</td>
<td>53</td>
<td>.3656</td>
<td>.4151</td>
</tr>
<tr>
<td>4000</td>
<td>95</td>
<td>37</td>
<td>.3895</td>
<td>93</td>
<td>34</td>
<td>.3656</td>
</tr>
<tr>
<td>6000</td>
<td>131</td>
<td>53</td>
<td>.4046</td>
<td>135</td>
<td>54</td>
<td>.4000</td>
</tr>
<tr>
<td>8000</td>
<td>169</td>
<td>69</td>
<td>.4083</td>
<td>170</td>
<td>71</td>
<td>.4176</td>
</tr>
<tr>
<td>10000</td>
<td>207</td>
<td>81</td>
<td>.3913</td>
<td>209</td>
<td>87</td>
<td>.4163</td>
</tr>
<tr>
<td>12000</td>
<td>243</td>
<td>95</td>
<td>.3909</td>
<td>242</td>
<td>96</td>
<td>.3967</td>
</tr>
<tr>
<td>14000</td>
<td>281</td>
<td>108</td>
<td>.3843</td>
<td>277</td>
<td>115</td>
<td>.4124</td>
</tr>
<tr>
<td>16000</td>
<td>319</td>
<td>130</td>
<td>.4075</td>
<td>312</td>
<td>131</td>
<td>.4199</td>
</tr>
<tr>
<td>18000</td>
<td>349</td>
<td>136</td>
<td>.3897</td>
<td>345</td>
<td>146</td>
<td>.4232</td>
</tr>
<tr>
<td>20000</td>
<td>382</td>
<td>150</td>
<td>.3927</td>
<td>380</td>
<td>160</td>
<td>.4211</td>
</tr>
<tr>
<td>22000</td>
<td>418</td>
<td>158</td>
<td>.3780</td>
<td>411</td>
<td>174</td>
<td>.4234</td>
</tr>
<tr>
<td>24000</td>
<td>449</td>
<td>172</td>
<td>.3831</td>
<td>450</td>
<td>196</td>
<td>.4356</td>
</tr>
<tr>
<td>26000</td>
<td>480</td>
<td>181</td>
<td>.3771</td>
<td>479</td>
<td>209</td>
<td>.4363</td>
</tr>
<tr>
<td>28000</td>
<td>515</td>
<td>195</td>
<td>.3786</td>
<td>513</td>
<td>225</td>
<td>.4386</td>
</tr>
<tr>
<td>30000</td>
<td>546</td>
<td>208</td>
<td>.3810</td>
<td>545</td>
<td>242</td>
<td>.4440</td>
</tr>
<tr>
<td>32000</td>
<td>576</td>
<td>222</td>
<td>.3854</td>
<td>577</td>
<td>257</td>
<td>.4454</td>
</tr>
<tr>
<td>34000</td>
<td>610</td>
<td>235</td>
<td>.3852</td>
<td>614</td>
<td>266</td>
<td>.4332</td>
</tr>
<tr>
<td>36000</td>
<td>638</td>
<td>243</td>
<td>.3809</td>
<td>647</td>
<td>281</td>
<td>.4343</td>
</tr>
<tr>
<td>38000</td>
<td>672</td>
<td>251</td>
<td>.3735</td>
<td>673</td>
<td>291</td>
<td>.4324</td>
</tr>
<tr>
<td>40000</td>
<td>705</td>
<td>263</td>
<td>.3730</td>
<td>709</td>
<td>314</td>
<td>.4429</td>
</tr>
<tr>
<td>50000</td>
<td>855</td>
<td>329</td>
<td>.3848</td>
<td>866</td>
<td>381</td>
<td>.4400</td>
</tr>
<tr>
<td>60000</td>
<td>1016</td>
<td>392</td>
<td>.3858</td>
<td>1012</td>
<td>441</td>
<td>.4358</td>
</tr>
<tr>
<td>70000</td>
<td>1154</td>
<td>437</td>
<td>.3787</td>
<td>1157</td>
<td>502</td>
<td>.4339</td>
</tr>
<tr>
<td>80000</td>
<td>1301</td>
<td>495</td>
<td>.3805</td>
<td>1308</td>
<td>568</td>
<td>.4343</td>
</tr>
<tr>
<td>90000</td>
<td>1447</td>
<td>555</td>
<td>.3836</td>
<td>1455</td>
<td>631</td>
<td>.4337</td>
</tr>
<tr>
<td>100000</td>
<td>1596</td>
<td>618</td>
<td>.3872</td>
<td>1597</td>
<td>683</td>
<td>.4277</td>
</tr>
<tr>
<td>110000</td>
<td>1742</td>
<td>683</td>
<td>.3921</td>
<td>1734</td>
<td>750</td>
<td>.4325</td>
</tr>
<tr>
<td>120000</td>
<td>1881</td>
<td>734</td>
<td>.3902</td>
<td>1882</td>
<td>816</td>
<td>.4336</td>
</tr>
<tr>
<td>130000</td>
<td>2022</td>
<td>786</td>
<td>.3887</td>
<td>2026</td>
<td>888</td>
<td>.4383</td>
</tr>
<tr>
<td>140000</td>
<td>2176</td>
<td>860</td>
<td>.3952</td>
<td>2169</td>
<td>943</td>
<td>.4348</td>
</tr>
<tr>
<td>150000</td>
<td>2318</td>
<td>918</td>
<td>.3960</td>
<td>2304</td>
<td>1000</td>
<td>.4340</td>
</tr>
<tr>
<td>160000</td>
<td>2462</td>
<td>986</td>
<td>.4005</td>
<td>2440</td>
<td>1067</td>
<td>.4373</td>
</tr>
<tr>
<td>170000</td>
<td>2601</td>
<td>1042</td>
<td>.4006</td>
<td>2572</td>
<td>1127</td>
<td>.4382</td>
</tr>
<tr>
<td>180000</td>
<td>2737</td>
<td>1095</td>
<td>.4001</td>
<td>2720</td>
<td>1185</td>
<td>.4357</td>
</tr>
<tr>
<td>190000</td>
<td>2867</td>
<td>1150</td>
<td>.4011</td>
<td>2861</td>
<td>1245</td>
<td>.4352</td>
</tr>
<tr>
<td>200000</td>
<td>2994</td>
<td>1200</td>
<td>.4008</td>
<td>2988</td>
<td>1293</td>
<td>.4327</td>
</tr>
</tbody>
</table>
Figure 1

Plot of $R(X)$ versus $X$

For

$$R(X) = \frac{H_a(A, B; X)}{\pi(A, B; X)}$$

$A=2$, $B=9$
Figure 2

Plot of \( R(X) \) versus \( X \)

For

\[
R(X) = \frac{H_2(A, B; X)}{\pi(A, B; X)}, \quad A=5, \ B=9
\]
Figure 3

Plot of \( R(X) \) versus \( X \)

For

\[
R(X) = \frac{H_2(A,B;X)}{\pi(A,B;X)}, \quad A=8, \ B=9
\]


