Some Results Concerning Voronoi’s Continued Fraction Over $\mathbb{Q}(\sqrt[3]{D})$

By H. C. Williams

Abstract. Let $D$ be a cube-free integer and let $e_0$ be the fundamental unit of the pure cubic field $\mathbb{Q}(\sqrt[3]{D})$. It is well known that Voronoi’s algorithm can be used to determine $e_0$. In this work several results concerning Voronoi’s algorithm in $\mathbb{Q}(\sqrt[3]{D})$ are derived and it is shown how these results can be used to increase the speed of calculating $e_0$ for many values of $D$. Among these $D$ values are those such that $D (> 3)$ is not a prime $\equiv 8 \pmod{9}$ and the class number of $\mathbb{Q}(\sqrt[3]{V})$ is not divisible by 3. A frequency table of all class numbers not divisible by 3 for all $\mathbb{Q}(\sqrt[3]{V})$ with $D < 2 \times 10^5$ is also presented.

1. Introduction. It is well known (see, for example, Perron [9]) that if $\phi$ is a given real number and if we define $\phi_0 = \phi$, $q_0 = [\phi_0]$, $\phi_{n+1} = (\phi_n - q_n)^{-1}$, $q_{n-1} = [\phi_{n+1}]$ $(n = 0, 1, 2, 3, \ldots)$, then

$$\phi = q_0 + \frac{1}{q_1 + \frac{1}{q_2 + \frac{1}{q_3 + \ldots + \frac{1}{q_{n-1} + \frac{1}{\phi_n}}}}}$$

is the continued fraction expansion of $\phi$. We denote this by the less cumbersome $\phi = [q_0, q_1, q_2, \ldots, q_{n-1}, \phi_n]$.

If $A_{-1} = B_{-2} = 1$, $A_{-2} = B_{-1} = 0$ and $A_{r+1} = q_{r+1}A_r + A_{r-1}$, $B_{r+1} = q_{r+1}B_r + B_{r-1}$ $(r = -1, 0, 1, 2, 3, \ldots)$, we have

$$\frac{A_n}{B_n} = [q_0, q_1, q_2, \ldots, q_n].$$

Let $d$ be a square free positive integer and let $\phi = \sqrt{d}$. In this case we have

$$\phi_n = \frac{P_n + \sqrt{d}}{Q_n}.$$
where

\[ Q_0 = 1, \quad P_0 = 0, \quad q_0 = \lceil \sqrt{d} \rceil \quad \text{and} \]

\[ P_{r+1} = q_r Q_r - P_r, \quad Q_{r+1} = (d - P_{r+1}^2)/Q_r \quad (r = 0, 1, 2, 3, \ldots). \]

Let \( \mathbb{Q}(\sqrt{d}) \) be the quadratic field formed by adjoining \( \sqrt{d} \) to the rationals \( \mathbb{Q} \). If \( N(\alpha) \) is the norm of \( \alpha \in \mathbb{Q}(\sqrt{d}) \) \( (N(\alpha) = \bar{\alpha}\alpha, \text{where} \bar{\alpha} \text{is the conjugate of} \alpha) \), then

\[ N(A_n + \sqrt{d} B_n) = A_n^2 - dB_n^2 = (-1)^{n+1} Q_{n+1}. \]

Also, there always exists a least nonnegative integer \( s \) such that \( Q_{s+1} = 1 \). If \( \eta_0 > 1 \) is the fundamental unit of \( \mathbb{Q}(\sqrt{d}) \), then

\[ \eta_0 = A_s + \sqrt{d} B_s \quad \text{or} \quad \eta_0^3 = A_s + \sqrt{d} B_s. \]

The latter case occurs only when \( d > 5, \ d \equiv 5 \pmod{8} \) and \( Q_{k+1} = 4 \) for some \( k < s/2 \). In this event

\[ (1.1) \quad \eta_0 = (A_r + \sqrt{d} B_r)/2, \]

where \( r \) is the least positive integer such that \( Q_{r+1} = 4 \).

When \( N(\eta) = +1 \) (and no \( r \) as defined above exists), it is known that \( P_j = P_{j+1} \)

for a minimal \( j > 1 \). In this case we have \( s = 2j \) and

\[ (1.2) \quad \eta_0 = (A_{j-1} + \sqrt{d} B_{j-1})/Q_j \]

(see Williams and Broere [12]). Thus, in order to determine \( \eta_0 \) it is never necessary to go beyond \( q_{s/2} \) in the determination of the continued fraction expansion of \( \sqrt{d} \).

Note that \( Q_j \mid 2P_j \) and therefore \( \eta_j \mid 2d \). In fact, \( Q_j \) is a principal factor of the discriminant of \( \mathbb{Q}(\sqrt{d}) \) (see Barrucand and Cohn [1]).

In this paper we consider the pure cubic field \( \mathbb{Q}(\sqrt[3]{D}) \), where \( D = ab^2 \) is cube free and \( a, b \) are coprime integers. If \( \theta \in \mathbb{Q}(\sqrt[3]{D}) \), then \( \theta = (c_1 + c_2\delta + c_3\delta^2)/c_4 \), where \( \delta^3 = ab^2, \delta = a^2b, c_1, c_2, c_3, c_4 \in \mathbb{Q} \) (the set of rational integers). Also, we define the norm of \( \theta \) (written \( N(\theta) \)) to be \( N(\theta) = \theta^* \theta^{\prime*} \), where

\[ \theta^* = (c_1 + c_2\omega\delta + c_3\omega^2\delta^2)/c_4, \quad \theta^{\prime*} = (c_1 + c_2\omega^2\delta + c_3\omega\delta^2)/c_4, \]

and \( \omega \) is a primitive cube root of unity, i.e., an arbitrary but fixed zero of \( x^2 + x + 1 \).

Let \( \epsilon_0 > 1 \) be the fundamental unit of \( \mathbb{Q}(\delta) \). The usual continued fraction algorithm described above is not very useful for determining \( \epsilon_0 \). (It can be used to find \( \epsilon_0 \), however, when any nontrivial unit is known; see Jeans and Hendy [8]). In 1896 Voronoi [11] described an extension of the continued fraction algorithm which can be used to find \( \epsilon_0 \). A version of this algorithm is described in detail in Williams, Cormack, and Seah [13]. In this paper we extend the earlier work of Williams [14] by developing some further results concerning Voronoi's continued fraction algorithm which are analogous to the results (1.1) and (1.2) above. It will be seen that these developments allow us to increase the speed of calculating \( \epsilon_0 \) for many values of \( D \) and certainly for those values of \( D > 3 \) such that \( D \) is not a prime \( \equiv 8 \pmod{9} \) and the class number of \( \mathbb{Q}(\sqrt[3]{D}) \) is not divisible by 3. We also present a frequency table of all class numbers not divisible by three for all \( \mathbb{Q}(\sqrt[3]{D}) \) such that \( D < 2 \times 10^5 \).
2. Preliminary Results Concerning \( \mathcal{O}(\delta) \). We first require some well-known results on pure cubic fields.

If \( D \not\equiv \pm 1 \pmod{9} \), then \([1, \delta, \delta] \) is a basis of the ring of integers \( \mathcal{O}(\delta) \) of \( \mathcal{O}(\delta) \), and the discriminant \( \Delta \) of \( \mathcal{O}(\delta) \) is \(-27a^2b^2\). If \( D \equiv \pm 1 \pmod{9} \), then \([1, \delta, (1 + a\delta + b\delta)/3] \) is a basis of \( \mathcal{O}(\delta) \) and \( \Delta = -3a^2b^2 \). Thus, if \( x_1, x_2, x_3, \sigma \in \mathcal{O} \), g.c.d.\((x_1, x_2, x_3, \sigma) = 1 \) and \( \alpha = (x_1 + x_2\delta + x_3\bar{\delta})/\sigma \in \mathcal{O}(\delta) \), then \( \sigma = 1 \) when \( D \not\equiv \pm 1 \pmod{9} \) and \( \sigma = 3 \), \( x_1 \equiv ax_2 \equiv bx_3 \) (mod 3) when \( D \equiv \pm 1 \pmod{9} \). Further, \( N(\alpha) \in \mathcal{O} \) and

\[
(2.1) \quad \sigma^3N(\alpha) = x_1^3 + ab^2x_2^3 + a^2bx_3^3 - 3abx_1x_2x_3.
\]

If \( \epsilon \in \mathcal{O}(\delta) \) and \( N(\epsilon) = 1 \), we say that \( \epsilon \) is a unit of \( \mathcal{O}(\delta) \). Further, \( \epsilon = \pm \epsilon_0^\sigma \), where \( \sigma \in \mathcal{O} \). If \( 3 \mid D \), put \( S = \sigma/27 \); otherwise put \( S = \sigma/3 \). \( S \) is simply the square of the product of all primes \( p \in \mathcal{O} \) such that the principal ideal \([p] = P^3 \), where \( P \) is a prime ideal of \( \mathcal{O}(\delta) \) and the norm of \( P \), \( N(P) \), is \( p \). It should also be noted that if \( 3 \mid S \), then \([3] = PQ^2 \), where \( P, Q \) are distinct prime ideals of \( \mathcal{O}(\delta) \) and \( N(P) = N(Q) = 3 \).

We now present three simple lemmas which will be needed in the work that follows.

**Lemma 2.1.** Let \( \alpha = x_1 + x_2\delta + x_3\bar{\delta} \), where \( x_1, x_2, x_3 \in \mathcal{O} \).

(a) If \( 3 \mid D \), then \( 3 \mid N(\alpha) \) if and only if \( x_1 + ax_2 + bx_3 \equiv 0 \pmod{3} \).

(b) If \( 3 \mid D \) and \( D \equiv \pm 1 \pmod{9} \), then \( 9 \mid N(\alpha) \) if and only if \( x_1 \equiv ax_2 \equiv bx_3 \) (mod 3).

(c) If \( D \equiv \pm 1 \pmod{9} \), then \( 3 \mid \alpha \) if and only if \( x_1 \equiv ax_2 \equiv bx_3 \) (mod 3); also, if \( 27 \mid N(\alpha) \), then \( \alpha^\sigma /3 \in \mathcal{O}(\delta) \).

**Proof.** The first of (a) follows easily from (2.1) with \( \sigma = 1 \). To prove (b) we first note that \( \alpha^\sigma \in \mathcal{O}(\delta) \) and

\[
\alpha^\sigma = (x_1^2 - abx_1x_3) + (ax_2^2 - x_1x_2)\delta + (bx_3^2 - x_1x_3)\bar{\delta} \equiv \alpha^2 \pmod{3}.
\]

Since \([3] = P^3 \), we have \( \alpha^2 \equiv 0 \pmod{P^3} \), and \( \alpha'\alpha'' \equiv \alpha^2 \pmod{P^3} \); thus, \( \alpha \equiv 0 \pmod{P^3} \) and \( 3 \mid \alpha'\alpha'' \). It follows that \( 3 \mid x_1^2 - abx_1x_3, 3 \mid ax_2^2 - x_1x_2, 3 \mid bx_3^2 - x_1x_3 \), and therefore \( x_1 \equiv ax_1 \equiv bx_3 \pmod{3} \).

The proof of the first part of (c) follows easily from our previous remarks concerning the integers in \( \mathcal{O}(\delta) \). To prove the second part, we note that \([3] = PQ^2 \), \( \alpha'\alpha'' \equiv 0 \pmod{P^3Q^6} \), \( \alpha'\alpha'' \equiv \alpha^2 \pmod{PQ^2} \). Thus, \( \alpha'\alpha'' \equiv 0 \pmod{PQ^2} \) and \( \alpha'\alpha''/3 \in \mathcal{O}(\delta) \).

**Lemma 2.2.** If \( \alpha = (x_1 + x_2\delta + x_3\bar{\delta})/\sigma \in \mathcal{O}(\delta) \), \( t^3 \mid N(\alpha) \), and \( t \mid S \), then g.c.d.\((x_1, x_2, x_3) \equiv 0 \pmod{t} \).

**Proof.** See Lemma 2 of [14].

**Lemma 2.3.** Let \( \alpha \in \mathcal{O}(\delta) \) and let \( t = ef^2 \), where \( e = e_1e_2, f = f_1f_2 \), and \( e_1f_1 \mid a, e_2f_2 \mid b \). If \( t \mid N(\alpha) \), then

\[
\frac{\delta\alpha}{e_2f} \quad \frac{\overline{\delta}\alpha}{e_1f} \in \mathcal{O}(\delta). \]
Proof. From (2.1) and the fact that \( ef \mid ab \), we have \( f \mid x_1, e \mid x_1, f_1 \mid x_2, f_2 \mid x_3 \); thus

\[
\sigma \delta \alpha = x_1 \delta + x_2 b \delta + x_3 ab \equiv 0 \pmod{e_2 f},
\]
\[
\sigma \delta \alpha = x_1 \delta + x_2 ab + x_3 a \delta \equiv 0 \pmod{e_1 f}.
\]

Since \((\sigma, ab) = 1\), the lemma follows. \( \square \)

It is easy to see that if \( \alpha \in \mathbb{Z}[\delta] \) and \( N(\alpha) \mid S \), then \( \alpha^3 / N(\alpha) \in \mathbb{Z}[\delta] \). If such an \( \alpha \) exists and \( |N(\alpha)| \neq 1 \), \( ab^2 \), \( a^2b \), we say that \( |N(\alpha)| \) is a principal factor of the discriminant \( \Delta \); cf. [1]. Since \( N(\alpha^3 / N(\alpha)) = 1 \), we see that the determination of a unit of \( \mathbb{Z}(\delta) \) is a simple matter when such an \( \alpha \) is known. Several results concerning the existence of these principal factors can be found in Barrucand and Cohn [1], [2], Brunotte, Klinglen, and Steurich [4], and Halter-Koch [6].

Lemma 2.4. Let \( \alpha \in \mathbb{Z}[\delta] \) and suppose \( N(\alpha) \mid S \). Put \( N(\alpha) = 3^3d_1d_2d_3d_2d_5 \), where

\[
a = d_1d_2d_3, b = d_4d_5d_6.
\]

If

\[
\lambda^3 = 3^m \min\{d_1d_2d_3d_6^2, d_3d_5d_1d_6^2, d_2d_4d_2d_5^2\},
\]

then \( \beta = \lambda \alpha / N(\alpha)^{1/3} \in \mathbb{Z}[\delta] \). Further, \( N(\beta) \mid S \) and, if we put \( N(\beta) = 3^m m^2 \), where \( m = m_1m_2, n = n_1n_2, m_1n_1 \mid a, m_2n_2 \mid b \), then

\[
\frac{\delta}{m_2n}, \frac{\delta}{m_1n} > 1.
\]

Proof. Let \( \kappa_1 = d_1d_2d_6^2 / d_4d_5d_2^2 = (\delta / d_2d_4d_5)^3, \kappa_2 = d_3d_5d_6 / d_1d_2d_5^2 = (\delta / d_1d_2d_5)^3 \). We have \( N(\beta) = \lambda^3 \) and \( \lambda^3 / N(\alpha) = \min(1, \kappa_1, \kappa_2) \); hence, by Lemma 2.3, we have \( \beta \in \mathbb{Z}[\delta] \). Also, \( \{(\delta / m_2n)^3, (\delta / m_1n)^3\} \) is one of \( \{\kappa_1, \kappa_2\}, \{\kappa_2\kappa_1^{-1}, \kappa_1^{-1}\} \). If \( \lambda^3 / N(\alpha) = 1 \), then \( (\delta / m_2n)^3 = \kappa_1 > 1 \) and \( (\delta / m_1n)^3 = \kappa_2 > 1 \); if \( \lambda^3 / N(\alpha) = \kappa_1 \), then \( (\delta / m_2n)^3 = \kappa_2 \kappa_1^{-1} > 1 \) and \( (\delta / m_1n)^3 = \kappa_1^{-1} > 1 \); if \( \lambda^3 / N(\alpha) = \kappa_2 \), then \( (\delta / m_2n)^3 = \kappa_2^{-1} > 1 \) and \( (\delta / m_1n)^3 = \kappa_1 \kappa_2^{-1} > 1 \).

Thus, if we can find \( \alpha \in \mathbb{Z}[\delta] \) such that \( N(\alpha) \mid S \), we can easily find \( \beta \in \mathbb{Z}[\delta] \) such that \( N(\beta) \mid S \), \( N(\beta) = 3^m m^2 \), \( m = m_1m_2, n = n_1n_2, m_1n_1 \mid a, m_2n_2 \mid b \), and \( \delta / m_2n, \delta / m_1n > 1 \). Since \( \mathbb{Z}(\sqrt{ab^2}) = \mathbb{Z}(\sqrt{a^2b}) \), we can assume without loss of generality that \( a \) and \( b \) are such that

\[
\gamma_1 = \delta / m_2n < \gamma_2 = \delta / m_1n.
\]

For, if this is not the case, we can simply interchange the values of \( a \) and \( b \), \( m_1 \) and \( m_2 \), and \( n_1 \) and \( n_2 \).

We conclude this section by pointing out that if \( \alpha \in \mathbb{Z}[\delta], d = N(\alpha) \mid S \) and \( N(\alpha) = 3^3d_1d_2d_3d_2d_5 \), where \( d_1, d_2, d_3, d_4, d_5, d_6 \) are defined as above, then, by Lemmas 2.2 and 2.3, the six numbers

\[
\alpha, \frac{\delta \alpha}{d_1d_2d_3}, \frac{\delta \alpha}{d_1d_2d_5}, \frac{\alpha^2}{d_1d_2}, \frac{\delta \alpha^2}{d_2d_1d_4}, \frac{\delta \alpha^2}{d_2d_5d_1d_4}
\]

are all in \( \mathbb{Z}[\delta] \) and their norms all divide \( S \); thus, as noted in [1], each of the elements of the set

\[
(2.2) \{3^3d_1d_2d_3d_2, 3^3d_1d_2d_3d_2, 3^3d_2d_1d_2d_5, 3^3d_2d_1d_2d_5, 3^3d_2d_1d_2d_5, 3^3d_4d_3d_2d_5\}.
\]
where

\[ \nu = \begin{cases} 
0 & \text{when } \tau = 0, \\
1 & \text{when } \tau = 2, \\
2 & \text{when } \tau = 1,
\end{cases} \]

is a principal factor whenever \( d \) is. We call this set a **principal factor set**. If \( t \) is the number of distinct prime factors of \( S \), there are \((3^t - 3)/6\) sets of the form (2.2) but there can be at most one principal factor set; see [1].

### 3. Relative Minima

We first summarize some of the basic ideas concerning relative minima over a pure cubic lattice. For a more detailed discussion of these ideas see [13], [11], Delone and Faddeev [5] and Steiner [10].

Let \( \alpha = 2(\delta) \) 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 \( 2(\delta) \) and the upper-case letter to the corresponding ordered triple. Let \( \mu, \nu \in 2(\delta) \) and let

\[ \mathcal{R} = \{ A \mid A \approx x + y\mu + z\nu, x, y, z \in \mathbb{Z} \}. \]

We say that \( \mathcal{R} \) is a lattice with basis \([1, \mu, \nu]\).

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

\[ (3.1) \theta_1, \theta_2, \theta_3, \ldots, \theta_n, \ldots \]

a **chain** of relative minima. If \( \Theta_i \) precedes \( \Theta_j \) in such a chain we say that \( \Theta_i \) is less than \( \Theta_j \). It is easy to see that if \( \Phi \) is any relative minimum of \( \mathcal{R} \) and \( \phi > \theta_1 \), then \( \Phi = \Theta_k \) for some \( k \).

In [11] 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 \( \Theta_g \) adjacent to \((1, 0, 1)\). Here we shall concern ourselves with finding \( \Theta_g \approx \theta_g \) such that \( \theta_g > 1 \). Let \( \mathcal{R}_1 = \mathcal{R} \) 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 \((1, 0, 1)\) 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

\[ \theta_n = \prod_{i=1}^{n-1} \theta_g(i), \quad \theta_g(r) = \left( m_1 + m_2\delta + m_3\bar{\delta} \right)/\sigma_r, \]

\[ \theta_h(r) = \left( n_1 + n_2\delta + n_3\bar{\delta} \right)/\sigma_r, \]

\( m_1, m_2, m_3, n_1, n_2, n_3, \sigma_r \in \mathbb{Z}, \sigma_r > 0 \) and g.c.d.\((\sigma_r, m_1, m_2, m_3, n_1, n_2, n_3) = 1 \).
From now on we shall assume that $\mathfrak{R}_1$ is the lattice with basis $[1, \mu, \nu]$, where $[1, \mu, \nu]$ is an integral basis of $\mathcal{O}[\delta]$. We note that $(1, 0, 1)$ is a relative minimum of $\mathfrak{R}$ and so is $E \approx e$, where $e$ is any unit of $\mathcal{O}(\delta)$. Thus, since this algorithm gives us a method of finding all relative minima $\Theta$ such that $\theta > 1$, it can be used to find $e_0$. If we put $e_0 = m_2n_3 - n_2m_3$, by Theorem 3.1 of [13], we have $N(\theta) = \sigma^2 / |e_0|$. Thus, if $r > 1$ is the least integer such that $\sigma^2 = |e_0|\sigma$, then $e_0 = \theta_r$.

When $D \equiv \pm 1 \pmod{9}$, let $\mathfrak{R}_1$ be the lattice with basis $[1, \delta, \delta]$. If $E_0 \approx e_0$ and $E_0 \in \mathfrak{R}_1$, then $E_0$ is certainly a relative minimum of $\mathfrak{R}_1$. If, however, $E_0 \not\in \mathfrak{R}_1$, then $K_0 \approx k_0 = 3e_0$ is always in $\mathfrak{R}_1$, but it is not clear whether or not $K_0$ is a relative minimum of $\mathfrak{R}_1$. In fact, if $D = 44$, then $e_0 = (4007 + 1135\delta + 643\delta)/3$ and $K_0 \approx k_0 = 4007 + 1135\delta + 643\delta$ is not a relative minimum of $\mathfrak{R}_1$. In Theorem 3.1 we show that $D = 44$ is the largest $D$ value with $a > b$ such that $K_0$ is not a relative minimum of $\mathfrak{R}_1$.

**Theorem 3.1.** If $D \equiv \pm 1 \pmod{9}$, $\theta/3 \in \mathcal{O}[\delta]$ and $N(\theta) = 27$, then $\Theta (\approx \theta)$ is a relative minimum of $\mathfrak{R}_1$ whenever $a > b$ and $D > 44$.

**Proof.** If $\Theta$ is not a relative minimum of $\mathfrak{R}_1$, then there must exist $\gamma \approx \Gamma \in \mathfrak{R}_1$ such that $0 < \gamma < \theta$ and $\gamma'\gamma'' < \theta'\theta''$. Since $\theta/3 \in \mathcal{O}[\delta]$, we have $\theta'\theta''/9 \in \mathcal{O}[\delta]$; therefore, if $\rho = \theta'\theta''\gamma/3 = 9\gamma/\theta$, then $\rho = x_1 + x_2\delta + x_3\delta$, where $x_1, x_2, x_3 \in \mathbb{Z}$. Also, since $\rho \in \mathcal{O}[\delta]$ and $3 | \rho$, we have $x_1 \equiv ax_2 \equiv bx_3 \pmod{3}$ by Lemma 2.1. Since $|\delta| < 9$ and $|\rho'| = |\rho''| < 9$, we have $|x_1| < 9$, $|x_2| < 9$, $\delta|x_3| < 9$. It follows that if $\delta > 9$ and $\delta > 3$, then $x_2 = x_3 = 0$ and $x_1 = 9\gamma$; that is, $9 | x_1$ and therefore $x_1 = 0$ and $\Theta$ is a relative minimum of $\mathfrak{R}_1$. This will certainly be the case when $b > 9$; thus, there are only four possible values for $b$ such that $\Theta$ might not be a relative minimum of $\mathfrak{R}_1$. These are $1, 2, 5, 7$. If $b = 1$, then $D > 44$ means that $a > 44$, $\delta > 3$ and $\delta > 9$. If $b = 2$ and $a > 11$, then, since $a \equiv 2 \pmod{9}$, we must have $a > 29$; if $b = 5$, then $a \equiv 4 \pmod{9}$ and $a > 14$; if $b = 7$, then $a \equiv 2 \pmod{9}$ and $a > 11$. In all of these cases we see that $\delta > 9$ and $\delta > 3$, and the theorem now follows.

If $D \equiv \pm 1 \pmod{9}$, $\Theta (\approx \theta)$ is a relative minimum of $\mathfrak{R}_1$ and $N(\Theta) = 27$, it does not necessarily follow that $\theta/3 \in \mathcal{O}[\delta]$. For example, when $D = 62$, and $\theta = 15 + 48 + \delta$, we have $\Theta (\approx \theta)$ a relative minimum of $\mathfrak{R}_1$ and $\theta/3 \not\in \mathcal{O}[\delta]$. There is, however, a simple method of determining when a given $\Theta_r (\approx \theta_r)$ in the chain (3.1) of $\mathfrak{R}_1$ is such that $\theta_r/3 \in \mathcal{O}[\delta]$. We give this as

**Theorem 3.2.** If $\Theta_r (\approx \theta_r)$ is in the chain (3.1) of relative minima of $\mathfrak{R}_1$ with $\Theta_1 = (1, 0, 1)$ and $27 | N(\theta)$, then $\theta_r/3 \in \mathcal{O}[\delta]$ if and only if $3 | (\sigma_r/|e_r|)$.

**Proof.** The proof of this result makes use of the methods of Theorem 3.1 of [13]. Let $\gamma = \theta,\theta'' = g_1 + g_2\delta + g_3\delta$ and let $[1, \mu_r, \nu_r]$ be a basis of $\mathfrak{R}_r$. We have

\[
\begin{bmatrix}
1 \\
\mu_r \\
\nu_r
\end{bmatrix} = \frac{1}{\theta_r T \begin{bmatrix}
1 \\
\delta
\end{bmatrix}}
\]

where $T$ is a $3 \times 3$ matrix $(t_{ij})_{3 \times 3}$ with $t_{ij} \in \mathbb{Z}$ and $|T| = \pm 1$. Thus,

\[
\theta_r = t_{11} + t_{12}\delta + t_{13}\delta, \\
\theta_r \mu_r = t_{21} + t_{22}\delta + t_{23}\delta, \\
\theta_r \nu_r = t_{31} + t_{32}\delta + t_{33}\delta.
\]
and

\[ N(\theta_r) = (g_1 + g_2g + g_3g')(t_{11} + t_{12}g + t_{13}g') , \]

\[ N(\theta_r)\mu_r = (g_1 + g_2g + g_3g')(t_{21} + t_{22}g + t_{23}g') = u_1 + u_2g + u_3g, \]

\[ N(\theta_r)v_r = (g_1 + g_2g + g_3g')(t_{31} + t_{32}g + t_{33}g') = v_1 + v_2g + v_3g. \]

This can be written as

\[ (3.2) \]

\[
\begin{vmatrix}
27k & 0 & 0 \\
u_1 & u_2 & u_3 \\
v_1 & v_2 & v_3
\end{vmatrix}
= T
\begin{bmatrix}
g_1 & g_2 & g_3 \\
Dg_3 & g_1 & g_2 \\
Dg_2 & Dg_3 & g_1
\end{bmatrix},
\]

where \( k = N(\theta_r)/27 \). Taking determinants of both sides of (3.2), we get

\[ 27k(u_2v_3 - u_3v_2) = \pm N(\theta_r)^2 = \pm 27^2k^2 \]

and \( u_2v_3 - u_3v_2 = \pm 27k \). If we put

\[ d = \text{g.c.d.}(u_1, u_2, u_3, v_1, v_2, v_3, 27k), \]

we have \( \sigma_r = 27k/d \) and \( \epsilon_r = \pm 27k/d^2 \).

If \( \theta_r/3 \in \mathbb{Q}[\delta] \), then \( g_1 \equiv g_2 \equiv g_3 \equiv 0 \) (mod 3) and therefore \( 3 \mid d \). Since \( d = \sigma_r/|\epsilon_r| \), we have \( 3(\sigma_r/|\epsilon_r|) \).

If, on the other hand, \( 3 \mid (\sigma_r/|\epsilon_r|) \), then \( 3 \mid u_3 \) and \( 3 \mid v_3 \). Hence, from (3.2) we have \( TG \equiv 0 \) (mod 3), where

\[ G = \begin{bmatrix} g_3 \\ g_2 \\ g_1 \end{bmatrix}. \]

Since 27 is a divisor of \( N(\theta_r) \), we must have \( 3 \mid \theta_r/\theta_r'' \); hence, \( g_1 \equiv ag_2 \equiv bg_3 \) (mod 3) by Lemma 2.1. If \( 3 \mid g_1 \), then \( |T| \equiv 0 \) (mod 3), which is not true; thus \( g_1 \equiv g_2 \equiv g_3 \equiv 0 \) (mod 3). It follows that \( t_{11} \equiv at_{12} \equiv bt_{13} \) (mod 3) and \( \theta_r/3 \in \mathbb{Q}[\delta] \).

We now have a result analogous to (1.1) in the following

**Corollary.** If \( D \equiv \pm 1 \) (mod 9) \( (D > 44) \) and \( \Theta_r \approx \Theta_r \) is the first element of the chain (3.1) of relative minima of \( \mathcal{R}_1 \) with \( \Theta_1 = (1, 0, 1) \) such that \( N(\Theta_r) = 27 \) and \( 3 \mid (\sigma_r/|\epsilon_r|) \), then \( \epsilon_0 = \theta_r/3 \).

If we could find a relative minimum \( \Theta \approx \Theta_r \) of \( \mathcal{R}_1 \) such that \( N(\Theta) \mid S \), then, since \( N(\theta^3/N(\theta)) = 1 \), we could possibly shorten the labor needed in determining \( \epsilon_0 \). There are, however, certain divisors of \( S \) such that if \( N(a) \) is one of these divisors, then \( A \not\approx \alpha \) cannot be a relative minimum of \( \mathcal{R}_1 \). As we see in Lemma 3.3. two of these divisors of \( S \) are \( ab^2 \) and \( a^2b \).

**Lemma 3.3.** If \( \alpha \in \mathbb{Q}[\delta] \) and \( N(\alpha) = ab^2 \) or \( a^2b \), then \( A \not\approx \alpha \) cannot be a relative minimum of \( \mathcal{R}_1 \).

**Proof.** If \( N(\alpha) = ab^2 \), put \( \beta = a\delta/b \); if \( N(\alpha) = a^2b \), put \( \beta = a\delta/ab \). By Lemma 2.3, we must have \( \beta \in \mathbb{Q}[\delta] \). Since \( \delta \delta = ab \), we have \( 0 < \beta < \alpha \) and \( \beta' \beta'' < \alpha' \alpha'' \). It follows that \( A \) cannot be a relative minimum of \( \mathcal{R}_1 \).

Indeed, if \( N(\alpha) \) \( \mid S \) and \( \beta \) is defined as in Lemma 2.4, then \( A \not\approx \alpha \) cannot be a relative minimum of \( \mathcal{R}_1 \) whenever \( \alpha \neq \beta \). In Theorem 2 of [14] it was shown that if
THEOREM 3.4. Suppose there exists \( \alpha > 0 \) such that \( N(\alpha) \mid S \), \( 3 \mid N(\alpha) \), and either \( \tau > 0 \) or \( \sigma = 3 \) when \( \tau = 0 \). Let \( \beta, m, n, \gamma_1, \gamma_2 \) (\( \gamma_2 > \gamma_1 \)) be defined as in Lemma 2.4. Then \( B \approx \beta \) is not a relative minimum of \( R_1 \) if and only if there exists a nonzero \( \mu \in \mathbb{Z}[\delta] \) such that \( \mu = mn^2 \chi \), where \( \chi = X_1 + X_2 \gamma_1 + X_3 \gamma_2 \) (\( X_1, X_2, X_3 \in \mathbb{Z} \)) and

\[
\begin{align*}
(a) & \quad X_1 + am_2nX_2 + bm_1nX_3 \equiv 0 \pmod{3} \text{ when } \tau = 2, \\
(b) & \quad X_1 \equiv am_2nX_2 \equiv bm_1nX_3 \pmod{3} \text{ when } \tau = 1 \text{ or } 0,
\end{align*}
\]

\[
0 < \chi < 3,
\]

\[
F(\chi) = X_1^2 + \gamma_1^2X_2^2 + \gamma_2^2X_3^2 - \gamma_1X_1X_2 - \gamma_2X_1X_3 - \gamma_1\gamma_2X_2X_3 < 9.
\]

Proof. If \( B \) is not a relative minimum of \( R_1 \), there must exist \( \phi \in \mathbb{Z}[\delta] \) such that \( 0 < \phi < \beta \) and \( \phi'\phi'' < \beta'\beta'' \). If we put \( \rho = N(\beta)\phi/\beta \in \mathbb{Z}[\delta] \), we have

\[
0 < \rho < N(\beta),
\]

\[
|\rho'| = |\rho''| < N(\beta),
\]

\[
N(\rho) = N(\beta)^2N(\phi).
\]

If

\[
\rho = (x_1 + x_2\delta + x_3\bar{\delta})/\sigma, \quad (x_1, x_2, x_3 \in \mathbb{Z}),
\]

we have \( mn^2 \mid x_1, m_1n \mid x_2 \) and \( m_2n \mid x_3 \) by (3.8), Lemma 2.2, and Lemma 2.3.

If \( \sigma = 3 \), then \( D \equiv \pm 1 \pmod{9} \) and \( \tau = 0 \). If we put \( X_1 = x_1/mn^2, X_2 = x_2/m_1n, X_3 = x_3/m_2n \), we see that \( \mu = 3\rho, X_1 \equiv am_2nX_2 \equiv bm_1nX_3 \pmod{3} \) (Lemma 2.1) and \( 0 < \chi < 3, F(\chi) < 9 \) by (3.6) and (3.7).

If \( \sigma = 1 \) and \( \tau = 1 \), we find that \( \mu = \rho/3, 0 < \chi < 3, F(\chi) < 9 \), where \( X_1, X_2, X_3 \) are defined as above. Further, since \( 9 \mid N(\mu) \) (from (3.8)), we must have \( X_1 \equiv am_2nX_2 \equiv bm_1nX_3 \) by Lemma 2.1.

If \( \sigma = 1 \) and \( \tau = 2 \), then \( 81 \mid N(\mu) \) and \( 3 \mid x_1, 3 \mid x_2, 3 \mid x_3 \) by Lemma 2.2. Putting \( X_1 = x_1/3mn^2, X_2 = x_2/3m_1n, X_3 = x_3/3m_2n \), we get \( \mu = \rho/3, 0 < \chi < 3, F(\chi) < 9 \). Since \( N(\mu) = N(\rho)/27 \) and \( 81 \mid N(\mu), \) we have \( 3 \mid N(\mu) \); hence, \( X_1 + am_2nX_2 + bm_1nX_3 \equiv 0 \pmod{3} \) by Lemma 2.1.

Now suppose that \( \mu \) as described by the theorem exists. Define \( \theta = 3^r-1\mu\beta/N(\beta) \). By Lemma 2.1, we see that \( 3^{3-r} \mid N(\mu) \). Since \( m^2n^4 \mid N(\mu) \), we have \( N(\beta)^2 \mid N(3^{3-r}\mu) \) and \( N(\beta)^3 \mid N(3^{r-1}\mu) \). Since \( N(\beta) \mid S \), we see by Lemma 2.2 that \( \theta \in \mathbb{Z}[\delta] \). Also, since \( 0 < \chi < 3 \) and \( F(\chi) < 9 \), we have \( 0 < \theta < \beta \) and \( \theta'\theta'' < \beta'\beta'' \); thus, \( B \) cannot be a relative minimum of \( R_1 \).

COROLLARY. If \( B \) above is not a relative minimum of \( R_1 \), then \( \Theta \approx \theta = 3^{r-1}\mu\beta/N(\beta) \) is a relative minimum of \( R_1 \) when \( \mu = mn^2\chi \) and \( \chi \) is the least value of \( X_1 + X_2\gamma_1 + X_3\gamma_2 \) satisfying (3.3), (3.4), and (3.5).

In the next section we shall limit the possible values for the minimum \( \chi \) which satisfies (3.3), (3.4), and (3.5).

4. Some Lemmas Concerning \( \chi \). We first give a lemma which limits the possible values of \( X_1, X_2, X_3 \) with \( \text{g.c.d.}(X_1, X_2, X_3) = 1 \) for which \( \chi \) satisfies (3.4), (3.5), and (3.6).
**Lemma 4.1.** Let \( \chi = X_1 + X_2\gamma_1 + X_3\gamma_2 \), where \( X_1, X_2, X_3 \in \mathbb{Z} \), g.c.d.(\( X_1, X_2, X_3 \)) = 1, \( 0 < \chi < 3 \), \( F(\chi) < 9 \). If \( \mu = mn^2\chi, \mu \in \mathbb{Z}[\delta] \) and \( 3 \mid N(\mu) \), then values for \( X_1, X_2, X_3 \) must come from the 21 possible cases given in Tables 1, 2, and 3 below.

**Table 1**

<table>
<thead>
<tr>
<th>( X_1 )</th>
<th>1</th>
<th>1</th>
<th>-1</th>
<th>1</th>
<th>2</th>
<th>-1</th>
<th>2</th>
<th>-1</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>( X_2 )</td>
<td>-1</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>-1</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>-1</td>
</tr>
<tr>
<td>( X_3 )</td>
<td>2</td>
<td>-1</td>
<td>1</td>
<td>-1</td>
<td>1</td>
<td>1</td>
<td>-1</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>

**Table 2**

<table>
<thead>
<tr>
<th>( X_1 )</th>
<th>-1</th>
<th>0</th>
<th>0</th>
<th>2</th>
<th>2</th>
<th>-1</th>
</tr>
</thead>
<tbody>
<tr>
<td>( X_2 )</td>
<td>0</td>
<td>-1</td>
<td>2</td>
<td>-1</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>( X_3 )</td>
<td>2</td>
<td>2</td>
<td>-1</td>
<td>0</td>
<td>-1</td>
<td>0</td>
</tr>
</tbody>
</table>

**Table 3**

<table>
<thead>
<tr>
<th>( X_1 )</th>
<th>-1</th>
<th>-1</th>
<th>0</th>
<th>0</th>
<th>1</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>( X_2 )</td>
<td>0</td>
<td>1</td>
<td>-1</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>( X_3 )</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

**Proof.** Since \( F(\chi) < 9 \), we have \( |\chi + \omega X_2\gamma_1 + \omega^2 X_3\gamma_2| = |X_1 + \omega^2 X_2\gamma_1 + \omega X_3\gamma_2| < 3 \). We also have \( |\chi| < 3 \); hence, \( |X_1|, |X_2\gamma_1|, |X_3\gamma_2| < 3 \), and, since \( \gamma_1, \gamma_2 > 1 \), we have \( |X_1|, |X_2\gamma_1|, |X_3\gamma_2| < 3 \). Thus, there are at most \( 5 \times 5 \times 5 = 125 \) possible values for \( \chi \). Since \( 3 \mid N(\mu) \), we have \( X_1 + amnX_2 + bmnX_3 \equiv 0 \) (mod 3). If any two of \( X_1, X_2, X_3 \) are zero, the third must be zero. It follows that we can discard 13 of the 125 possible \( \chi \) values. Also, since g.c.d.(\( X_1, X_2, X_3 \)) = 1, we can eliminate 20 more of these possibilities. Since \( \gamma_2 > \gamma_1 > 1 \) and \( \chi > 0 \), we can eliminate 35 more cases and 14 additional ones can be deleted by noticing that \( \chi < 3 \).

Since \( F(\chi) = 3X_1^2 - 3X_1\chi + \chi^2 - 3X_2X_3\gamma_1\gamma_2 \), it is clear that if \( X_2X_3 = -2 \), then \( F(\chi) > 9 \) whenever \( X_1 = 0, 1 \). This allows us to reject 10 more cases. Since

\[
4F(\chi) = (2X_1 - \gamma_1X_2 - \gamma_2X_3)^2 + 3(X_2\gamma_1 - X_3\gamma_2)^2 < 36,
\]

we must have \( |X_2\gamma_1 - X_3\gamma_2| < 2\sqrt{3} \). Thus, if \( X_2X_3 < 0 \), we have \( |X_2\gamma_1| + |X_2\gamma_2| < 2\sqrt{3} \) and, consequently,

\[
|X_2X_3|\gamma_1\gamma_2 < 3.
\]

Therefore, we cannot have \( X_2X_3 = -4 \) and, as a result, we are able to eliminate three further cases. We also have \( |2X_1 - \gamma_1X_2 - \gamma_2X_3| < 6 \); hence, if \( X_1 = -2 \) and \( X_2, X_3 > 0 \), we must have \( \gamma_1|X_2| + \gamma_2|X_3| < 2 \). Since this is not possible, we can reject three more possibilities.
If \( x = -2 + y^2 \) and \( F(\chi) < 9 \), then \( y^2 < \sqrt{36 - \frac{3(\chi - X_2\gamma_1)^2}{X_1}} \). Since this means that \( \chi < 0 \), we cannot have \( x = -2 + y^2 \). Similarly, it is not possible to have \( x = -2 + \gamma_1 \) or \( x = -2\gamma_1 + \gamma_2 \), and we are able to reject three more cases.

If, for \( x = X_1 + X_2\gamma_1 + X_3\gamma_2 \), we are to have \( F(\chi) < 9 \), then it is necessary and sufficient that

\[
(4.2) \quad X_1 + X_2\gamma_1 - \sqrt{36 - 3(X_1 - X_2\gamma_1)^2} < 2X_3\gamma_2 < X_1 + X_2\gamma_1 + \sqrt{36 - 3(X_1 - X_2\gamma_1)^2}.
\]

Thus, if \( x = 1 - 2\gamma_1 + \gamma_2 \) and \( F(\chi) < 9 \), we have

\[
2\gamma_2 < 1 - 2\gamma_1 + \sqrt{36 - 3(1 + 2\gamma_1)^2}.
\]

Since \( 28\gamma_1^2 + 4\gamma_1 > 32 \), we have

\[
2\gamma_1 > 1 - 2\gamma_1 + \sqrt{36 - 3(1 + 2\gamma_1)^2} > 2\gamma_2,
\]

which is a contradiction.

If \( x = -1 - \gamma_1 + \gamma_2 \) and \( 0 < x < 3 \), then \( \gamma_2 > \gamma_1 + 1 \). But \( 12\gamma_1^2 + 12\gamma_1 > 24 \) or \( 9(\gamma_1 + 1)^2 > 36 - 3(1 - \gamma_1)^2 \); hence, \( 2(\gamma_1 + 1) > -\gamma_1 - 1 + \sqrt{36 - 3(1 - \gamma_1)^2} > 2\gamma_2 \) when \( F(\chi) < 9 \). This is also a contradiction. Similarly, if \( \chi = -2 - \gamma_1 + \gamma_2 > 0 \), then \( \gamma_2 > 2 + \gamma_1 \). Here we have \( 2(2 + \gamma_1) > -2 - \gamma_1 + \sqrt{36 - 3(2 - \gamma_1)^2} > 2\gamma_2 \) when \( F(\chi) < 9 \). We have eliminated three more cases, and only the 21 cases given in Tables 1, 2, 3 remain. □

For the case in which we must have \( X_1 \equiv am_2nX_2 \equiv bm_1nX_3 \mod 3 \), we can limit the minimum value of \( \chi \) yet further. We do this in

**Lemma 4.2.** Let \( \mu = mn^2 \chi \in \mathbb{Z}[\delta] \) and let \( \chi \) be the least positive value of \( X_1 + X_2\gamma_1 + X_3\gamma_2 \) such that \( X_1, X_2, X_3 \in \mathbb{Z}, X_1 \equiv am_2nX_2 \equiv bm_1nX_3 \mod 3 \), and \( F(\chi) < 9 \). We can have \( \chi < 3 \) if and only if one of the following is true.

(i) \( am_2n \equiv 1, bm_1n \equiv -1 \mod 3 \),

\[
2\gamma_2 < -1 - \gamma_1 + \sqrt{36 - 3(\gamma_1 - 1)^2}, \quad \chi = 1 + \gamma_1 - \gamma_2.
\]

(ii) \( am_2n \equiv -1, bm_1n \equiv 1 \mod 3 \),

\[
2\gamma_2 < 1 - \gamma_1 + \sqrt{36 - 3(1 + \gamma_1)^2}, \quad \chi = 1 - \gamma_1 + \gamma_2.
\]

(iii) \( am_2n \equiv bm_1n \equiv -1 \mod 3 \),

\[
2\gamma_2 < -1 + \gamma_1 + \sqrt{36 - 3(1 + \gamma_1)^2}, \quad \chi = -1 + \gamma_1 + \gamma_2.
\]

**Proof.** Clearly g.c.d.(\( X_1, X_2, X_3 \)) = 1 and none of the \( X_1 \)'s can be zero; thus, the only possibilities for \( X_1, X_2, X_3 \) are those given in Table 1.

Suppose \( X_3 > 0 \); if \( F(\chi) < 9 \), then by (4.2) we must have

\[
(4.3) \quad 2\gamma_2 X_3 - X_1 - X_2\gamma_1 < \sqrt{36 - 3(X_1 - X_2\gamma_1)^2}.
\]

On the other hand, if (4.3) is true for \( (X_1, X_2) = (1, -1), (-1, 1), (2, -1), (-1, 2) \), the left-hand side of (4.3) must exceed zero; hence,

\[
4F(\chi) = (2\gamma_2 X_3 - X_1 - X_2\gamma_1)^2 + 3(X_1 - X_2\gamma_1)^2 < 36.
\]
Also, for the above values of $X_1$ and $X_2$ it is easy to verify that

$$(X_2Y_1 + X_1)^2 - X_1X_2Y_1 > 3(X_1 + X_2Y_1);$$

thus,

$$\sqrt{36 - 3(X_1 - \gamma_1X_2)^2} < 6 - 3X_1 - 3X_2Y_1,$$

and $X_3Y_2 < 3 - X_1 - X_2Y_1$ or $X < 3$. Hence, since $X > 0$ for the values of $X_1$ and $X_2$ in Table 1 when $X > 0$, we see that, for these values of the $X$’s, we have $F(X) < 9$ and $0 < X < 3$ whenever (4.3) is true.

Suppose $X_3 < 0$ and

$$(4.4) \quad 2\gamma_2X_3 > X_1 + \gamma_1X_2 - \sqrt{36 - 3(X_1 - \gamma_1X_2)^2}.$$  

We have

$$X_1 + X_2Y_1 - 2X_3Y_2 < \sqrt{36 - 3(X_1 - \gamma_1X_2)^2}.$$

For $(X_1, X_2, X_3) = (1, 1, -1), (1, 2, -1), (2, 1, -1)$, we also have $X_1 + X_2Y_1 - 2X_3Y_2 > 0$; hence,

$$4F(X) = (2X_3Y_2 - X_1 - X_2Y_1)^2 + 3(X_1 - X_2Y_1)^2 < 36.$$

Since $X_2X_3 < 0$, we see from (4.1) that $|X_2X_3|\gamma_1Y_2 < 3$. Consequently, $0 < X_2Y_1 < \sqrt{3}$ (as $X_2X_3 = -1, -2$) and $X < 3$. We also have $X_1^2 + X_1X_2Y_1 + X_2^2Y_1 > 3$; therefore,

$$9(X_1 + \gamma_1X_2)^2 > 36 - 3(X_1 - \gamma_1X_2)^2 \quad \text{and} \quad X > 0.$$

Thus, if $X_3 < 0$ and (4.4) is true, then $0 < X < 3$ and $F(X) < 9$.

If $am_2n \equiv bm_1n \equiv 1$ (mod 3), we must have $X_1 \equiv X_2 \equiv X_3$ (mod 3), and no such case exists in Table 1.

If $am_2n \equiv bm_1n \equiv -1$ (mod 3), then $X$ must be one of $X_1 = 1 - \gamma_1 + 2\gamma_2$, $X_2 = 1 + 2\gamma_1 - \gamma_2, X_3 = -1 + \gamma_1 + \gamma_2$. Put $4r_1 = -\gamma_1 + 1 + \sqrt{36 - 3(1 + \gamma_1)^2}$, $2r_2 = -1 - 2\gamma_1 + \sqrt{36 - 3(1 - 2\gamma_1)^2}$, $2r_3 = -1 + \gamma_1 + \sqrt{36 - 3(1 + \gamma_1)^2}$.

From the results proved above, we see that if $\gamma_2 < r_3$, then $F(X) < 9$ and $0 < \chi < 3$. Since $\gamma_1 > 1$, it can be verified that $r_3 > r_1, r_3 > r_2$ and $r_2 < 1 + \gamma_1/2$. If $X_3 > X_2$, then $\gamma_2 > 1 + \gamma_1/2 > r_2$ and $F(X_2) > 9$ by (4.2). If $X_3 > X_1$, then $\gamma_2 < 2\gamma_1 - 2$; hence, $\gamma_1 < 2\gamma_1 - 2$ and $\chi > 2$. But, if $F(X_3) < 9$, we must have $\gamma_2Y_1 < 3$, by (4.1), and therefore $\gamma_1 < \sqrt{3}$, which is a contradiction. It follows that, if either of $X_1$ or $X_2$ is such that $0 < \chi < 3$ and $F(X) < 9$, $0 < \chi < 3$ and $F(X_3) < 9$, thus, $X = X_3$.

The values of $\chi$ for $am_2n \equiv 1, bm_1n \equiv 1$ (mod 3) and $am_2n \equiv -1, bm_1n \equiv 1$ (mod 3) can be verified in a similar fashion.

As an example of this result, we notice that, if $\alpha = 4 + 2\delta + \vec{\delta}$ when $D = 10$, then $N(\alpha) = 4$ and $4 | S$. We have $d_1 = d_4 = d_5 = d_6 = 1, d_2 = 2, d_3 = 5$ and $\lambda^3 = m_1m_2n^2 = \min(4, 5, 20) = 4$; hence, $\beta = \alpha$. Also, $am_2n = 20 \equiv -1$ (mod 3) and $bm_1n = 2 \equiv -1$ (mod 3), $\gamma_1 = \sqrt{10}/2 \approx 1.08, \gamma_2 = \sqrt{10}/2 \approx 2.32$ and $2\gamma_2 < -1 + \gamma_1 + \sqrt{3(1 + \gamma_1)^2}$. Thus, $B (\approx \beta = \alpha)$ is not a relative minimum of $R_1$. In fact, if $\theta = (11 + 5\delta + 2\vec{\delta})/3 = (-4 + 2\delta + 2\vec{\delta}) \cdot (4 + 2\delta + \vec{\delta})/12$, then $\Theta (\approx \theta)$ is a relative minimum of $R_1$.

We now limit the possibilities for $\chi$ when (3.3a) is true but (3.3b) is not.
Lemma 4.3. Let $\mu \in \mathbb{G}[\delta]$ and $\mu = mn^2x$, where $x$ is the least positive value of $X_1 + \gamma_1X_2 + \gamma_2X_3$ such that $X_1, X_2, X_3 \in \mathbb{G}$, $F(x) < 9$ and $X_1 + am_2nX_2 + bm_1nX_3 \equiv 0 \pmod{3}$. If it is not the case that $X_1 \equiv am_2nX_2 \equiv bm_1nX_3 \pmod{3}$, then $x < 3$ if and only if one of the following is true.

(i) $am_2n \equiv bm_1n \equiv 1 \pmod{3}$, $\gamma_1 < (\sqrt{33} - 1)/2$. In this case $x$ is one of $\gamma_1 - 1$ or $\gamma_2 - \gamma_1$;

(ii) $am_2n \equiv bm_1n \equiv -1 \pmod{3}$, $\gamma_1 < 2$. In this case $x$ is one of $\gamma_2 - \gamma_1, 2 - \gamma_1, 1 + \gamma_1$;

(iii) $am_2n \equiv 1, bm_1n \equiv -1, \gamma_1 < (\sqrt{33} - 1)/2$. In this case $x = -1 + \gamma_1$;

(iv) $am_2n \equiv -1, bm_1n \equiv 1 \pmod{3}$, $\gamma_1 < (\sqrt{33} - 1)/2$ or $\gamma_1 < 2$. In this case $x$ is one of $-1 + \gamma_2, 2 - \gamma_1, 2 - \gamma_1, 2 - \gamma_1$.

Proof. We can assume once again that $\gcd(X_1, X_2, X_3) = 1$. Thus, from Lemma 4.1 we can only have values for $X_1, X_2, X_3$ given by those in Tables 2 and 3. Also, if the values of $X_1, X_2, X_3 (X_3 \neq 0)$ are selected from Table 2, then, in order for $F(x) < 9$, we must have $y_2 < 2$.

The proofs of the remaining cases are similar to the following proof of case (iii); thus, we will only prove this case of the lemma here. If $am_2n \equiv 1, bm_1n \equiv -1 \pmod{3}$, the only possible values for $X_1, X_2, X_3$ are given in Table 4 below.

<table>
<thead>
<tr>
<th>$X_1$</th>
<th>-1</th>
<th>0</th>
<th>1</th>
<th>-1</th>
<th>0</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>$X_2$</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>-1</td>
<td>2</td>
</tr>
<tr>
<td>$X_3$</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>-1</td>
<td>-1</td>
</tr>
</tbody>
</table>

If $\gamma_1 > (\sqrt{33} - 1)/2$, then $F(-1 + \gamma_1) > 9$ and $x \neq -1 + \gamma_1$; also, since $\gamma_2 > \gamma_1$, we see that $x$ cannot be given by any of the remaining possibilities for $X_1, X_2, X_3$ in Table 4.

If $\gamma_1 < (\sqrt{33} - 1)/2$, then $F(-1 + \gamma_1) < 9$ and $0 < -1 + \gamma_1 < 3$; thus, $x$ could be $-1 + \gamma_1$. Since $-1 + \gamma_1 < 1 + \gamma_2 < \gamma_1 + \gamma_2$ and $-1 + \gamma_1 < -\gamma_1 + 2\gamma_2 < -1 + 2\gamma_2$, we see that $x \neq 1 + \gamma_2, \gamma_1 + \gamma_2, -\gamma_1 + 2\gamma_2$ or $-1 + 2\gamma_2$. Also, if $F(2\gamma_1 - \gamma_2) < 9$ or $F(2 - \gamma_2) < 9$, then $y_2 < \sqrt{6} - 1$. If this is so, then $\gamma_1 + \gamma_2 < 3$ and $-1 + \gamma_1 < 2 - \gamma_2 < 2\gamma_1 - \gamma_2$. Thus, we can only have $\gamma = -1 + \gamma_1$ when $\gamma_1 < (\sqrt{33} - 1)/2$.

As an example, we mention that if $D = 22$ and $\alpha = 196 + 70\delta + 25\bar{\delta}$, then $N(\alpha) = 36$ and $36 \mid S$. We find here that $\tau = 2, d_1 = d_4 = d_5 = d_6 = 1, d_3 = 11, d_2 = 2$. Also, $\lambda^2 = 3^2 \min\{4, 11, 2.11^2\} = 36, \beta = \alpha, m = 1, n = 2, \gamma_1 = \sqrt{22} /2 \simeq 1.40, \gamma_2 = \sqrt{484} /2 \simeq 3.93, am_2n = 44 \equiv -1 \pmod{3}, bm_1n = 2 \equiv -1 \pmod{3}$. Since $\gamma_1 < 2$, we have the result that $B \simeq \beta$ cannot be a relative minimum of $\mathbb{R}_1$. Further, $2 - \gamma_1 < 1 + \gamma_1 < \gamma_2 - \gamma_1$ and $F(2 - \gamma_1) < 9$; hence, $x = 2 - \gamma_1$. If $\theta = 3 \cdot 4 \cdot (2 - \gamma_1)\beta/n(\beta)$, then $\theta = 39 + 14\delta + 5\bar{\delta}$ and $\Theta (\simeq \theta)$ is a relative minimum of $\mathbb{R}_1$.

5. The Main Results. Results for the pure cubic case which are analogous to (1.2) in the quadratic case will be presented in Theorem 5.4; however, we must first prove
Theorem 5.1. Let \( \alpha \in \mathbb{Z}[8] \) and \( N(\alpha) \mid S \). Put \( N(\alpha) = 3d_1d_4d_2d_3^2 \), where \( a = d_1d_2d_3 \), \( b = d_4d_5d_6 \) and let \( \lambda^2/3' = m_1m_2n^2 = \min \{ d_1d_4d_2d_3^2, d_5d_6d_2d_3^2, d_2d_6d_4d_3^2 \} \), where \( m_1 \mid a, m_2 \mid b \). If \( \gamma_1 = \min \{ \delta/m_1n, \delta/m_1n \} \) and \( \gamma_2 = \max \{ \delta/m_1n, \delta/m_1n \} \), then \( B (\approx \beta = \lambda \beta / N(\alpha)^{1/3}) \) is a relative minimum of \( R_1 \) if

(i) \( D \equiv \pm 1 \pmod{9} \) and \( \tau = 0 \),
(ii) \( D \equiv \pm 1 \pmod{9} \) and \( \gamma_2 > \sqrt{6} \),
(iii) \( D \equiv \pm 1 \pmod{9} \), \( \tau = 1 \), and \( \gamma_2 > \sqrt{6} \),
(iv) \( D \equiv \pm 1 \pmod{9} \), \( \tau = 2 \), and \( \gamma_1 > (\sqrt{33} - 1)/2 \).

Proof. We saw in Section 3 that (i) is true. If \( B \) is not a relative minimum of \( R_1 \), there must exist a \( \chi \) as described in Theorem 3.4. It is a simple matter to verify that if \( \gamma_1 > 1 \), we must have

\[-1 - \gamma_1 + \sqrt{36 - 3(\gamma_1 - 1)^2} < 4, \quad 1 - \gamma_1 + \sqrt{36 - 3(\gamma_1 + 1)^2} < 2\sqrt{6}, \]
\[-1 + \gamma_1 + \sqrt{36 - 3(\gamma_1 + 1)^2} < 2\sqrt{6}.\]

Thus, in cases (ii) and (iii) above, we see, by Lemma 4.2, that we cannot have a \( \chi \) value as specified by Theorem 3.4. Hence \( B \) must be a relative minimum of \( R_1 \).

If \( \gamma_1 > (\sqrt{33} - 1)/2 \), we have \(-1 + \gamma_1 + \gamma_2 > 3 \). If \( F(\chi) < \theta \) and \( \chi = 1 + \gamma_1 - \gamma_2 \) or \( 1 - \gamma_1 + \gamma_2 \), then \( \gamma_1 < \sqrt{3} \) by (4.1). Thus, in case (iv), we cannot have \( X_1 \equiv am_2nX_2 \equiv bm_1nX_3 \pmod{3} \). But, if it is not true that \( X_1 \equiv am_2nX_2 \equiv bm_1nX_3 \pmod{3} \), we see, by Lemma 4.3, that we cannot have a \( \chi \) value satisfying the properties specified by Theorem 3.4. It follows that if \( \tau = 2 \) and \( \gamma_1 > (\sqrt{33} - 1)/2 \), then \( B \) is a relative minimum of \( R_1 \). \( \square \)

It should be mentioned here that conditions (ii), (iii), and (iv) of Theorem 5.4 are only sufficient conditions for \( B \) to be a relative minimum of \( R_1 \). In any individual case one should consult the more detailed results of Lemmas 4.2 and 4.3.

We will now attempt to describe when we have \( \epsilon_0 = \theta_k^2 / N(\Theta_k) \), where \( \Theta_k (\approx \theta_k) \) is a member of the chain (3.1) of relative minima of \( R_1 \) with \( \Theta_1 = (1, 0, 1) \). In order to do this we require Theorem 5.3; however, we first prove

Lemma 5.2. If \( \Theta (\approx \theta > 0) \) is a relative minimum of \( R_1 \), then \( \Phi (\approx \phi = \epsilon_0^2 \theta, n \in \mathbb{Z}) \) is also a relative minimum of \( R_1 \).

Proof. If \( \Phi \) is not a relative minimum of \( R_1 \), there must exist a \( \gamma (> 0) \) such that \( \gamma \in \mathbb{Z}[\theta] \) and \( \gamma < \phi \) and \( \gamma'\gamma'' < \phi'\phi'' \). That is, \( \gamma < \epsilon_0^2 \theta \) and \( \gamma'\gamma'' < (\epsilon_0^2 \theta')^2 \). If we put \( \rho = \epsilon_0^2 \gamma \in \mathbb{Z}[\theta] \), we see that \( 0 < \rho < \theta \) and \( \rho^2 \rho'' < \theta'\theta'' \). This contradicts the given fact that \( \Theta \) is a relative minimum of \( R_1 \); thus, \( \Phi \) is a relative minimum of \( R_1 \). \( \square \)

Note that since \( N(\pm \epsilon_0^2 \theta) = \pm N(\theta) \), we can say that, if we have any relative minimum \( \Theta \) of \( R_1 \), \( \Theta \approx \theta \), then there exists a relative minimum \( \Phi (\approx \phi \) in the chain (3.1) of relative minima of \( R_1 \) such that \( N(\phi) = |N(\theta)| \).

The following theorem is an extension of Lemma 6 of [14].

Theorem 5.3. Suppose \( \psi (\approx \psi) \) and \( \phi (\approx \phi) \) are relative minima of \( R_1 \) such that \( N(\phi) \neq N(\psi), \ N(\phi), \ N(\psi) \neq 1, N(\phi) | S \) and \( N(\psi) | S \). If \( \Theta_k (\approx \theta_k) \) is the first element in the chain (3.1) of relative minima of \( R_1 \) with \( \Theta_1 = (1, 0, 1) \) such that \( N(\theta_k) | S \), then \( \epsilon_0 = \theta_k^2 / N(\theta_k) \).
Proof. Since \( N(\psi), N(\phi) \neq 1 \), we must have \( \varepsilon_0^{m_1} < \psi < \varepsilon_0^{m_1+1}, \varepsilon_0^{m_2} < \phi < \varepsilon_0^{m_2+1} \)
for some \( m_1, m_2 \in \mathbb{Z} \). Thus, if \( \psi^* = \varepsilon_0^{-m_1}\psi, \phi^* = \varepsilon_0^{-m_2}\phi \), then \( \psi^*, \phi^* \in \mathbb{Q}[\delta] \) and
\( 1 < \psi^* < \varepsilon_0, \phi^* < \varepsilon_0 \). By Lemma 5.2, \( \Theta^* (\approx \theta^*) \) and \( \Phi^* (\approx \phi^*) \) are relative
minima of \( \mathcal{R}_1 \); hence they must be in the chain (3.1). Further, there must exist a least \( \Theta_k (\approx \theta_k) \) in the chain (3.1) such that
\( N(\Theta_k) | S \) and \( 1 < \theta_k < \varepsilon_0 \). Now
\[
N\left( \frac{\theta_k^2}{N(\Theta_k)} \right) = N\left( \frac{\psi^*\psi^*}{N(\psi^*)} \right) = N\left( \frac{\phi^*\phi^*}{N(\phi^*)} \right) = 1;
\]
hence,
\[
\theta_k^2/N(\Theta_k) = \varepsilon_0^n, \quad \psi^3/N(\psi^*) = \varepsilon_0^n, \quad \phi^3/N(\phi^*) = \varepsilon_0^n,
\]
where \( n_1, n_2, n_3 \in \mathbb{Z} \). Since, \( \theta_k, \psi^*, \phi^* < \varepsilon_0 \), we see that \( n_i < 2 \) (i = 1, 2, 3). Also, \( \theta_k^2, \psi^*, \phi^*, \psi^*\phi^* < 1 \); thus, \( \theta_k^2/N(\Theta_k), \psi^3/N(\psi^*), \phi^3/N(\phi^*) > 1 \) and \( n_i > 1 \)
(i = 1, 2, 3).

Since \( N(\psi^*) \neq N(\phi^*) \), we may assume with no loss of generality that \( \psi^* < \phi^* \). Thus, since \( \Phi^* \) is a relative minimum of \( \mathcal{R}_1 \), we must have \( \psi^*\psi^*\phi^* > \phi^*\phi^*\phi^* \) and \( \psi^3/N(\psi^*) < \phi^3/N(\phi^*) \). It follows that \( \psi^3/N(\psi^*) = \varepsilon_0 \) and \( \phi^3/N(\phi^*) = \varepsilon_0^2 \). By
definition of \( \theta_k \), we must have \( \theta_k < \psi^* \). Since \( \theta_k^2/N(\Theta_k) < \psi^3/N(\psi^*) \) and
\( \theta_k^3/N(\Theta_k) \) cannot be less than \( \varepsilon_0 \), we see that \( \varepsilon_0 = \theta_k^2/N(\Theta_k) \). \( \square \)

We remark here that we have shown that there can be at most two elements \( \Theta_i \)
(\( \approx \theta_i \)) and \( \Theta_j \) in the chain (3.1) of relative minima of \( \mathcal{R}_1 \) such that
\( \theta_i, \theta_j < \varepsilon_0 \) and \( N(\Theta_i) | S \), \( N(\Theta_j) | S \).

If \( \Theta_k \approx \theta_k \) is the least element in the chain (3.1) of relative minima of \( \mathcal{R}_1 \) with \( \Theta_1 = (1, 0, 0) \) such that \( \theta_i, \theta_j < \varepsilon_0 \) and \( N(\Theta_i) | S \), then it can occur that \( \varepsilon_0 \neq \theta_k^3/N(\Theta_k) \). In these
cases we get \( \varepsilon_0^2 = \theta_k^2/N(\Theta_k) \). For example, this occurs when \( D = 14, 52, 77, 92, \) etc.

However, we are able to prove

**Theorem 5.4.** Let \( \Theta_k \approx \theta_k \) be the least relative minimum in the chain (3.1) of
relative minima of \( \mathcal{R}_1 \) with \( \Theta_1 = (1, 0, 0) \) such that \( N(\Theta_k) \neq 1 \). If
\( N(\Theta_k) = 3^a d_1 d_2 d_3 d_4 d_5 \), where \( a = d_1 d_2 d_3, b = d_4 d_5 d_6 \), let
\[
m_1, m_2 n^2 = \min\{d_2 d_5 d_2 d_4, d_3 d_4 d_2 d_6, d_1 d_6 d_3 d_2\},
\]
where \( m_1 | a \) and \( m_2 | b \). Put \( \gamma_1 = \min\{\delta/m_2 n, \bar{\delta}/m_1 n\} \), \( \gamma_2 = \max\{\delta/m_2 n, \bar{\delta}/m_1 n\} \). We have \( \varepsilon_0 = \theta_k^2/N(\Theta_k) \) if any of the following is true:
(i) \( D \equiv \pm 1 (\mod 9) \), \( \tau = 0 \),
(ii) \( D \equiv \pm 1 (\mod 9) \), \( \gamma_2 > \sqrt{6} \),
(iii) \( D \equiv \pm 1 (\mod 9) \), \( \tau = 2, \gamma_2 > \sqrt{6} \),
(iv) \( D \equiv \pm 1 (\mod 9) \), \( \tau = 1, \gamma_1 > (\sqrt{33} - 1)/2 \).

**Proof.** Put \( \alpha = \theta_k^2/d_1 d_2 \) when \( \tau = 0 \) and put \( \alpha = \theta_k^2/3 d_2 d_5 \) when \( \tau = 2 \). We
have \( \alpha \in \mathbb{Q}[\delta], N(\alpha) = 3^a d_1 d_2 d_3 d_4 d_5 \), where
\[
\nu = \begin{cases} 
0 & \text{when } \tau = 0, \\
1 & \text{when } \tau = 2, \\
2 & \text{when } \tau = 1,
\end{cases}
\]
and \( N(\alpha) \neq S \). If we define \( \beta \) as in Lemma 2.4, we have \( N(\beta) \neq S \) and we see, by
Theorem 5.1, that \( B \approx \beta \) must be a relative minimum of \( \mathcal{R}_1 \). If \( \tau > 0 \), we have
\( (3, ab) = 1 \) and therefore \( N(\beta) \neq N(\Theta_k) \), \( N(\beta) \neq 1 \). Suppose \( \tau = 0 \). Since \( N(\beta) = m_1 m_2 n^2 \), \( a \) and \( b \) are square free and
\( N(\Theta_k) \neq 1 \), we see that, if \( N(\beta) = N(\Theta_k) \) or \( N(\beta) = 1 \), we must have \( N(\Theta_k) = a^2 b \) or \( a^2 b \). By Lemma 3.3, this is not possible;
thus, \( N(\theta_k) \neq N(\beta), N(\beta) \neq 1, N(\theta_k) \neq 1 \) and \( N(\beta) | S, N(\theta_k) | S \). By Theorem 5.3, we get \( \epsilon_0 = \Theta_k^3 \). \( \square \)

6. Some Special Results. It has already been noted in [14] that, when \( ab \) is a prime or the triple of a prime, Voronoi’s algorithm can be used to find values of \( \alpha \in \mathbb{Q}[\delta] \) such that \( N(\alpha) \) \( \square \). We show in this section how the more general results of Sections 4 and 5 can be used to find such values of \( \alpha \) when \( ab \) is the product of two distinct primes. In these cases we also characterize some values of \( \alpha \) and \( b \) for which \( \epsilon_0 = \Theta_k^3 \), where \( \Theta_k (\approx \theta_k) \) is the least relative minimum of \( \mathfrak{R}_1 \) such that \( \theta_k > 1 \) and \( N(\theta_k) | S \). In this section we use the symbols \( p \) and \( q \) to denote distinct primes in \( \mathbb{Z} \).

**Theorem 6.1.** Let \( D = pq \equiv \pm 1 \) (mod 9). If \( D > 10 \) and \( N(\alpha) = p \) is solvable for \( \alpha \in \mathbb{Q} \), there exists a relative minimum \( B (\approx \beta) \) in \( \mathcal{R}_1 \) such that \( N(\beta) \) \( \square \). Further, if \( \Theta_k (\approx \theta_k) \) is the least relative minimum in the chain (3.1) with \( \Theta_1 = (1, 0, 1) \) such that \( N(\Theta_k) | S \), then \( \epsilon_0 = \Theta_k^3 \).

**Proof.** Since \( N(\alpha) = p \), we have \( d_1 = p, d_2 = 1, d_3 = q, d_4 = d_5 = d_6 = 1, \tau = 0 \) and

\[
m_1 m_2 n_2 = \lambda^3 = \min \{p, p^2, q^2\} = \min \{p, q^3\}.
\]

If \( p < q^2 \), then \( \lambda^3 = p, m_1 = m_2 = 1, n = q, \gamma_2 = \max \left\{ \frac{3}{\sqrt{pq}}, \frac{3}{p^2 q^2} \right\} \). Supposing \( pq > 10 \), we see that \( \frac{3}{\sqrt{pq}} > \sqrt{6} \) and \( \gamma_2 > \sqrt{6} \). Thus, by Theorem 5.1, \( B_1 \approx \beta_1 = \alpha \) is a relative minimum of \( \mathfrak{R}_1 \).

If \( p > q^2 \), we have \( \lambda^3 = q^2, m_1 = m_2 = 1, n = q, \gamma_2 = \max \left\{ \frac{3}{\sqrt{pq}/q}, \frac{3}{p^2 q^2} / q \right\} 
= \frac{3}{p^2 q^2} / q \). Since \( p > q^2 \), we have \( p^2 > q^4 > (\sqrt{6})^3 q \) when \( q > \sqrt{6} \). If \( q = 2 \), then, since \( pq > 10 \), we must have \( q > 13 \) and \( p^2 > 2(\sqrt{6})^3 = (\sqrt{6})^3 q \).

Thus, we have \( \gamma_2 > \sqrt{6} \), and \( B_2 (\approx \beta_2 = \lambda \alpha / p^{1/3}) \) is a relative minimum of \( \mathfrak{R}_1 \) and \( N(\beta_2) | S \).

We next consider \( \alpha^2 \). We have \( N(\alpha^2) = p^2 \) and \( d_1 = 1, d_2 = p, d_3 = q, d_4 = d_5 = d_6 = 1, m_1 m_2 n_2 = \lambda^3 = \min \{p^2, q, q^2 p\} = \min \{p^2, q\} \). If \( p^2 < q \), then \( \lambda^3 = p^2, m_1 = m_2 = 1, n = p \) and \( \gamma_2 = \max \left\{ \frac{3}{\sqrt{pq}/p}, \frac{3}{p^2 q^2} / p \right\} \). We have already seen that \( \frac{3}{p^2 q^2} / p > \sqrt{6} \); hence, \( B_3 (\approx \beta_3 = \alpha^2) \) is a relative minimum of \( \mathfrak{R}_1 \).

If \( p^2 > q \), then \( \lambda^3 = q, m_1 = q, m_2 = 1, n = 1, \gamma_2 = \max \left\{ \frac{3}{\sqrt{pq}/q}, \frac{3}{\sqrt{pq}} / q \right\} > \sqrt{6} \);

thus, \( B_4 (\approx \beta_4 = \frac{3}{\sqrt{pq}} \alpha / p) \) is a relative minimum of \( \mathfrak{R}_1 \).

We have now shown that one of \( B_1 \) or \( B_2 \) and one of \( B_3 \) or \( B_4 \) are relative minima of \( \mathfrak{R}_1 \). Further, \( N(\beta_1) = p, N(\beta_2) = q^2, N(\beta_3) = p^2, N(\beta_4) = q \); hence, no two of these norms are equal and none of them is 1. The theorem now follows from Theorem 5.3. \( \square \)

We also have

**Theorem 6.2.** Let \( D = pq^2 \equiv \pm 1 \) (mod 9). If \( N(\alpha) = p \) is solvable for \( \alpha \in \mathbb{Q}[\delta] \), there exists a relative minimum \( B (\approx \beta) \) in \( \mathfrak{R}_1 \) such that \( N(\beta) \) \( \square \). Further, if \( \Theta_k (\approx \theta_k) \) is the least relative minimum in the chain (3.1) with \( \Theta_1 = (1, 0, 1) \) such that \( N(\theta_k) | S \), then \( \epsilon_0 = \Theta_k^3 \).
Proof. Similar to the proof of Theorem 6.1. □

In [2] it was shown that if $D$ has no prime factor $\equiv 1 \pmod{3}$ and $D$ has at least one prime factor $\equiv 2$ or $5 \pmod{9}$, then there exists a principal factor of $\Delta$. Now if $D = pq \equiv \pm 1 \pmod{9}$, the only possible principal factor set is

$$\{ p, p^2q, q^2, p, pq^2 \},$$

and if $D = pq^2 \equiv \pm 1 \pmod{9}$, the only possible principal factor set is

$$\{ p, q, p^2q^2, p^2, q^2, pq \};$$

thus, if $D = pq$ with $p \equiv 2, q \equiv 5 \pmod{9}$ or if $D = pq^2$ with $p \equiv q \equiv 2$ or $5 \pmod{9}$, we have a solution $a \in \mathbb{O}[\delta]$ such that $N(a) = p$.

Those fields $\mathbb{O}[\delta]$ for which 3 is not a divisor of the class number of $\mathbb{O}(\delta)$ are given by (Honda [7])

(i) $D = 3$,
(ii) $D = p, p \equiv -1 \pmod{3}$,
(iii) $D = 3p$ or $9p$, where $p \equiv 2, 5 \pmod{9}$,
(iv) $D = pq$, where $p \equiv 2, q \equiv 5 \pmod{9}$,
(v) $D = pq^2$, where $p \equiv q \equiv 2, 5 \pmod{9}$.

If $D \neq p \equiv 8 \pmod{9}$, we know from [14] that in cases (ii) and (iii) we have $\varepsilon_0 = \theta_k^2 / N(\theta_k)$, where $\Theta_k \approx \theta_k$ is the least element of the chain (3.1) with $\Theta_1 = (1, 0, 1)$ such that $N(\theta_k) = 3$ or 9. We also know that such a $\Theta_k$ will always exist in these cases. We have now seen by Theorems 6.1 and 6.2 that if $D$ is given by cases (iv) or (v), there always exists a least $\Theta_k \approx \theta_k$ in the chain (3.1) such that $N(\theta_k) | S$ and for this $\theta_k$ we have $\varepsilon_0 = \theta_k^2 / N(\theta_k)$. This observation allows us to calculate the regulator of $\mathbb{O}(\delta)$ (see [14]) about 3 times faster than it would take by using the method of going through the entire set of relative minima of (3.1) until $\Theta_n \approx \theta_n$ was found such that $N(\theta_n) = 1$. Once the regulator has been determined it is not very difficult to calculate the class number $h(D)$ of $\mathbb{O}(\delta)$ (see Barrucand, Williams, and Baniuk [3]; the Euler product method was used here). In Table 5 below, we present the frequency $f(h)$ of each class number $h = h(D)$ for all 16843 $\mathbb{O}(\sqrt{D})$ such that $3 \mid h(D)$, $D = ab^2 < 2 \times 10^5$, and $a > b$. In the third column of this table, we give the least $D$ such that $\mathbb{O}(\sqrt{D})$ has the $h$ in the first column as its class number.

<table>
<thead>
<tr>
<th>h</th>
<th>f(h)</th>
<th>D</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>8230</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>4136</td>
<td>11</td>
</tr>
<tr>
<td>4</td>
<td>1700</td>
<td>113</td>
</tr>
<tr>
<td>5</td>
<td>507</td>
<td>263</td>
</tr>
<tr>
<td>7</td>
<td>275</td>
<td>235</td>
</tr>
<tr>
<td>8</td>
<td>587</td>
<td>141</td>
</tr>
<tr>
<td>10</td>
<td>224</td>
<td>303</td>
</tr>
<tr>
<td>11</td>
<td>79</td>
<td>2348</td>
</tr>
<tr>
<td>13</td>
<td>47</td>
<td>1049</td>
</tr>
<tr>
<td>14</td>
<td>98</td>
<td>514</td>
</tr>
<tr>
<td>16</td>
<td>185</td>
<td>681</td>
</tr>
</tbody>
</table>

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
Table 5 (continued)

<table>
<thead>
<tr>
<th>h</th>
<th>f(h)</th>
<th>D</th>
</tr>
</thead>
<tbody>
<tr>
<td>17</td>
<td>27</td>
<td>8511</td>
</tr>
<tr>
<td>19</td>
<td>32</td>
<td>667</td>
</tr>
<tr>
<td>20</td>
<td>106</td>
<td>761</td>
</tr>
<tr>
<td>22</td>
<td>42</td>
<td>281</td>
</tr>
<tr>
<td>23</td>
<td>16</td>
<td>21241</td>
</tr>
<tr>
<td>25</td>
<td>14</td>
<td>10181</td>
</tr>
<tr>
<td>26</td>
<td>23</td>
<td>3403</td>
</tr>
<tr>
<td>28</td>
<td>59</td>
<td>509</td>
</tr>
<tr>
<td>29</td>
<td>9</td>
<td>12079</td>
</tr>
<tr>
<td>31</td>
<td>5</td>
<td>16553</td>
</tr>
<tr>
<td>32</td>
<td>37</td>
<td>2399</td>
</tr>
<tr>
<td>34</td>
<td>18</td>
<td>1719</td>
</tr>
<tr>
<td>35</td>
<td>9</td>
<td>37207</td>
</tr>
<tr>
<td>37</td>
<td>7</td>
<td>5545</td>
</tr>
<tr>
<td>38</td>
<td>13</td>
<td>12813</td>
</tr>
<tr>
<td>40</td>
<td>27</td>
<td>2733</td>
</tr>
<tr>
<td>41</td>
<td>7</td>
<td>6659</td>
</tr>
<tr>
<td>43</td>
<td>6</td>
<td>32847</td>
</tr>
<tr>
<td>44</td>
<td>16</td>
<td>4817</td>
</tr>
<tr>
<td>46</td>
<td>9</td>
<td>59975</td>
</tr>
<tr>
<td>47</td>
<td>1</td>
<td>198377</td>
</tr>
<tr>
<td>49</td>
<td>5</td>
<td>8171</td>
</tr>
<tr>
<td>50</td>
<td>14</td>
<td>14372</td>
</tr>
<tr>
<td>52</td>
<td>15</td>
<td>4793</td>
</tr>
<tr>
<td>53</td>
<td>4</td>
<td>38373</td>
</tr>
<tr>
<td>55</td>
<td>3</td>
<td>147257</td>
</tr>
<tr>
<td>56</td>
<td>14</td>
<td>857</td>
</tr>
<tr>
<td>58</td>
<td>7</td>
<td>6814</td>
</tr>
<tr>
<td>59</td>
<td>1</td>
<td>95905</td>
</tr>
<tr>
<td>61</td>
<td>2</td>
<td>36161</td>
</tr>
<tr>
<td>62</td>
<td>3</td>
<td>42407</td>
</tr>
<tr>
<td>64</td>
<td>12</td>
<td>9749</td>
</tr>
<tr>
<td>65</td>
<td>2</td>
<td>88169</td>
</tr>
<tr>
<td>67</td>
<td>4</td>
<td>14073</td>
</tr>
<tr>
<td>68</td>
<td>4</td>
<td>9521</td>
</tr>
<tr>
<td>70</td>
<td>4</td>
<td>3467</td>
</tr>
<tr>
<td>71</td>
<td>3</td>
<td>3539</td>
</tr>
<tr>
<td>73</td>
<td>2</td>
<td>133709</td>
</tr>
<tr>
<td>74</td>
<td>5</td>
<td>3581</td>
</tr>
<tr>
<td>76</td>
<td>7</td>
<td>23469</td>
</tr>
<tr>
<td>77</td>
<td>2</td>
<td>134189</td>
</tr>
<tr>
<td>$h$</td>
<td>$f(h)$</td>
<td>$D$</td>
</tr>
<tr>
<td>-----</td>
<td>-------</td>
<td>------</td>
</tr>
<tr>
<td>79</td>
<td>2</td>
<td>61741</td>
</tr>
<tr>
<td>80</td>
<td>10</td>
<td>4799</td>
</tr>
<tr>
<td>83</td>
<td>1</td>
<td>17362</td>
</tr>
<tr>
<td>85</td>
<td>3</td>
<td>10783</td>
</tr>
<tr>
<td>86</td>
<td>4</td>
<td>43403</td>
</tr>
<tr>
<td>88</td>
<td>2</td>
<td>132011</td>
</tr>
<tr>
<td>89</td>
<td>3</td>
<td>64882</td>
</tr>
<tr>
<td>92</td>
<td>2</td>
<td>15131</td>
</tr>
<tr>
<td>95</td>
<td>4</td>
<td>15797</td>
</tr>
<tr>
<td>97</td>
<td>1</td>
<td>131302</td>
</tr>
<tr>
<td>98</td>
<td>2</td>
<td>130859</td>
</tr>
<tr>
<td>100</td>
<td>6</td>
<td>31547</td>
</tr>
<tr>
<td>101</td>
<td>3</td>
<td>48767</td>
</tr>
<tr>
<td>104</td>
<td>7</td>
<td>11549</td>
</tr>
<tr>
<td>107</td>
<td>1</td>
<td>180298</td>
</tr>
<tr>
<td>110</td>
<td>5</td>
<td>17333</td>
</tr>
<tr>
<td>112</td>
<td>5</td>
<td>11665</td>
</tr>
<tr>
<td>115</td>
<td>1</td>
<td>99973</td>
</tr>
<tr>
<td>118</td>
<td>2</td>
<td>47093</td>
</tr>
<tr>
<td>119</td>
<td>1</td>
<td>197003</td>
</tr>
<tr>
<td>121</td>
<td>1</td>
<td>57543</td>
</tr>
<tr>
<td>122</td>
<td>1</td>
<td>160345</td>
</tr>
<tr>
<td>124</td>
<td>2</td>
<td>35349</td>
</tr>
<tr>
<td>125</td>
<td>1</td>
<td>189575</td>
</tr>
<tr>
<td>127</td>
<td>2</td>
<td>2741</td>
</tr>
<tr>
<td>128</td>
<td>4</td>
<td>5987</td>
</tr>
<tr>
<td>130</td>
<td>1</td>
<td>103429</td>
</tr>
<tr>
<td>136</td>
<td>4</td>
<td>3209</td>
</tr>
<tr>
<td>139</td>
<td>1</td>
<td>143326</td>
</tr>
<tr>
<td>140</td>
<td>4</td>
<td>36263</td>
</tr>
<tr>
<td>148</td>
<td>3</td>
<td>60149</td>
</tr>
<tr>
<td>149</td>
<td>2</td>
<td>52737</td>
</tr>
<tr>
<td>152</td>
<td>2</td>
<td>118113</td>
</tr>
<tr>
<td>154</td>
<td>2</td>
<td>9041</td>
</tr>
<tr>
<td>155</td>
<td>1</td>
<td>36107</td>
</tr>
<tr>
<td>158</td>
<td>1</td>
<td>66813</td>
</tr>
<tr>
<td>160</td>
<td>1</td>
<td>168092</td>
</tr>
<tr>
<td>161</td>
<td>3</td>
<td>95001</td>
</tr>
<tr>
<td>170</td>
<td>1</td>
<td>45321</td>
</tr>
<tr>
<td>173</td>
<td>1</td>
<td>139109</td>
</tr>
<tr>
<td>175</td>
<td>2</td>
<td>5711</td>
</tr>
</tbody>
</table>
**Table 5 (continued)**

<table>
<thead>
<tr>
<th>h</th>
<th>f(h)</th>
<th>D</th>
</tr>
</thead>
<tbody>
<tr>
<td>181</td>
<td>1</td>
<td>12251</td>
</tr>
<tr>
<td>182</td>
<td>1</td>
<td>115751</td>
</tr>
<tr>
<td>188</td>
<td>1</td>
<td>119921</td>
</tr>
<tr>
<td>190</td>
<td>1</td>
<td>193247</td>
</tr>
<tr>
<td>191</td>
<td>1</td>
<td>47639</td>
</tr>
<tr>
<td>193</td>
<td>2</td>
<td>66783</td>
</tr>
<tr>
<td>196</td>
<td>1</td>
<td>10522</td>
</tr>
<tr>
<td>200</td>
<td>4</td>
<td>12197</td>
</tr>
<tr>
<td>202</td>
<td>1</td>
<td>158867</td>
</tr>
<tr>
<td>214</td>
<td>3</td>
<td>16823</td>
</tr>
<tr>
<td>224</td>
<td>1</td>
<td>103627</td>
</tr>
<tr>
<td>230</td>
<td>1</td>
<td>4451</td>
</tr>
<tr>
<td>232</td>
<td>2</td>
<td>84093</td>
</tr>
<tr>
<td>248</td>
<td>1</td>
<td>194811</td>
</tr>
<tr>
<td>254</td>
<td>1</td>
<td>8002</td>
</tr>
<tr>
<td>259</td>
<td>1</td>
<td>148763</td>
</tr>
<tr>
<td>262</td>
<td>1</td>
<td>28979</td>
</tr>
<tr>
<td>263</td>
<td>1</td>
<td>164737</td>
</tr>
<tr>
<td>268</td>
<td>1</td>
<td>112757</td>
</tr>
<tr>
<td>280</td>
<td>1</td>
<td>35969</td>
</tr>
<tr>
<td>284</td>
<td>1</td>
<td>25913</td>
</tr>
<tr>
<td>296</td>
<td>1</td>
<td>26601</td>
</tr>
<tr>
<td>305</td>
<td>1</td>
<td>39821</td>
</tr>
<tr>
<td>316</td>
<td>2</td>
<td>39106</td>
</tr>
<tr>
<td>319</td>
<td>1</td>
<td>171629</td>
</tr>
<tr>
<td>329</td>
<td>1</td>
<td>183347</td>
</tr>
<tr>
<td>334</td>
<td>2</td>
<td>87257</td>
</tr>
<tr>
<td>340</td>
<td>1</td>
<td>18257</td>
</tr>
<tr>
<td>352</td>
<td>1</td>
<td>51549</td>
</tr>
<tr>
<td>358</td>
<td>1</td>
<td>27329</td>
</tr>
<tr>
<td>370</td>
<td>1</td>
<td>73779</td>
</tr>
<tr>
<td>389</td>
<td>1</td>
<td>24023</td>
</tr>
<tr>
<td>392</td>
<td>1</td>
<td>67157</td>
</tr>
<tr>
<td>400</td>
<td>1</td>
<td>53434</td>
</tr>
<tr>
<td>421</td>
<td>1</td>
<td>47303</td>
</tr>
<tr>
<td>431</td>
<td>1</td>
<td>114221</td>
</tr>
<tr>
<td>433</td>
<td>1</td>
<td>69539</td>
</tr>
<tr>
<td>490</td>
<td>1</td>
<td>169007</td>
</tr>
<tr>
<td>559</td>
<td>1</td>
<td>114833</td>
</tr>
<tr>
<td>581</td>
<td>1</td>
<td>192754</td>
</tr>
<tr>
<td>583</td>
<td>1</td>
<td>63766</td>
</tr>
</tbody>
</table>
If \( D = pq \equiv \pm 1 \pmod{9} \) (\( p, q \neq 3 \)), there are four possible principal factor sets. These are

\[
\begin{align*}
\{3, 3pq, 3p^2q^2, 9, 9pq, 9p^2q^2\}, \\
\{p, p^2q, q^2, p^2, q, q^2p\}, \\
\{3p, 3p^2q, 3q^2, 9p^2, 9q, 9q^2p\}, \\
\{3q, 3q^2p, 3p^2, 9q^2, 9p^2q, 9p\}.
\end{align*}
\]

If one of \( p \) or \( q \) is \( \equiv 2 \) or \( 5 \pmod{9} \) and the other is \( \equiv -1 \pmod{3} \), we know that there must exist a principal factor of \( \Delta \). If this principal factor is in either of the first two sets, then it is a simple matter to show that \( e_0 = 9k/N(\theta_k) \), where \( \theta_k \) has the usual meaning assigned to it in this section. Also, such a \( \theta_k \) must exist. We now describe what happens when the principal factor is in either of the other two sets.

**Theorem 6.3.** If \( D \) is given as above and \( N(\alpha) = 3p \) (3q) is solvable for some \( \alpha \in \mathcal{Z}[\delta] \), there exists a relative minimum \( B \) (\( \approx \beta \)) of \( \mathcal{R}_1 \) such that \( N(\beta) \mid S \). Further, if \( q > 8p^2 \) and \( \Theta_k \) (\( \approx \theta_k \)) is the first element of the chain (3.1) such that \( N(\theta_k) \mid S \), then \( e_0 = \frac{\theta_k^3}{N(\theta_k)} \).
Proof. The proof of the first part of this theorem is similar to that of Theorem 6.1. In fact, we show that one of \( B_1 \) \((\approx \alpha)\) or \( B_2 \) \((\approx \beta_2 = 3\sqrt{D^2} \alpha/N(\alpha))\) must be a relative minimum of \( \Omega_1 \).

If we have \( N(\alpha^2) = 9p^2 \), then \( d_1 = 1, d_2 = p, d_3 = q, d_4 = d_5 = d_6 = 1, \tau = 2, m_1m_2n_2 = \min(p^2, q, q^2p) = p^2 \) when \( q > 8p^2 \). Hence \( m_1 = m_2 = 1, n = p \), and \( am_2n \equiv bm_1n \equiv -1 \) \((\mod 3)\). We also have \( \gamma_1 = \min\left(3\sqrt[pq]{p}/p, 3p^2q^2/p\right) = 3\sqrt[pq]{p}/p > 2 \). By Lemma 4.3, we see that \( B_3 (\approx \alpha^2) \) is a relative minimum of \( \Omega_1 \).

If we have \( N(\alpha^2) = 9q^2 \), then \( d_1 = 1, d_2 = q, d_3 = p, d_4 = d_5 = d_6 = 1, \tau = 2, m_1m_2n_2 = \min(q^2, p, p^2q) = p^2 \). Also, \( \gamma_1 = \min\left(3\sqrt[pq]{q}, 3p^2q^2/p\right) \). Since

\[
\sqrt[pq]{pq} > 2p > \left(\sqrt[3]{33} - 1\right)/2 \quad \text{and} \quad q^2 > 64p^4 > \left(\left(\sqrt[3]{33} - 1\right)/2\right)^3 p,
\]
we have \( \gamma_1 > \left(\sqrt[3]{33} - 1\right)/2, \) and \( B_4 (\approx \beta_4 = a^2\sqrt[pq]{pq}/q) \) is a relative minimum of \( \Omega_1 \). Since \( N(\beta_1) = 3p \left(3q\right), N(\beta_2) = 3q^2 \left(3p^2\right), N(\beta_3) = 9p^2, N(\beta_4) = 9p \) are all distinct, the theorem follows from Theorem 5.3. \( \square \)

Thus, we have seen that if \( D = pq \), where \( p \equiv q \equiv -1 \) \((\mod 3)\), one of \( p, q \equiv 2, 5 \) \((\mod 9)\) and \( q > 8p^2 \), then there exists \( \theta_k \) as described above and \( \theta_k^3/N(\theta_k) = e_0 \). We remark here that restriction \( q > 8p^2 \) can be replaced by the restriction \( q > 8p^2 - 3 \). This is simply because \( q \) must be a prime and \( q \equiv -1 \) \((\mod 3)\). This inequality is actually sharp for \( p = 2 \) and \( p = 5 \). For, when \( D = 2 \cdot 29 \) or \( 5 \cdot 197 \), we find that \( \theta_k^3/N(\theta_k) = e_0^2 \).

We can also show that if \( D = pq^2 \), where \( p > \left(\left(\sqrt[3]{33} - 1\right)/2\right)^2q, p \equiv q \equiv -1 \) \((\mod 3)\) and one of \( p, q \) is congruent to 2 or 5 \((\mod 9)\), then there exists a least \( \Theta_k \) \((\approx \theta_k)\) of the chain (3.1) such that \( N(\theta_k) | S \). Also, \( e_0 = \theta_k^3/N(\theta_k) \) here.

We conclude by pointing out that, although the ordinary continued fraction algorithm for \( \sqrt{d} \) always finds a principal factor (as a norm of \( A_{j-1} + \sqrt{d} B_{j-1} \)) whenever one exists, Voronoi's algorithm does not always do this. For example, when \( D = 850 \), we find that \( N(\alpha) = 150 \) and \( 150 | S \) for \( \alpha = 180 + 195 + 105; \) however, the only \( \Theta_r \) in the chain (3.1) such that \( N(\theta_r) | S \) has \( N(\theta_r) = 1 \).

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


