MATHEMATICS OF COMPUTATION
VOLUME 38, NUMBER 157
JANUARY 1982

Determination of Principal Factors in $\mathbb{Q}(\sqrt{D})$ and $\mathbb{Q}(\sqrt[3]{D})$

By H. C. Williams

Abstract. Let $l = 2$ or 3 and let D be a positive l-power-free integer. Also, let R be the product of all the rational primes which completely ramify in $K = \mathbb{Q}(D^{1/l})$. The integer d is a principal factor of the discriminant of K if $d = N(\alpha)$, where α is an algebraic integer of K and $d \mid R^{l-1}$. In this paper algorithms for finding these principal factors are described. Special attention is given to the case of $l = 3$, where it is shown that Voronoi's continued fraction algorithm can be used to find principal factors. Some results of a computer search for principal factors for all $\mathbb{Q}(\sqrt[3]{D})$ with $2 < D < 15000$ are also presented.

1. Introduction. Let $l = 2$ or 3, D be a positive l-power-free integer and, $K = \mathbb{Q}(D^{1/l})$ be the algebraic number field formed by adjoining $D^{1/l}$ to the rationals $\mathbb{Q}$. In this paper our main concern will be with the case of $l = 3$, but we will also briefly discuss the case where $l = 2$.

Denote by $\mathbb{Q}[D^{1/l}]$ the ring of algebraic integers in K and let $\mathbb{Z}$ be the set of rational integers. We say that any algebraic integer of K is *primitive* if it is not divisible by a rational integer greater than 1. We denote by $N(\alpha)$ the norm (product of α and its conjugates) of any $\alpha \in K$. Let ε (> 1) be the fundamental unit of K, and let R be the product of totally ramified primes in K.

When $l = 2$, we have

$$R = \begin{cases} D, & D \equiv 1, 2 \pmod 4, \\ 2D, & D \equiv 3 \pmod 4. \end{cases}$$

We also have the following

THEOREM [1]. *If $N(\varepsilon) = 1$, there exist two primitive $\pm\alpha_1, \pm\alpha_2 \in \mathbb{Q}[\sqrt{D}]$ such that*

$$\varepsilon = \frac{\alpha_1^2}{|N(\alpha_1)|} = \frac{\alpha_2^2}{|N(\alpha_2)|}. \tag{1.1}$$

If we denote by α' the conjugate of α in K, then

$$\alpha_1\alpha_2' = \begin{cases} 2D^{1/2} & \text{when } D \equiv 3 \pmod 4 \text{ and } 2 \nmid N(\alpha_1), \\ D^{1/2} & \text{otherwise.} \end{cases} \tag{1.2}$$

Received March 10, 1981; revised June 22, 1981.
1980 *Mathematics Subject Classification.* Primary 12A25, 12A30, 12-04.
Key words and phrases. Principal factors, Voronoi's algorithm, Diophantine equations.

0025-5718/82/0000-0489/$04.50

Thus, we see that $N(\alpha_1)$ and $N(\alpha_2)$ are divisors of R. These integers are called *principal factors of the discriminant of* $\mathfrak{Q}(\sqrt{D})$, or more simply, principal factors for $\mathfrak{Q}(\sqrt{D})$.

If $N(\varepsilon) = -1$, then from (1.1) it is clear that no principal factors of K can exist. We can express some of these results in the following fashion. We have

$$\frac{\varepsilon'}{\varepsilon} = (-1)^i\gamma^2, \quad \gamma\,(=\varepsilon') \in K, \qquad 0 \leqslant i \leqslant 1. \tag{1.3}$$

If $i = 0$, we have principal factors in K; if $i = 1$, we do not have principal factors in K.

Note that the problem of existence of principal factors in $\mathfrak{Q}(\sqrt{D})$ is as difficult as the famous problem of whether or not there are integer solutions of the Pellian equation

$$x^2 - Dy^2 = -1. \tag{1.4}$$

Recently Morton [6] and Lagarias [7] have obtained some important results concerning this problem.

A simple method of determining these principal factors can be developed by using continued fractions. We let $\phi_0 = \phi \in K$ and let

$$\phi_0 = \langle q_0, q_1, q_2, \ldots, q_{n-1}, \phi_n\rangle \tag{1.5}$$

be the continued fraction expansion of ϕ_0. If $A_{-2} = 0$, $A_{-1} = 1$, $B_{-2} = 1$, $B_{-1} = 0$, and

$$\begin{cases} A_{k+1} = q_{k+1}A_k + A_{k-1}, \\ B_{k+1} = q_{k+1}B_k + B_{k-1} \qquad (k = -1, 0, 1, 2, 3, \ldots), \end{cases} \tag{1.6}$$

the convergents $C_m = \langle q_0, q_1, q_2, \ldots, q_m\rangle$ of (1.5) are given by A_m/B_m. Put

$$\mu = \begin{cases} \sqrt{D}\,, & D \not\equiv 1 \pmod 4, \\ (1+\sqrt{D})/2, & D \equiv 1 \pmod 4. \end{cases} \tag{1.7}$$

If we let $\phi_0 = \mu$, the continued fraction expansion of ϕ_0 has period p, and we have

$$\phi_n = (P_n + \sqrt{D})/Q_n, \qquad P_n, Q_n \in \mathfrak{Z},$$

and $\phi_{p+1} = \phi_1$. We must have a least positive integer j such that either

$$Q_{j-1} = Q_j \quad (N(\varepsilon) = -1), p = 2j-1,$$

or

$$P_{j-1} = P_j \quad (N(\varepsilon) = +1), p = 2j - 2.$$

In the latter case, since

$$N(A_{j-2} - \mu' B_{j-2}) = (-1)^{j-1}Q_{j-1}/Q_0,$$

and

$$\varepsilon = A_{p-1} - \mu' B_{p-1} = Q_0(A_{j-2} - \mu' B_{j-2})^2/Q_{j-1} \tag{1.8}$$

(see, for example, [9]), we see from (1.1) that Q_{j-1}/Q_0 is a principal factor of $\mathfrak{Q}(\sqrt{D})$.

Thus, the continued fraction algorithm provides us with the principal factors whenever they exist. It can also be used to find α_1 and α_2 (by (1.2)) in (1.1).

When $l = 3$ we let $\delta^3 = D = ab^2$ and $\bar{\delta}^3 = \bar{D} = a^2b$, where a, b are coprime square-free integers. We have

$$R = \begin{cases} 3ab, & D \not\equiv \pm 1 \pmod 9 \text{ and } 3 \nmid D, \\ ab, & \text{otherwise.} \end{cases}$$

Denote by α' and α'' the conjugates of any $\alpha \in K$, and write

$$\varepsilon = \left(g_1 + g_2\delta + g_3\bar{\delta}\right)/3 \qquad (g_1, g_2, g_3 \in \mathfrak{Z}). \tag{1.9}$$

Note that since $N(\varepsilon) = 1$, we have $g_1^3 \equiv 27 \pmod{ab}$.

If $k\varepsilon = \beta^3$ is solvable for $\beta \in K$ and k $(\neq 0) \in \mathfrak{Z}$, then there exist six unique primitive integers $\pm\alpha_1$, $\pm\alpha_2$, $\pm\alpha_3$, $\pm\beta_1$, $\pm\beta_2$, $\pm\beta_3$ of K such that

$$\begin{cases} \varepsilon = \alpha_i^3/N(\alpha_i), \\ \varepsilon^2 = \beta_i^3/N(\beta_i) \quad (i = 1, 2, 3). \end{cases} \tag{1.10}$$

Here $N(\alpha_i)$, $N(\beta_i)$ are divisors of R^2 and are called the principal factors of the discriminant of $K = \mathfrak{Q}(\sqrt[3]{D})$. These numbers have been discussed in some detail by Barrucand and Cohn [1], [2].

In fact, if $\alpha \in \mathfrak{Q}[\delta]$, $N(\alpha) \mid R^2$, and $N(\alpha) = 3^\tau d_1 d_2^2 d_4 d_5^2$, where $a = d_1d_2d_3$, $b = d_4d_5d_6$, then the six numbers α, $\delta\alpha/d_2d_4d_5$, $\bar{\delta}\alpha/d_1d_2d_5$, α^2/d_2d_5, $\delta\alpha^2/d_1d_2d_4d_5^2$, $\bar{\delta}\alpha^2/d_1d_2^2d_4d_5$ are all in $\mathfrak{Q}[\delta]$, and each of their norms divides R^2. Thus, each of the elements of the set

$$\left\{3^\tau d_1d_2^2d_4d_5^2,\ 3^\tau d_1^2d_3d_5d_6^2,\ 3^\tau d_2d_3^2d_4^2d_6,\ 3^\nu d_1^2d_2d_4^2d_5,\ 3^\nu d_2^2d_3d_4d_6^2,\ 3^\nu d_1d_3^2d_5^2d_6\right\}, \tag{1.11}$$

where $(\tau, \nu) = (0, 0)$, $(1, 2)$ or $(2, 1)$ is a principal factor whenever $N(\alpha)$ is.

Let ρ be a primitive cube root of unity and put $\Omega = \mathfrak{Q}(\rho)$, $L = K(\rho)$. If H is the class number of L and h is the class number of K, then

$$H = rh^2/3, \tag{1.12}$$

where $r = 1$ or 3, see [2]. Using the results of [2] together with a later result of Halter-Koch [5], we get the following

THEOREM. *Consider the equation*

$$\frac{\varepsilon'}{\varepsilon} = \rho^i\gamma^3 \qquad (\gamma \in L = K(\rho)),\ 0 \leqslant i < 2, \tag{1.13}$$

(i) (1.13) *has no solution if and only if* $r = 1$,

(ii) (1.13) *has a solution with* $i = 0$ *if and only if principal factors exist for* K,

(iii) (1.13) *has a solution with* $i \neq 0$ *if and only if there exists a unit* $E \in L$ *such that the relative norm,*

$$N_{L/\Omega}(E) = \rho. \tag{1.14}$$

The equation (1.13) is completely analogous to (1.3). But note that we have three possible cases here not just two. When $l = 2$ there is no analogue to case (i). We also point out that Eq. (1.14) is the $l = 3$ version of (1.4).

Brunotte, Klingen, and Steurich [3] have shown that r in (1.12) is 3 if and only if g_1 in (1.9) satisfies

$$g_1 \equiv 3 \pmod{ab}. \tag{1.15}$$

This allows us to find a method of distinguishing between (i) and the other two cases (ii) and (iii). However, we cannot distinguish between (ii) and (iii). In [2] it is shown that principal factors must exist if D has no prime factors of the form $1 + 3t$ and at least one prime factor of the form $2 + 9t$ or $5 + 9t$. Further, if (iii) holds, then each prime factor of D must be 3 or of the form $9t + 1$. These conditions are not enough, however, for if $D = 19$, then case (i) holds, and if $D = 51$, then case (ii) holds. We do note that if D is a prime of the form $9t - 1$, then (iii) holds. This is because $r = 3$ by (1.15) and principal factors cannot exist because $R = D$.

Since principal factors can play an important role in the determination of the fundamental unit of K (see Williams [11] and [12]) and since their existence tells us that the Diophantine equation

$$N(\alpha) = d$$

is solvable for some $d \mid R^2$, it is of some interest to develop a means of finding the principal factors for any $Q(\sqrt[3]{D})$ when they exist or showing that they do not exist. In this paper we describe a technique for distinguishing between cases (ii) and (iii). The method is analogous to the continued fraction method described above for $l = 2$, but there are some complications which must be taken into consideration. We also present some numerical results from a computer run of our algorithm on all values of D between 1 and 15,000.

2. Relative Minima and the Algorithm of Voronoi When $l = 2$. In the next two sections we give a very brief description of Voronoi's [8] idea for extending the continued fraction algorithm over $\mathfrak{Q}(\sqrt{D})$ into $\mathfrak{Q}(\sqrt[3]{D})$. It should be emphasized that our treatment here is much less general than that of [8].

Let $\lambda, \mu \in \mathfrak{Q}(\sqrt{D})$ and put $\Lambda = (\lambda, \lambda')$, $M = (\mu, \mu')$. Let $\mathbb{S}$ be the lattice defined by

$$\mathbb{S} = \{uA + vM \mid u, v \in \mathfrak{Z}\}.$$

We say that $\mathbb{S}$ is a lattice with *basis* $[\Lambda, M]$. If $A = (\alpha, \alpha') \in \mathbb{S}$, we define the *normed body* of A to be

$$\mathfrak{N}(A) = \{(x, y) | x, y \in \mathfrak{R}, |x| < |\alpha|, |y| \leqslant |\alpha'|\},$$

where $\mathfrak{R}$ is the set of reals. If $\Theta \in \mathbb{S}$ and $\mathfrak{N}(\theta) \cap \mathbb{S} = \{(0, 0)\}$, we say that Θ is a *relative minimum* of $\mathbb{S}$.

Since $\mathbb{S}$ is symmetric about the y axis, we will lose no generality by working with only those points of $\mathbb{S}$ which have a nonnegative first component. If $\Theta = (\theta, \theta')$, $\Phi = (\phi, \phi')$ are relative minima of $\mathbb{S}$ with $\theta > \phi > 0$, we say that they are *adjacent* if there does not exist $\Psi = (\psi, \psi')$ $(\neq (0, 0)) \in \mathbb{S}$ such that $|\psi| < |\theta|$ and $|\psi'| < |\phi'|$. Voronoi proved

THEOREM 2.1. *Let $\Theta = (\theta, \theta')$, $\Phi = (\phi, \phi')$ be elements of $\mathbb{S}$ such that $\theta > \phi > 0$. If $[\Theta, \Phi]$ is a basis of $\mathbb{S}$, then Θ and Φ are adjacent relative minima if and only if $|\theta'| < |\phi'|$ and $\theta'\phi' < 0$.*

COROLLARY. *Let $\mathbb{S}$ have basis $[(1, 1), (\theta, \theta')]$. If $0 < \theta < 1$ and $\theta' < -1$, then $\mathbb{S}$ has $(1, 1)$ and $(\theta + [-\theta'], \theta' + [-\theta'])$ as adjacent relative minima.**

* Here we use the notation $[\alpha]$ to denote that rational integer such that $\alpha - 1 < [\alpha] \leqslant \alpha$.

If $\Theta_i = (\theta_i, \theta_i') \in \mathfrak{S}$ $(i = 1, 2, 3, \ldots)$, where $0 < \theta_i < \theta_{i+1}$ and Θ_i and Θ_{i+1} are adjacent relative minima, we call

$$\Theta_1, \Theta_2, \Theta_3, \ldots, \Theta_n, \ldots \tag{2.1}$$

a *chain* of relative minima of $\mathfrak{S}$. Voronoi showed that if $A = (\alpha, \alpha')$ is a relative minimum of $\mathfrak{S}$ and $\alpha > \theta_1$, then A must be one of the Θ_i in the chain (2.1).

Let $\mathfrak{S}$ have $[(1, 1), (\theta, \theta')]$, where $0 < \theta < 1$ and $\theta' < -1$, as a basis, and let

$$\Theta_1 = (1, 1), \Theta_2, \Theta_3, \ldots, \Theta_n, \ldots \tag{2.2}$$

be a chain of relative minima of $\mathfrak{S}$. Put $\Theta_g^{(1)} = (\theta_g^{(1)}, \theta_g^{(1)'}) = \Theta_2$. We see by the corollary of Theorem 2.1 that $\Theta_2 = (\theta + [-\theta'], \theta' + [-\theta'])$; hence $\mathfrak{S}_1 = \mathfrak{S}$ has $[(1, 1), \Theta_g^{(1)}]$ as a basis. Let $\mathfrak{S}_2$ have $[(1, 1), (1/\theta_g^{(1)}, 1/\theta_g^{(1)'})]$ as a basis, and let $\Theta_g^{(2)}$ be the relative minimum adjacent to (1, 1) in $\mathfrak{S}_2$ such that $\theta_g^{(2)} > 1$. Then, by the corollary of Theorem 2.1,

$$\theta_g^{(2)} = 1/\theta_g^{(1)} + \left[-1/\theta_g^{(1)'}\right],$$

and $\theta_3 = \theta_g^{(1)}\theta_g^{(2)}$. In fact, if $\mathfrak{S}_n$ has basis $[(1, 1), (1/\theta_g^{(n-1)}, 1/\theta_g^{(n-1)'})]$, we find that

$$\theta_g^{(n)} = 1/\theta_g^{(n-1)} + \left[-1/\theta_g^{(n-1)'}\right] > 1$$

is the relative minimum adjacent to (1, 1) in $\mathfrak{S}$. Also, if $\Theta_n = (\theta_n, \theta_n')$, then

$$\theta_n = \prod_{i=1}^{n-1} \theta_g^{(i)}. \tag{2.3}$$

Putting $\phi_0 = -\theta'$, $q_0 = [\phi_0]$, $q_{k+1} = [-1/\theta_g^{(k)'}]$, $\phi_k = (\theta_g^{(k)'})^{-1}$, we see that $\langle q_0, q_1, q_2, \ldots, q_{n-1}, \phi_n \rangle$ is the continued fraction expansion of ϕ_0.

If μ is defined as in (1.7), we note that since μ and $[\mu] - \mu'$ differ by an integer, their continued fraction expansions have the same values for ϕ_k in (1.5) for $k = 1, 2, 3, \ldots$. Putting $\theta = \mu - [\mu]$ above, it is a simple matter to show that

$$\theta_g^{(k)} = (\phi_k')^{-1} = \frac{Q_k}{\sqrt{D} - P_k} = \frac{P_k + \sqrt{D}}{Q_k} \qquad (k = 1, 2, 3, \ldots).$$

Further

$$\theta_n = \prod_{i=1}^{n-1} \frac{P_i + \sqrt{D}}{Q_i} = A_{n-2} - \mu' B_{n-2},$$

and if we define $N(\Theta)$ the norm of $\Theta = (\theta, \theta')$ to be $N(\theta) = \theta\theta'$, then

$$N(\Theta_n) = (-1)^{n-1} Q_{n-1}/Q_0.$$

Thus, from the results in Section 1 we see that principal factors of $\mathfrak{Q}(\sqrt{D})$ exist if and only if for some n such that $2 \leqslant n \leqslant p$, we have $\mathfrak{N}(\Theta_n) \mid R$.

3. Relative Minima and the Algorithm of Voronoi When $l = 3$. The reason we have given such a lengthy discussion of Voronoi's continued fraction algorithm for $l = 2$ is that it is a simple matter to extend several of these ideas to the case of $l = 3$. In this case, we let $\lambda, \mu, \nu \in \mathfrak{Q}(\sqrt[3]{D})$ and put

$$\Lambda = (\lambda, (\lambda' - \lambda'')/2i, (\lambda' + \lambda'')/2),$$
$$M = (\mu, (\mu' - \mu'')/2i, (\mu' + \mu'')/2),$$
$$N = (\nu, (\nu' - \nu'')/2i, (\nu' + \nu'')/2),$$

where i is a fixed zero of $x^2 + 1$. All components of Λ, M, N are real. We let $\mathbb{S}$ be the lattice defined by

$$\mathbb{S} = \{u\Lambda + vM + wN \mid u, v, w \in \mathfrak{Z}\},$$

and we say that $\mathbb{S}$ has basis $[\Lambda, M, N]$ or $[\lambda, \mu, \nu]$. If $A \in \mathbb{S}$, then

$$A = (\alpha, (\alpha' - \alpha'')/2i, (\alpha' + \alpha'')/2).$$

We often write this as $A \approx \alpha$ or $\alpha \approx A$. If $A \in \mathbb{S}$, we define the *normed body* of A to be

$$\mathfrak{N}(A) = \{(x, y, z) \mid x, y, z \in \mathfrak{R}, |x| < |\alpha|, y^2 + z^2 \leqslant |\alpha'|^2\}.$$

It should be noted here that

$$|\alpha'|^2 = |\alpha''|^2 = \alpha'\alpha'' = N(\alpha)/\alpha = ((\alpha' - \alpha'')/2i)^2 + ((\alpha' + \alpha'')/2)^2.$$

If $\Theta \in \mathbb{S}$ and $\mathfrak{N}(\Theta) \cap \mathbb{S} = \{(0, 0, 0)\}$, we say that Θ is a *relative minimum* of $\mathbb{S}$. If $\Theta \approx \theta$ and $\Phi \approx \phi$ are relative minima of $\mathbb{S}$ with $\theta > \phi > 0$, we say that they are *adjacent* if there does not exist a Ψ $(\neq (0, 0, 0)) \in \mathbb{S}$ such that if $\Psi \approx \psi$ then $|\psi| < |\theta|$ and $|\psi'| < |\phi'|$. If $\Theta_i \in \mathbb{S}$ $(i = 1, 2, 3, \ldots)$, where $\Theta_i \approx \theta_i$, $0 < \theta_i < \theta_{i+1}$ and Θ_i and Θ_{i+1} are adjacent relative minima of $\mathbb{S}$, we call

$$\Theta_1, \Theta_2, \Theta_3, \ldots, \Theta_n, \ldots \tag{3.1}$$

a chain of relative minima of $\mathbb{S}$. We also have the result that if $A \approx \alpha$ is a relative minimum of $\mathbb{S}$ and $\alpha > \theta_1$, then A must occur as an element in (3.1).

If (1, 0, 1) is a relative minimum of $\mathbb{S}$ and

$$\Theta_1 = (1, 0, 1), \Theta_2, \Theta_3, \ldots, \Theta_n, \ldots \tag{3.2}$$

is a chain of relative minima of $\mathbb{S}$, we can find the elements in (3.2) if we can develop a method of finding the relative minimum $\Theta_g \approx \theta_g > 1$ adjacent to (1, 0, 1) in any lattice of type $\mathbb{S}$ in which (1, 0, 1) is a relative minimum. We do this as we did in the case when $l = 2$. Simply let $\mathbb{S}_1 = \mathbb{S}$ and $\Theta_g^{(1)} \approx \theta_g^{(1)} > 1$ be the relative minimum adjacent to (1, 0, 1) in $\mathbb{S}_1$. Embed 1, $\theta_g^{(1)}$ in a basis of $\mathbb{S}_1$ and let this basis be $[1, \theta_g^{(1)}, \theta_h^{(1)}]$. Let $\mathbb{S}_2$ have basis $[1, 1/\theta_g^{(1)}, \theta_h^{(1)}/\theta_g^{(1)}]$. We see that (1, 0, 1) is a relative minimum of $\mathbb{S}_2$, and we find the relative minimum $\Theta_g^{(2)} \approx \theta_g^{(2)} > 1$ adjacent to (1, 0, 1) in $\mathbb{S}_2$. We continue this process by defining $\mathbb{S}_n$ to be the lattice with basis $[1, 1/\theta_g^{(n-1)}, \theta_h^{(n-1)}/\theta_g^{(n-1)}]$, where $\Theta_g^{(n-1)} \approx \theta_g^{(n-1)} > 1$ is the relative minimum adjacent to (1, 0, 1) in $\mathbb{S}_{n-1}$. It follows that

$$\theta_n = \prod_{i=1}^{n-1} \theta_g^{(i)}, \qquad \theta_g^{(k)} = \left(m_1^{(k)} + m_2^{(k)}\delta + m_3^{(k)}\bar{\delta}\right)/\sigma_k,$$

$$\theta_h^{(k)} = \left(n_1^{(k)} + n_2^{(k)}\delta + n_3^{(k)}\bar{\delta}\right)/\sigma_k,$$

where $m_1^{(k)}, m_2^{(k)}, m_3^{(k)}, n_1^{(k)}, n_2^{(k)}, n_3^{(k)}, \sigma_k \in \mathfrak{Z}$, $\sigma_k > 0$, and

$$\text{g.c.d.}\left(\sigma_k, m_1^{(k)}, m_2^{(k)}, m_3^{(k)}, n_1^{(k)}, n_2^{(k)}, n_3^{(k)}\right) = 1.$$

When there is no doubt as to the value of k in the superscripts here, we will omit them.

In the remainder of this paper we assume that $\mathbb{S}_1$ is the lattice with basis $[1, \mu, \nu]$, where $[1, \mu, \nu]$ is a basis of the algebraic integers of $\mathfrak{Q}(\delta)$. In this case (1, 0, 1) is a relative minimum of $\mathbb{S}_1$ and so is $E \approx \varepsilon$. This algorithm is periodic with period p, i.e., $\theta_g^{(k)} = \theta_g^{(k+p)}$ $(k = 1, 2, 3, \ldots)$, where $\theta_{p+1} = \varepsilon$. Unfortunately, we do not

have a simple theorem like Theorem 2.1 to help us find the values of $\theta_g^{(k)}$. In [8] Voronoi gave a method of doing this without proof. He did give a proof of a method for finding the elements of a different chain from (3.2). This method is described in Delone and Faddeev [4]. In Williams, Cormack, and Seah [10] a proof is provided of a relatively rapid technique for finding these $\theta_g^{(k)}$'s.

In order to use the above ideas as part of a method for finding principal factors for $\mathfrak{Q}(\delta)$, we would like to have a result similar to the one at the end of Section 2. If we define $N(\Theta_n) = N(\theta_n)$ when $\Theta_n \approx \theta_n$, it is certainly true that if $2 \leqslant n \leqslant p$ $(l = 3)$ and $N(\Theta_n) \mid R^2$, then $N(\Theta_n)$ is a principal factor. But must this occur if $\mathfrak{Q}(\delta)$ has principal factors? We shall see that it does not. In spite of this we will still be able to use Voronoi's algorithm to find principal factors. In order to do this, we will have to use several results from [12]. One of these is

LEMMA 3.1. *Let* $\alpha \in \mathfrak{Q}[\delta]$, *and suppose* $N(\alpha) \mid R^2$. *Put* $N(\alpha) = 3^\tau d_1 d_2^2 d_4 d_5^2$, *where* $a = d_1 d_2 d_3$, $b = d_4 d_5 d_6$. *If*

$$\lambda^3 = 3^\tau \min\{d_1 d_2^2 d_4 d_5^2,\ d_1^2 d_3 d_5 d_6^2,\ d_2 d_3^2 d_4^2 d_6\},$$

then $\gamma = \lambda\alpha / N(\alpha)^{1/3} \in \mathfrak{Q}[\delta]$. *Furthermore,* $N(\gamma) \mid R^2$, *and if we put* $N(\gamma) = 3^\tau r s^2$, *where* $r = r_1 r_2$, $s = s_1 s_2$, $r_1 s_2 \mid a$, $r_2 s_2 \mid b$, *then*

$$\delta / r_2 s, \quad \bar{\delta} / r_1 s > 1.$$

By using (1.11) and this result, we know that if there is a principal factor for $\mathfrak{Q}(\delta)$, then there must be some $\gamma \in \mathfrak{Q}(\delta)$ such that

$$\begin{cases} \gamma \in \mathfrak{Q}[\delta], \\ N(\gamma) = 3^\tau r s^2, \quad N(\gamma) \mid R^2 \ (\tau = 0, 1), \\ \delta_1 = \delta / r_2 s > 1, \quad \delta_2 = \bar{\delta} / r_1 s > 1. \end{cases} \tag{3.3}$$

By Theorem 2 of [11] we know that if $D \not\equiv \pm 1 \pmod 9$ and $N(\gamma) = r s^2$, then $\Gamma \approx \gamma$ is a relative minimum of $\mathfrak{S}_1$, and we can find Γ by using Voronoi's algorithm. We will assume that the values of D with which we are dealing are such that either $D \equiv \pm 1 \pmod 9$ or $N(\alpha) = 3 r s^2$. Under this assumption we have

$$\tau = \begin{cases} 0 & \text{when } D \equiv \pm 1 \pmod 9, \\ 1 & \text{when } D \not\equiv \pm 1 \pmod 9. \end{cases} \tag{3.4}$$

THEOREM 3.2 [12]. *Suppose that there exists some* $\alpha \in \mathfrak{Q}[\delta]$ *such that* $N(\alpha) \mid R^2$. *Let* γ *be defined as in* (3.3) *and* (3.4). *Then* $\Gamma \approx \gamma$ *is not a relative minimum of* $\mathfrak{S}_1$ *if and only if there exists a nonzero* $\kappa \in \mathfrak{Q}[\delta]$ *such that* $\kappa = r s^2 \chi$, *where* $\chi = X_1 + X_2\delta_1 + X_3\delta_2$ $(X_1, X_2, X_3 \in \mathfrak{Z})$ *and*

$$X_1 \equiv a r_2 s X_2 \equiv b r_1 s X_3 \pmod 3, \tag{3.5}$$

$$0 < \chi < 3, \tag{3.6}$$

$$F(\chi) = X_1^2 + \delta_1^2 X_2^2 + \delta_2^2 X_3^2 - \delta_1 X_1 X_2 - \delta_2 X_1 X_3 - \delta_1\delta_2 X_2 X_3 < 9. \tag{3.7}$$

COROLLARY. *If* Γ *above is not a relative minimum of* $\mathfrak{S}_1$, *then* $\Theta \approx \theta = 3^{\tau-1}\kappa\gamma / N(\gamma)$ *is a relative minimum of* $\mathfrak{S}_1$ *when* $\kappa = r s^2 \chi$ *and* χ *is the least value of* $X_1 + X_2\delta_1 + X_3\delta_2$ *such that* (3.5), (3.6), *and* (3.7) *are satisfied.*

In the next section we will show how Voronoi's algorithm can be used to find Γ when it is not a relative minimum of $\mathfrak{S}_1$.

4. The Algorithm. We must first find the κ of the corollary of Theorem 3.2. To do this we use

THEOREM 4.1. *Suppose* γ *is given by* (3.3) *and* (3.4) *and* $\Gamma \approx \gamma$. *Let* $\eta_1 \equiv ar_2s$, $\eta_2 \equiv br_1s \pmod 3$, *where* $|\eta_i| = 1$ $(i = 1, 2)$, *and put* $X_1 = -\eta_1\eta_2$, $X_2 = -\eta_2$, $X_3 = -\eta_1$, $\chi = X_1 + X_2\gamma_1 + X_3\gamma_2$, $\kappa = rs^2\chi$. Γ *is not a relative minimum of* $\mathfrak{S}_1$ *if and only if* $\eta_1 + \eta_2 \neq 2$ *and* $F(\chi) < 9$. *Further, if* Γ *is not a relative minimum of* $\mathfrak{S}_1$, *then* $\Theta \approx \theta = 3^{\tau-1}\kappa\gamma/N(\gamma)$ *is*.

The proof follows easily from Lemma 4.2 of [12] and the corollary of Theorem 3.2. It should be noted that the proof of Lemma 4.2 of [12] assumed that $\delta_1 < \delta_2$; but, as remarked in [12], if this is not the case, we need only interchange the values of a and b, r_1 and r_2 and s_1 and s_2. This has the effect of interchanging the values of δ_1 and δ_2, η_1 and η_2 while keeping γ the same. □

We now define an *admissible d-set* for $\mathfrak{Q}(\delta)$. Let d be any divisor of R^2 such that

$$d = 3^\tau d_1 d_2^2 d_4 d_5^2 \qquad (\tau = 0, 1),$$

where $a = d_1d_2d_3$, $b = d_4d_5d_6$, and

$$d_1d_3d_6^2 > d_2^2d_4d_5, \qquad d_3^2d_4d_6 > d_1d_2d_5^2. \tag{4.1}$$

Put $X_2 \equiv -d_1d_2d_4d_6$, $X_3 \equiv -d_1d_3d_4d_5$, $X_1 \equiv -X_2X_3 \pmod 3$, where $|X_i| = 1$ $(i = 1, 2, 3)$; also, let

$$Q = 3^{\tau-3}\left(3^{-\tau}dX_1 + d_1^2d_3d_5d_6^2X_2 + d_2d_3^2d_4^2d_6X_3 + 3ab\right). \tag{4.2}$$

We say that $\{\tau, d_1, d_2, d_3, d_4, d_5, d_6\}$ is an admissible d-set of $\mathfrak{Q}(\delta)$ if $X_2 + X_3 \neq -2$ and

$$d(2d - 3^\tau abX_1 + 3QX_1) > 3Q^2. \tag{4.3}$$

THEOREM 4.2. *Let* γ *satisfy* (3.3) *and* (3.4), *and put* $d_1 = r_1$, $d_2 = s_1$, $d_4 = r_2$, $d_5 = s_2$, $d_3 = a/d_1d_2$, $d_6 = b/d_3d_4$. *If* $\Gamma \approx \gamma$ *is not a relative minimum of* $\mathfrak{S}_1$, *then* $\{\tau, d_1, d_2, d_3, d_4, d_5, d_6\}$ *must be an admissible d-set of* $\mathfrak{Q}(\delta)$.

Proof. Since $\delta_1, \delta_2 > 1$ in (3.3), we must have (4.1). Also $X_1 = -\eta_1\eta_2$, $X_2 = -\eta_2$, $X_3 = -\eta_1$ in Theorem 4.1 and $\kappa = rs^2\chi$, where $\chi = X_1 + X_2\delta_1 + X_3\delta_2$; hence,

$$\kappa = d_1d_2^2d_4d_5^2X_1 + d_1d_2d_5X_2\delta + d_2d_4d_5X_3\bar{\delta}, \tag{4.4}$$

and Q in (4.2) is given by

$$Q = 3^{3\tau-3}N(\kappa)/N(\gamma)^2. \tag{4.5}$$

Since Γ is not a relative minimum, we must have $\eta_1 + \eta_2 \neq 2$, and therefore $X_2 + X_3 \neq -2$. Further, $\chi > 0$ and $F(\chi) < 9$. Now $F(\chi) = \kappa'\kappa''/r^2s^4$; hence, $F(\chi) < 9$ if and only if

$$N(\kappa)/\kappa < 9r^2s^4 \quad \text{or} \quad Q < 3^{\tau-1}\kappa \quad \text{or} \quad N(3^{\tau-1}\kappa - Q) > 0.$$

Since

$$N(3^{\tau-1}\kappa - Q) = Q\left(2 \cdot 3^{2\tau-1}d_1^2d_2^4d_4^2d_5^4 - 3^{2\tau-1}d_1^2d_2^3d_3d_4^2d_5^3d_6X_1 + 3^\tau d_1d_2^2d_4d_5^2X_1Q - Q^2\right),$$

we see that (4.3) also holds. Hence $\{\tau, d_1, d_2, d_3, d_4, d_5, d_6\}$ is an admissible d-set. □

If $\Gamma \approx \gamma$ is not a relative minimum here, we know that $\Theta \approx \theta = 3^{\tau-1}\kappa\gamma/N(\gamma)$ is a relative minimum. Since $N(\Theta) = N(\theta) = 3^{3\tau-3}N(\kappa)/N(\gamma^2)$, we see that $N(\theta) = Q$ by (4.5). Thus, given any value of D, we need only find all the possible admissible d-sets and keep the corresponding Q values. As we proceed through Voronoi's algorithm in generating $\Theta_2, \Theta_3, \Theta_4, \ldots$ etc., we check to see whether any $N(\Theta_i)$ either divides R^2 or is equal to one of these Q values. In [10] it is shown that these values of $N(\Theta_i) = N(\theta_i)$ are easy to determine; in fact, $N(\theta_i) = \sigma_i^2/\sigma_1|e_i|$, where $e_i = m_2^{(i)}n_3^{(i)} - n_2^{(i)}m_3^{(i)}$.

The one main difficulty in using this approach is the possibility of a large number of admissible d-sets for a particular $\mathfrak{Q}[\delta]$. However, we see in Table 1 below that this does not seem to happen very often. In this table n is the number of admissible d-sets and $f(n)$ is the number of cube-free values of $D \leqslant 15000$ such that $\mathfrak{Q}(\sqrt[3]{D})$ has n admissible d-sets. There are 12478 cube-free values of D such that $2 \leqslant D \leqslant 15000$.

TABLE 1

n	$f(n)$	n	$f(n)$	n	$f(n)$
0	10998	12	34	27	4
1	280	13	3	30	1
2	205	14	1	33	4
3	386	15	26	36	2
4	64	16	2	39	4
5	29	17	5	42	4
6	218	18	28	45	3
7	16	19	1	48	4
8	20	20	2	51	6
9	78	21	18	54	5
10	10	22	2	57	2
11	5	24	7	60	1
TOTAL $f(n)$:		12478			

If $N(\theta_i) \mid R^2$, then $N(\theta_i)$ is a principal factor of $\mathfrak{Q}(\delta)$; if this does not occur but $N(\theta_i) = Q$ for a d-set $\{\tau, d_1, d_2, d_3, d_4, d_5, d_6\}$, we must then determine whether the corresponding γ value is an algebraic integer of $\mathfrak{Q}(\delta)$. This value of γ is given by

$$\gamma = \theta_i N(\gamma)/3^{\tau-1}\kappa, \tag{4.6}$$

where $N(\gamma) = 3^\tau d = 3^\tau d_1 d_2^2 d_4 d_5^2$, and κ is given by (4.4). Clearly, if $\gamma \in \mathfrak{Q}[\delta]$, then $N(\gamma)$ is a principal factor for $\mathfrak{Q}(\delta)$.

We first note that $\kappa'\kappa'' = 3^{-\tau}d(k_1 + k_2\delta + k_3\bar{\delta})$, where

$$k_1 = 3^{-\tau}d + abX_1, \quad k_2 = d_2d_3d_4 + d_1d_2d_5X_3, \quad k_3 = d_1d_5d_6 + d_2d_4d_5X_2. \tag{4.7}$$

We now have

THEOREM 4.3. *If, for some admissible d-set, we get* $N(\Theta_i) = Q$ *for some* Θ_i *in the chain* (3.2), *then* γ *in* (4.6) *is an algebraic integer of* $\mathfrak{Q}(\delta)$ *if and only if*

$$\text{(4.8)} \qquad \begin{cases} k_2n_3 - k_3n_2 \equiv k_2m_3 - k_3m_2 \equiv 0 \pmod{3\sigma_i}, \\ k_1e_i - (k_2n_3 - k_3n_2)m_1 + (k_2m_3 - k_3m_2)n_1 \equiv 0 \pmod{3\sigma_i^2}, \end{cases}$$

where $\theta_g^{(i)} = (m_1 + m_2\delta + m_3\bar{\delta})/\sigma_i$, $\theta_h^{(i)} = (n_1 + n_2\delta + n_3\bar{\delta})/\sigma_i$, $e_i = m_2n_3 - m_3n_2$ *and* k_j $(j = 1, 2, 3)$ *are given by* (4.7).

Proof. If $\mu_i, \nu_i \in \mathfrak{Q}(\delta)$ and $[1, \mu_i, \nu_i]$ is a basis of $\mathfrak{S}_i$, then

$$\begin{bmatrix} 1 \\ \mu_i \\ \nu_i \end{bmatrix} = \frac{1}{\theta_i} T \begin{pmatrix} 1 \\ \mu \\ \nu \end{pmatrix},$$

where T is a matrix with integer entries and $|T| = \pm 1$. Thus, $\gamma \in \mathfrak{Q}[\delta]$ if and only if $\gamma/\theta_i = x + y\mu_i + z\nu_i$ $(x, y, z \in \mathfrak{Z})$, and therefore $\gamma \in \mathfrak{Q}[\delta]$ if and only if there exist $x, y, z \in \mathfrak{Z}$ such that

$$\text{(4.9)} \qquad \frac{N(\gamma)}{3^{\tau-1}\kappa} = x + y\mu_i + z\nu_i.$$

Now, from (4.5),

$$\frac{N(\gamma)}{3^{\tau-1}} = \frac{3^{2\tau-2}\kappa'\kappa''}{N(\gamma)Q};$$

hence, (4.9) becomes

$$\text{(4.10)} \qquad 3^{\tau-2}\left(k_1 + k_2\delta + k_3\bar{\delta}\right) = Q(x + y\mu_i + z\nu_i).$$

Since $[1, \theta_g^{(i)}, \theta_h^{(i)}]$ is a basis of $\mathfrak{S}_i$, we can assume without loss of generality that $\mu_i = \theta_g^{(i)}$, $\nu_i = \theta_h^{(i)}$. Also, since $Q = N(\Theta_i) = \sigma_i^2/\sigma_1|e_i|$ and $\sigma_1 = 3^{1-\tau}$ by (3.4), we get

$$|e_i|k_1 = 3\sigma_i(\sigma_i x + ym_1 + zn_1), \quad |e_i|k_2 = 3\sigma_i(ym_2 + zn_2),$$
$$|e_i|k_3 = 3\sigma_i(ym_3 + zn_3),$$

from (4.10). Solving these equations for x, y, z, we get

$$3\sigma_i e_i y = |e_i|(k_2n_3 - k_3n_2), \quad 3\sigma_i e_i z = -|e_i|(k_2m_3 - k_3n_2),$$
$$3\sigma_i^2 x = |e_i|k_1 - 3\sigma_i ym_1 - 3\sigma_i zn_1.$$

Thus, x, y, z are integers if and only if the congruences (4.8) hold. □

Our algorithm for determining whether or not $\mathfrak{Q}(\delta)$ has a principal factor is the following sequence of three steps

(1) Determine whether or not any $N(\Theta_i)$ for Θ_i in the chain (3.2) and $2 < i < p$ is such that $N(\Theta_i) \mid R^2$. If so, we have a principal factor $N(\Theta_i)$ of $\mathfrak{Q}(\delta)$, and we can terminate the algorithm.

(2) If no such Θ_i is found by step (1), find all admissible d-sets for $\mathfrak{Q}(\delta)$ and their corresponding Q values. Check if any of these Q values is $N(\Theta_i)$ for $i < p$. If none is, we know that we have no principal factors for $\mathfrak{Q}(\delta)$, and we can terminate the algorithm.

(3) If $N(\Theta_i) = Q_j$ for one of the Q's in step (2), check whether the congruences (4.8) hold. If they do for some Q, then we have a principal factor $3^\tau d_j$; otherwise, there is no principal factor for $\mathfrak{Q}(\delta)$.

As an example, we mention that for $D = 850$, we get

$$\theta_2 = 18 + 2\delta + \bar{\delta}, \quad \theta_3 = 161 + 17\delta + \bar{\delta}, \quad \varepsilon = \theta_4 = 341 + 36\delta + 19\bar{\delta}.$$

Here, $N(\theta_2) = 52$, $N(\theta_3) = 121$. Thus, Voronoi's algorithm does not find a principal factor. However, we see that $\{1, 2, 1, 17, 1, 5, 1\}$ ($d = 3 \cdot 2 \cdot 5^2$) is an admissible d-set, and with $\kappa = -50 + 10\delta + 5\bar{\delta}$ we get $\gamma = 180 + 19\delta + 10\bar{\delta} \in \mathfrak{Q}[\delta]$ and $N(\gamma) = 150$; thus, 150 is a principal factor.

5. Determination of r. We have seen that the value of r in (1.12) can be determined when we know the value of g_1 modulo ab. In this section we describe how Voronoi's algorithm can be used to find $g_1 \pmod{ab}$.

We note that if $n > 1$, $\theta_{n-1} = \prod_{i=1}^{n-2} \theta_g^{(i)}$, $\theta_n = \theta_g^{(n-1)}\theta_{n-1}$, $\psi_n = \theta_h^{(n-1)}\theta_{n-1}$, then $[\theta_{n-1}, \theta_n, \psi_n]$ is a basis of the integers in $\mathfrak{Q}(\delta)$. Thus, we have

$$\text{(5.1)} \qquad \begin{cases} \theta_{k+1} = x_1^{(k)}\theta_k + y_1^{(k)}\theta_{k-1} + z_1^{(k)}\psi_k, \\ \psi_{k+1} = x_2^{(k)}\theta_k + y_2^{(k)}\theta_{k-1} + z_2^{(k)}\psi_k, \end{cases}$$

where $x_i^{(k)}, y_i^{(k)}, z_i^{(k)} \in \mathfrak{Z}$ ($i = 1, 2$). If we put

$$\theta_k = \left(G_1^{(k)} + G_2^{(k)}\delta + G_3^{(k)}\bar{\delta}\right)/3, \qquad \psi_k = \left(H_1^{(k)} + H_2^{(k)}\delta + H_3^{(k)}\bar{\delta}\right)/3,$$

we get

$$\text{(5.2)} \qquad \begin{cases} G_i^{(k+1)} = x_1^{(k)}G_i^{(k)} + y_1^{(k)}G_i^{(k-1)} + z_1^{(k)}H_i^{(k)}, \\ H_i^{(k+1)} = x_2^{(k)}G_i^{(k)} + y_2^{(k)}G_i^{(k-1)} + z_2^{(k)}H_i^{(k)} \qquad (i = 1, 2, 3). \end{cases}$$

These are the formulas which are analogous to (1.6) for the usual continued fraction. Also, $G_1^{(1)} = 3$, $G_2^{(1)} = G_3^{(1)} = 0$, $G_i^{(2)} = 3m_i^{(1)}/\sigma_1$, $H_i^{(2)} = 3n_i^{(1)}/\sigma_1$.

If we put $i = 1$ in (5.2), we can use (5.2) as a pair of congruences modulo ab to find $g_1 = G_1^{(p+1)} \pmod{ab}$. All that is needed is a method of calculating $x_i^{(k)}$, $y_i^{(k)}$, $z_i^{(k)}$, $i = 1, 2$.

If we divide each of the equations in (5.1) by θ_k, we get

$$\text{(5.3)} \qquad \begin{cases} \theta_g^{(k)} = x_1^{(k)} + y_1^{(k)}/\theta_g^{(k-1)} + z_1^{(k)}\theta_h^{(k-1)}/\theta_g^{(k-1)}, \\ \theta_h^{(k)} = x_2^{(k)} + y_2^{(k)}/\theta_g^{(k-1)} + z_2^{(k)}\theta_h^{(k-1)}/\theta_g^{(k-1)}. \end{cases}$$

Let

$$1/\theta_g^{(k-1)} = \left(m_1^{*(k)} + m_2^{*(k)}\delta + m_3^{*(k)}\bar{\delta}\right)/\sigma_k,$$

$$\theta_h^{(k-1)}/\theta_g^{(k-1)} = \left(n_1^{*(k)} + n_2^{*(k)}\delta + n_3^{*(k)}\bar{\delta}\right)/\sigma_k.$$

From (5.3) we get six equations in the six unknowns $x_i^{(k)}, y_i^{(k)}, z_i^{(k)}$ ($i = 1, 2$). Solving these, we get

$$e_k^* y_1^{(k)} = m_2^{(k)}n_3^{*(k)} - m_3^{(k)}n_2^{*(k)}, \qquad e_k^* y_2^{(k)} = n_2^{(k)}n_3^{*(k)} - n_3^{(k)}n_2^{*(k)},$$

$$e_k^* z_1^{(k)} = m_3^{(k)}m_2^{*(k)} - m_2^{(k)}m_3^{*(k)}, \qquad e_k^* z_2^{(k)} = n_3^{(k)}m_2^{*(k)} - n_2^{(k)}m_3^{*(k)},$$

$$\sigma_k x_1^{(k)} = m_1^{(k)} - y_1^{(k)}m_1^{*(k)} + z_1^{(k)}n_1^{*(k)}, \qquad \sigma_k x_2^{(k)} = n_1^{(k)} - y_2^{(k)}m_1^{*(k)} - z_2^{(k)}n_1^{*(k)},$$

where $e_k^* = m_2^{*(k)}n_3^{*(k)} - n_2^{*(k)}m_3^{*(k)}$.

Since, in the process of carrying out the calculations involved in Voronoi's algorithm, we have to evaluate $m_j^{*(k)}$, $n_j^{*(k)}$, $m_j^{(k)}$, $n_j^{(k)}$ ($j = 1, 2, 3$), it is not too much extra work to find $x_i^{(k)}, y_i^{(k)}, z_i^{(k)}$ ($i = 1, 2$) and then use (5.2) to find $g_1 \pmod{ab}$. By using this method to find $g_1 \pmod{ab}$, we avoid multi-precise operations, since we only require any $G_1^{(k)}$, $H_1^{(k)}$ modulo ab. The actual values of $G_1^{(k)}$ and $H_1^{(k)}$ can get very large; for example, when $D = 199109$, $G_1^{(p+1)}$ is a number of over 197000 decimal digits.

6. Computational Results. The algorithms of Sections 4 and 5 were implemented on an Amdahl 470-V7 computer and run for all $\mathcal{Q}(\sqrt[3]{D})$ with $D \leqslant 15000$. There are 12220 values of $D = ab^2$ such that D is cube-free, $(a, b) = 1$, $a < b$ and $2 \leqslant D \leqslant 15000$. Of the corresponding 12220 cubic fields investigated, it was found that 9053 have principal factors. Of the remaining 3177 fields, only 881 were such that the only prime factors of D were 3 or a prime of the form $9t \pm 1$. For these 881 fields, it was found that (1.12) was satisfied in 556 cases. Thus, 2611 of our 12220 fields are of type (i) in Section 1, 9053 are of type (ii) and 556 are of type (iii). For the quadratic case we have 7306 square-free D such that $2 \leqslant D \leqslant 15000$ and $\mathcal{Q}(\sqrt{D})$ has a principal factor and 1813 D such that $\mathcal{Q}(\sqrt{D})$ does not.

By Theorem 5.3 of [12], we know that there can be at most two elements Θ_i ($\approx \theta_i$) and Θ_j ($\approx \theta_j$) in the chain (3.2) such that $2 \leqslant i, j \leqslant p$ and $N(\Theta_i) \mid R^2$, $N(\Theta_j) \mid R^2$. That is, there can exist at most two principal factors for $\mathcal{Q}(\delta)$ that can be found as norms of relative minima of $\mathcal{S}_1$. When this occurs and $\theta_i < \theta_j$, we have

$$\varepsilon = \theta_i^3 / N(\theta_i), \qquad \varepsilon^2 = \theta_j^3 / N(\theta_j).$$

For example, when $D = 42$, we get

$$\theta_2 = 24 + 7\delta + 2\bar{\delta}, \quad \theta_3 = 254 + 73\delta + 21\bar{\delta}, \quad \theta_4 = 278 + 80\delta + 23\bar{\delta},$$

$$\theta_5 = 737 + 212\delta + 61\bar{\delta}, \quad \theta_6 = 1015 + 292\delta + 84\bar{\delta},$$

$$\theta_7 = 10077 + 2899\delta + 834\bar{\delta}, \quad \theta_8 = 21169 + 6090\delta + 1752\bar{\delta}.$$

Here, $N(\theta_2) = 6$, $N(\theta_3) = 50$, $N(\theta_4) = 20$, $N(\theta_5) = 29$, $N(\theta_6) = 7$, $N(\theta_7) = 15$, $N(\theta_8) = 1$, and we see that $i = 2, j = 6$, $\varepsilon = \theta_8 = \theta_2^3/6$, and $\varepsilon^2 = \theta_6^3/7$.

This simplifies the problem of computing ε. Certain values of D for which this must occur are given in [12]. Of the 9053 fields above which have principal factors, 8462 had two of their principal factors as norms of elements in their chain (3.2), 572 had only one of their principal factors as a norm of an element in (3.2) and only 16 had none. We list these 16 fields according to their value of D in Table 2 below.

When $D = 2$, we have $p = 1$, and therefore we cannot find a principal factor as a norm of an element in (3.2) because the period length is minimal. This is not the case, however, with the rest of these numbers; in fact, for $D = 6061$, we have $p = 972$.

On looking at Table 2, we notice that there is no D value in it such that $D \equiv \pm 1 \pmod 9$. In fact, of the 575 fields $\mathcal{Q}(\sqrt[3]{D})$ which have only one Θ_i in (3.2) such that $N(\Theta_i) \mid R^2$, only 12 have $D \equiv \pm 1 \pmod 9$. These are: 10, 325, 350, 1700, 2366, 4114, 4420, 7514, 8470, 9044, 11132, 13294. In only one case in the remaining 563 fields was the value of $N(\Theta_i)$ which divides R^2 divisible by 9. This occurs for $D = 4165$ with $N(\Theta_i) = 153$.

TABLE 2

D	Principal factor
2	3
$455 = 5 \cdot 7 \cdot 13$	$525 = 3 \cdot 5^2 \cdot 7$
$833 = 7^2 \cdot 17$	$147 = 3 \cdot 7^2$
$850 = 2 \cdot 5^2 \cdot 17$	$150 = 2 \cdot 3 \cdot 5^2$
$1078 = 2 \cdot 7^2 \cdot 11$	$294 = 2 \cdot 3 \cdot 7^2$
$1235 = 5 \cdot 13 \cdot 19$	$1425 = 3 \cdot 5^2 \cdot 19$
$1573 = 11^2 \cdot 13$	$363 = 3 \cdot 11^2$
$3857 = 7 \cdot 19 \cdot 29$	$4263 = 3 \cdot 7^2 \cdot 29$
$4901 = 13^2 \cdot 29$	$507 = 3 \cdot 13^2$
$6061 = 11 \cdot 19 \cdot 29$	$10527 = 3 \cdot 11^2 \cdot 29$
$6358 = 2 \cdot 11 \cdot 17^2$	$867 = 3 \cdot 17^2$
$8294 = 2 \cdot 11 \cdot 13 \cdot 29$	$11154 = 2 \cdot 3 \cdot 11 \cdot 13^2$
$8959 = 17^2 \cdot 31$	$867 = 3 \cdot 17^2$
$12121 = 17 \cdot 23 \cdot 31$	$19941 = 3 \cdot 17^2 \cdot 23$
$12818 = 2 \cdot 13 \cdot 17 \cdot 29$	$14703 = 3 \cdot 13^2 \cdot 29$
$14801 = 19^2 \cdot 41$	$1083 = 3 \cdot 19^2$

In [1] Barrucand and Cohn conjecture that principal factors exist except in those cases where $N(\alpha) \mid R^2$ is congruentially excluded. From this conjecture we can infer (as is done in [1]) that if $D \equiv \pm 1 \pmod 9$, $D = r_1 r_2$ or $r_1 r_2^2$, $r_1 \equiv r_2 \equiv 1 \pmod 3$, and r_1 and r_2 are primes, then a principal factor exists for $\mathfrak{Q}(\sqrt[3]{D})$ if $(r_1/r_2)_3 = (r_2/r_1)_3 = 1$. For example, if $D = 223 \cdot 7^2$, we found that 49 is a principal factor. (For the significance of this result, see [1, p. 20].) However, this conjecture is false for $D = 8299 = 43 \cdot 193$. Here $(43/193)_3 = (193/43)_3 = 1$, but we found that there is no principal factor for $\mathfrak{Q}(\sqrt[3]{8299})$. The conjecture is also false for $D = 11089 = 13 \cdot 853$ and $D = 14203 = 7 \cdot 2029$.

The conjecture is still of some interest where it applies to $D = p$, $3p$ or $9p$, where p is a prime and $p \equiv 4, 7 \pmod 9$. According to the conjecture we would expect that $N(\alpha) = 3$ is always solvable for some $\alpha \in \mathfrak{Q}[\delta]$ whenever $(3/p)_3 = 1$. That is, if $(\tau, \nu) = (0, 0), (1, 2), (2, 1)$, there exist $x_1, x_2, x_3 \in \mathfrak{Z}$ such that

$$x_1^3 + 3^\tau p x_2^3 + 3^\nu p^2 x_3^3 - 3^{(\tau+\nu+3)/3} p x_1 x_2 x_3 = 3$$

whenever $(3/p)_3 = 1$. This part of the conjecture has not been violated by any of our calculations and may well be true. However, it appears to be rather difficult to prove.

After examining the fundamental unit for a number of different fields $\mathfrak{Q}(\delta)$, M. D. Hendy (personal communication) discovered that $g_1 - 3$ was often a highly composite number. Peter Montgomery gave a partial answer to the question of why this happened by noting that principal factors existed for the fields which Hendy examined. When $\varepsilon = \alpha^3/N(\alpha)$ and $\alpha = (x_1 + x_2\delta + x_3\bar{\delta})/3$, then

$$g_1 = 3 + (abx_1x_2x_3)/N(\alpha).$$

Hence $g_1 - 3$ usually has a large number of factors. As we have seen above, $\mathbb{Q}(\sqrt[3]{D})$ has a principal factor for most of the values of $D \leqslant 15000$. However, whether this trend continues or not is unknown.

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

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

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

3. H. BRUNOTTE, J. KLINGEN & M. STEURICH, "Einige Bemerkungen zu Einheiten in reinen kubischen Körpern," *Arch. Math.*, v. 29, 1977, pp. 154–157.

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

5. F. HALTER-KOCH, "Eine Bemerkung über kubische Einheiten," *Arch. Math.*, v. 27, 1976, pp. 593–595.

6. P. MORTON, "On Redei's Theory of the Pell equation," *J. Reine Angew. Math.*, v. 307/308, 1979, pp. 373–398.

7. J. C. LAGARIAS, "On the computational complexity of determining the solvability of the equation $X^2 - DY^2 = -1$," *Trans. Amer. Math. Soc.*, v. 260, 1980, pp. 485–508.

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

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

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

11. H. C. WILLIAMS, "Improving the speed of calculating the regulator of certain pure cubic fields," *Math. Comp.*, v. 35, 1980, pp. 1423–1434.

12. H. C. WILLIAMS, "Some results concerning Voronoi's continued fraction over $\mathbb{Q}(\sqrt[3]{D})$," *Math. Comp.*, v. 36, 1981, pp. 631–652.