MATHEMATICS OF COMPUTATION
VOLUME 41, NUMBER 163
JULY 1983, PAGES 235–286

A Rapid Method of Evaluating the Regulator and Class Number of a Pure Cubic Field

By H. C. Williams*, G. W. Dueck and B. K. Schmid

Abstract. Let $\mathcal{K} = \mathcal{Q}(\theta)$ be the algebraic number field formed by adjoining θ to the rationals $\mathcal{Q}$. Let R and h be, respectively, the regulator and class number of $\mathcal{K}$. Shanks has described a method of evaluating R for $\mathcal{Q}(\sqrt{D})$, where D is a positive integer. His technique improved the speed of the usual continued fraction algorithm for finding R by allowing one to proceed almost directly from the nth to the mth step, where m is approximately $2n$, in the continued fraction expansion of $\sqrt{D}$. This paper shows how Shanks' idea can be extended to the Voronoi algorithm, which is used to find R in cubic fields of negative discriminant. It also discusses at length an algorithm for finding R and h for pure cubic fields $\mathcal{Q}(\sqrt[3]{D})$, D an integer. Under a certain generalized Riemann Hypothesis the ideas developed here will provide a new method which will find R and h in $O(D^{2/5+\epsilon})$ operations. When h is small, this is an improvement over the $O(D/h)$ operations required by Voronoi's algorithm to find R. For example, with $D = 200171999$, it required only 5 minutes for an AMDAHL $470/V7$ computer to find that $R = 518594546.969083$ and $h = 1$. This same calculation would require about 8 days of computer time if it used only the standard Voronoi algorithm.

1. Introduction. Let $\mathcal{Z}$ be the set of rational integers, and let δ be the real root of the irreducible cubic equation

$$x^3 - Bx^2 + Cx - D = 0, \tag{1.1}$$

where $B, C, D \in \mathcal{Z}$ and the discriminant Δ of (1.1) is negative. Let $\mathcal{K} = \mathcal{Q}(\delta)$ be the *cubic field* formed by adjoining δ to the rationals $\mathcal{Q}$, and let $\mathcal{Q}[\delta]$ be the ring of algebraic integers in $\mathcal{K}$. It is well known (see, for example, Delone and Faddeev [6, pp. 111–112]) that $\mathcal{Q}(\delta)$ has an integral basis $\{1, \mu, \nu\}$, where

$$\mu = \left(m_1 + m_2\delta + m_3\delta^2\right)/\sigma, \qquad \nu = \left(n_1 + n_2\delta + n_3\delta^2\right)/\sigma, \tag{1.2}$$
$$\sigma, m_1, m_2, m_3, n_1, n_2, n_3 \in \mathcal{Z}, \qquad \sigma > 0, \quad \text{and}$$
$$\gcd(m_1, m_2, m_3, n_1, n_2, n_3, \sigma) = 1.$$

Also, if $e = m_2n_3 - m_3n_2$, then $e \mid \sigma$.

If $\omega \in \mathcal{K}$, we denote its *conjugates* by ω' and ω''. We also write the *norm* of ω as $N(\omega)$ and define it as $N(\omega) = \omega\omega'\omega''$. From the simple fact that

$$N(\omega)\begin{vmatrix} 1 & 1 & 1 \\ \delta & \delta' & \delta'' \\ \delta^2 & \delta'^2 & \delta''^2 \end{vmatrix} = \begin{vmatrix} \omega & \omega' & \omega'' \\ \delta\omega & \delta'\omega' & \delta''\omega'' \\ \delta^2\omega & \delta'^2\omega' & \delta''^2\omega'' \end{vmatrix}$$

Received November 3, 1982.
1980 *Mathematics Subject Classification.* Primary 12A35, 12A45, 12A50.
*Research supported by NSERC grant number A7649.

0025-5718/83/0000-1295/$14.50

we can deduce that if $\omega = (q_1 + q_2\delta + q_3\delta^2)/q_4$, $q_i \in \mathfrak{Z}$ $(i = 1, 2, 3, 4)$, then

$$(1.3)\quad q_4^3 N(\omega) = \begin{vmatrix} q_1 & q_2 & q_3 \\ Dq_3 & q_1 - q_3C & q_2 + Bq_3 \\ Dq_2 + DBq_3 & (D - BC)q_3 - q_2C & q_1 + Bq_2 + (B^2 - C)q_3 \end{vmatrix}.$$

If $\varepsilon \in \mathfrak{Q}[\delta]$ and $|N(\varepsilon)| = 1$, we say that ε is a *unit* of $\mathfrak{K}$. In the case of the complex cubic fields which we are discussing, there exists $\varepsilon_0 \in \mathfrak{Q}[\delta]$ such that $\varepsilon_0 > 1$ and, if ε is any unit of $\mathfrak{K}$, there exists some $n \in \mathfrak{Z}$ for which $\varepsilon = \pm\varepsilon_0^n$. We call ε_0 the *fundamental unit* of $\mathfrak{K}$, and we call $R = \log \varepsilon_0$ the *regulator* of $\mathfrak{K}$. We denote the class number of $\mathfrak{K}$ by h.

When $B = C = 0$ we say that $\mathfrak{K} = \mathfrak{Q}(\sqrt[3]{D})$ is a *pure* cubic field with *radicand* D. We may assume with no loss of generality that $D = g_1 g_2^2$ and $g_1 g_2$ is square free. When $D \not\equiv \pm 1 \pmod 9$, put $\iota = 0$; in this case values of m_i, n_i, σ in (1.2) are $\sigma = g_2$, $m_1 = 0$, $m_2 = g_2$, $m_3 = 0$, $n_1 = 0$, $n_2 = 0$, $n_3 = 1$. When $D \equiv \pm 1 \pmod 9$, put $\iota = 1$; in this case values of m_i, n_i, σ in (1.2) are $\sigma = 3g_2$, $m_1 = 0$, $m_2 = 3g_2$, $m_3 = 0$, $n_1 = g_2^2$, $n_2 = \pm g_2^2$, $n_3 = 1$. Put $J = 3^{1-\iota} g_1 g_2$.

Several previous papers (see Williams [16] for references) have dealt empirically with the problem of the distribution of those values of D for which h of $\mathfrak{Q}(\sqrt[3]{D})$ has value 1. It was very difficult to continue the computations for $D > 2 \times 10^5$, because the values of the regulators, which were needed in the determination of h, were taking so long to compute. Thus, in order to continue these calculations, a faster method of evaluating R is needed. In [12] Shanks discussed a rapid technique for finding the regulator of a real quadratic field $\mathfrak{Q}(\sqrt{D})$ when D is large. His technique improves the speed of the continued fraction scheme by allowing one to proceed almost directly from the nth step to the mth step in the continued fraction, where $m \simeq 2n$.** Recently Lenstra [9] and Schoof [11] have given another version of the ideas in [12]. Both Shanks (in [19] and [13]) and Lenstra (in [9]) pointed out that it should be possible to extend Shanks' ideas to the cubic case $Q(\delta)$. In this paper we describe a means by which this can be done in the case of a pure cubic field. Instead of using the usual continued fraction that Shanks discussed, we will centre our discussion around the continued fraction algorithm of Voronoi [15]. While we have tended to restrict our discussion to the pure cubic case with $D > 10^5$, the main ideas presented here can be extended to any cubic field with negative discriminant. Indeed, Section 2 and much of Sections 3, 4 and 7 are quite general in this respect.

In Table 1 below, we summarize some of the notation used in this paper.

TABLE 1

Symbol	Description
$\mathfrak{Z}$	The set of rational integers.
B, C, D, δ	δ is the real zero of an irreducible polynomial $x^3 - Bx^2 + Cx - D$ with integer coefficients and negative discriminant.

**We use the symbol $\simeq$ to denote "approximately equal to".

TABLE 1 (*continued*)

$\mathcal{K} = \mathcal{Q}(\delta), \mathcal{Q}$	The cubic field formed by adjoining δ to the rationals $\mathcal{Q}$.
$\mathcal{O}[\delta]$	The ring of algebraic integers in $\mathcal{Q}(\delta)$.
e, σ	For any basis $\{1, \mu, \nu\}$ of $\mathcal{O}[\delta]$, we have $\mu = (m_1 + m_2\delta + m_3\delta^2)/\sigma$, $\nu = (n_1 + n_2\delta + n_3\delta^2)/\sigma$, where $m_1, m_2, m_3, n_1, n_2, n_3, \sigma \in \mathcal{Z}$, $\sigma > 0$, $\gcd(m_1, m_2, m_3, n_1, n_2, n_3, \sigma) = 1$. The values of σ and $e = m_2n_3 - n_2m_3$ are independent of the choice of basis.
ε_0	The fundamental unit of $\mathcal{K}$.
$R = \log \varepsilon_0$	The regulator of $\mathcal{K}$.
h	The class number of $\mathcal{K}$.
g_1, g_2, ι, J	When $B = C = 0$, $\mathcal{K} = \mathcal{Q}(\sqrt[3]{D})$, where $D = g_1g_2^2$, $g_1, g_2 \in \mathcal{Z}$, g_1, g_2 are square free and $\gcd(g_1, g_2) = 1$. Also $\iota = \begin{cases} 0, & D \not\equiv \pm 1 \pmod 9, \\ 1, & D \equiv \pm 1 \pmod 9, \end{cases}$ $J = 3^{1-\iota}g_1g_2$, and $\Delta = -3J^2$.
$GL_n(\mathcal{Z})$	The group of all $n \times n$ matrices with rational integer entries and determinant equal to ± 1.
$\omega, \omega', \omega''$ $N(\omega)$	If $\omega \notin \mathcal{Q}$, we say that ω', ω'' are the two conjugates of ω. $N(\omega) = \omega\omega'\omega''$. If $\omega \in \mathcal{Q}$, then $N(\omega) = \omega^3$.
Ω	$\Omega = (\omega, (\omega' - \omega'')/2i, (\omega' + \omega'')/2)$, where $i^2 + 1 = 0$. This is equivalent to writing $\Omega \approx \omega$ or $\omega \approx \Omega$.
$\mathcal{R} = \langle \lambda_1, \lambda_2, \lambda_3 \rangle$ $\gamma\mathcal{R}$ $(\gamma \in \mathcal{K})$	For $\lambda_1, \lambda_2, \lambda_3 \in \mathcal{K}$, we have $\mathcal{R} = \langle \lambda_1, \lambda_2, \lambda_3 \rangle = \{\Omega \mid \Omega \approx \omega = l_1\lambda_1 + l_2\lambda_2 + l_3\lambda_3,$ $l_1, l_2, l_3 \in \mathcal{Z}\}$. $\mathcal{R}$ has a *basis* $\{\lambda_1, \lambda_2, \lambda_3\}$. $\gamma\mathcal{R} = \langle \gamma\lambda_1, \gamma\lambda_2, \gamma\lambda_3 \rangle$. If $\mathcal{R} = \langle 1, \mu, \nu \rangle$, $\mu, \nu \in \mathcal{K}$, we say that $\mathcal{R}$ is a 1-*lattice*
f, ρ	If $\mathcal{R}$ is a 1-lattice $\langle 1, \mu, \nu \rangle$ with $\mu = (m_1 + m_2\delta + m_3\delta^2)/\rho$, $\nu = (n_1 + n_2\delta + n_3\delta^2)/\rho$, where $m_1, m_2, m_3, n_1, n_2, n_3, \rho \in \mathcal{Z}$, $\rho > 0$, $\gcd(m_1, m_2, m_3, n_1, n_2, n_3, \rho) = 1$, then the values of ρ and $f = m_2n_3 - m_3n_2$ are independent of the basis selected for $\mathcal{R}$.
$\mathcal{C}, \mathcal{C}_1$	$\mathcal{C} = \{(x, y, z) \mid y^2 + z^2 \leqslant 1, (x, y, z) \in \mathcal{E}_3\}$, $\mathcal{C}_1 = \{(x, y, z) \mid \mid x \mid \leqslant 1, y^2 + z^2 \leqslant 1, (x, y, z) \in \mathcal{E}_3\}$; here $\mathcal{E}_3$ is Euclidean 3-space.
θ_g, Θ_g	Θ_g $(\approx \theta_g)$ is the relative minimum adjacent to $(1, 0, 1)$ in a reduced lattice $\mathcal{R}$.

TABLE 1 (*continued*)

$\mathfrak{R}_n$, e_n, σ_n, $\theta_g^{(n)}$	$\mathfrak{R}_1 = \langle 1, \bar{\mu}, \bar{\nu}\rangle$, where $\{1, \bar{\mu}, \bar{\nu}\}$ is any basis of $\mathfrak{Q}[\delta]$. $\theta_g^{(n)}$ is θ_g, σ_n is ρ and e_n is f for $\mathfrak{R}_n$, where $\mathfrak{R}_{j+1} = (1/\theta_g^{(j)})\mathfrak{R}_j$ $(j = 1, 2, 3, \ldots)$.
R_n, θ_n	$\theta_n = \prod_{i=1}^{n-1}\theta_g^{(i)}$, $R_n = \log \theta_n$.
$\mathfrak{R} \sim \mathfrak{S}$	$\mathfrak{R} \sim \mathfrak{S}$ if $\mathfrak{R}$ and $\mathfrak{S}$ are 1-lattices and $\mathfrak{R} = \gamma\mathfrak{S}$, $\gamma \in \mathfrak{K}$.
$F(Q)$, E	$F(Q) = \prod_{q \le Q} f(q)$, where the product is taken over all primes $q < Q$ where $q \equiv 1 \pmod 3$ (see Section 3). $E = \sqrt{3}\, c_2 J F(Q)/2\pi$.
c, d_i, d_i', d_i''	c is a solution of $\begin{cases} x^2 \equiv D \pmod{\sigma^2}, \\ 3x^2 \equiv 0 \pmod{\sigma}. \end{cases}$ If p is a prime, d_i (d_i', d_i'') is (are) solution(s) of $\begin{cases} x^3 \equiv D \pmod{\sigma^2 p^t}, \\ x \equiv c \pmod{\sigma} \end{cases}$ such that none of d_i, d_i', d_i'' satisfies $x^3 \equiv D \pmod{\sigma^2 p^{t+1}}$.
P, P', P'', r, s, s', $L(\mathfrak{a})$	If $\mathfrak{a}$ is any ideal of $\mathfrak{Q}[\delta]$ ($\delta = \sqrt[3]{D}$), and $\mathfrak{a}$ has no rational integer divisor, then $\mathfrak{a}$ has a basis of the form $\{P, P'(r + \delta), P''(s + s'\delta + \delta^2)/\sigma\}$, where P, P', P'', r, s, $s' \in \mathfrak{Z}$, $P'P'' \mid P$, $P'' \mid \sigma$ and (5.5) holds. $L(\mathfrak{a}) = P$.
m, n, n'	A *canonical* basis of $\mathfrak{R}$ $(\sim \mathfrak{R}_1)$ has the form $\{1, \lvert f\rvert (m + \delta)/\rho, (n + n'\delta + \delta^2)/\rho\}$, where m, n, $n' \in \mathfrak{Z}$. Also, if $\mathfrak{a}$ above is the ideal to to which $\mathfrak{R}$ corresponds, then $\rho = \sigma P/P''$, $f = \sigma P'/P''$, $P'' = \sigma/\gcd(\sigma, f)$, $m \equiv r \pmod{\rho/f}$, $n' \equiv s \pmod f$, $n \equiv s + r(n' - s) \pmod\rho$.
$\omega_p = (\xi_\omega, \eta_\omega)$ ζ_ω	If $\Omega \in \mathfrak{R}$ and $\Omega \approx \omega$, then $\xi_\omega = (2\omega - \omega' - \omega'')/2$, $\eta_\omega = (\omega' - \omega'')/2i$, $\zeta_\omega = (\omega' + \omega'')/2$. When $\mathfrak{K} = \mathfrak{Q}(\sqrt[3]{D})$ and $\omega = (q_1 + q_2\delta + q_3\delta^2)/\rho$, $q_1, q_2, q_3 \in \mathfrak{Z}$, then $\xi_\omega = 3\delta(q_2 + q_3\delta)/2\rho$, $\eta_\omega = \sqrt{3}\,\delta(q_2 - q_3\delta)/2\rho$, $\zeta_\omega = (2q_1 - \delta q_2 - \delta^2 q_3)/2\rho$.
Γ_g $(\approx \gamma_g)$, γ_h	Γ_g is a point of a 1-lattice $\mathfrak{R}$ $(\sim \mathfrak{R}_1)$ such that $\Gamma_g \in \mathfrak{C}_1$ and $\lvert\gamma_g\rvert \ne 1$. Further, γ_h is any element of $\mathfrak{R}$ such that $\mathfrak{R} = \langle 1, \gamma_g, \gamma_h\rangle$.
β	$\beta = 3.002\,\delta^2$.

TABLE 1 (*continued*)

$x_\omega, y_\omega, \bar{x}_\omega, \bar{y}_\omega,$ X_ω, Y_ω	For $\Omega\,(\approx \omega) \in \mathfrak{R}$, $\mathfrak{R} \sim \mathfrak{R}_1$, $\delta = \sqrt[3]{D}$, $\omega = (q_1 + q_2\delta + q_3\delta^2)/\rho$, we define $x_\omega = q_2 I_1 + [I_1\delta]q_3, y_\omega = q_2 I_1 - [I_1\delta]q_3$, $\bar{x}_\omega = [3\delta I_2]q_2 + [3\delta^2 I_2]q_3, \bar{y}_\omega = [\sqrt{3}\,\delta I_2]q_2 - [\sqrt{3}\,\delta^2 I_2]q_3$, $X_\omega = [\delta I_3]q_2 + [\delta^2 I_3]q_3$, $Y_\omega = [\delta I_3]q_3 - [\delta^2 I_3]q_3$, where $I_1, I_2, I_3 \in \mathfrak{Z}$, $I_1 > 3.1(4\beta)^3/\delta$, $I_2 > 2(3\beta)^3/\sqrt{3}\,\delta$, $I_3 > 489\beta\sqrt{D}$.
$K_1(a, b)$, $K_2(a, b)$, $K_3(a, b)$	$K_1(a, b) = \left(\begin{smallmatrix} a & 1 \\ b & 0 \end{smallmatrix}\right)$, $K_2(a, b) = \left(\begin{smallmatrix} 1 & a \\ 0 & b \end{smallmatrix}\right)$, $K_3(a, b) = \left(\begin{smallmatrix} 0 & a \\ 1 & b \end{smallmatrix}\right)$.

2. Ideals and Lattices. In this section, we give a brief discussion of some of the elementary properties of the ideals of $\mathfrak{Q}[\delta]$ and the lattices over $\mathfrak{Q}(\delta)$. For a more detailed description of these ideas we refer the reader to [6].

Let $\lambda_1, \lambda_2, \lambda_3 \in \mathfrak{Q}(\delta)$ such that

$$\sum_{i=1}^{3} l_i\lambda_i = 0 \qquad (l_1, l_2, l_3 \in \mathfrak{Z})$$

if and only if $l_1 = l_2 = l_3 = 0$. We say that $\mathfrak{O} = \{(\omega, \omega', \omega'') \mid \omega = l_1\lambda_1 + l_2\lambda_2 + l_3\lambda_3;\ l_1, l_2, l_3 \in \mathfrak{Z}\}$ is a *lattice* over $\mathfrak{Q}(\delta)$ with *basis* $\{\lambda_1, \lambda_2, \lambda_3\}$. Since we are dealing here with cubic fields with negative discriminant, we see that ω' and ω'' are complex. In order to work in real lattices, we use

$$\mathfrak{R} = \{\Omega = (\omega, (\omega' - \omega'')/2i, (\omega' + \omega'')/2) \mid \omega = l_1\lambda_1 + l_2\lambda_2 + l_3\lambda_3;\ l_1, l_2, l_3 \in \mathfrak{Z}\}, \tag{2.1}$$

where i is a fixed zero of $x^2 + 1$. Since Ω is uniquely determined by ω, we often identify Ω with ω and write $\Omega \approx \omega$ or $\omega \approx \Omega$. $\mathfrak{R}$ is completely characterized by $\lambda_1, \lambda_2, \lambda_3$. We say that $\{\lambda_1, \lambda_2, \lambda_3\}$ is a *basis* of $\mathfrak{R}$, and we write $\mathfrak{R} = \langle\lambda_1, \lambda_2, \lambda_3\rangle$. Throughout this paper, we shall be restricting our attention to lattices of type $\mathfrak{R}$ over $\mathfrak{Q}(\delta)$ which have a basis of the form $\{1, \lambda_2, \lambda_3\}$. We will call such a lattice a 1-lattice. We also note [6, p. 274] that if $\Omega\,(\approx \omega), \Phi\,(\approx \phi) \in \mathfrak{R}$ such that $\omega'\omega'' = \phi'\phi''$, then $\omega = \pm\phi$. Further,

$$|\omega'|^2 = |\omega''|^2 = \omega'\omega'' = \left(\frac{\omega' - \omega''}{2i}\right)^2 + \left(\frac{\omega' + \omega''}{2}\right)^2. \tag{2.2}$$

Let $GL_n(\mathfrak{Z})$ be the group of all $n \times n$ matrices T such that T has entries from $\mathfrak{Z}$ only and $|T| = \pm 1$. If $\mathfrak{R} = \langle\lambda_1, \lambda_2, \lambda_3\rangle$ and $\mathfrak{R}^* = \langle\mu_1, \mu_2, \mu_3\rangle$, then $\mathfrak{R} = \mathfrak{R}^*$ if and only if

$$\begin{pmatrix} \mu_1 \\ \mu_2 \\ \mu_3 \end{pmatrix} = T \begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \lambda_3 \end{pmatrix}, \tag{2.3}$$

where $T \in GL_3(\mathfrak{Z})$. If $\mathfrak{R} = \langle \lambda_1, \lambda_2, \lambda_3 \rangle$ and $\gamma\ (\neq 0) \in \mathfrak{K}$, we define $\gamma\mathfrak{R}$ to be the lattice $\langle \gamma\lambda_1, \gamma\lambda_2, \gamma\lambda_3 \rangle$. If

$$\gamma \begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \lambda_3 \end{pmatrix} = T \begin{pmatrix} 1 \\ \mu_1 \\ \mu_2 \end{pmatrix}, \tag{2.4}$$

where $T \in GL_3(\mathfrak{Z})$, then $\mathfrak{R}^* = \langle \gamma\lambda_1, \gamma\lambda_2, \gamma\lambda_3 \rangle$ is a 1-lattice. If $\mathfrak{R}$ and $\mathfrak{R}^*$ are both 1-lattices and $\mathfrak{R}^* = \gamma\mathfrak{R}$, we say that $\mathfrak{R}$ and $\mathfrak{R}^*$ are *similar* and write this as $\mathfrak{R} \sim \mathfrak{R}^*$. Since both $\mathfrak{R}$ and $\mathfrak{R}^*$ are 1-lattices, this relationship is clearly an equivalence relationship.

Let $\mathfrak{a} \neq 0$ be any ideal of $\mathfrak{Z}[\delta]$; then $\mathfrak{a}$ can be written as

$$\begin{aligned} \mathfrak{a} &= [\kappa_1, \kappa_2, \kappa_3, \ldots, \kappa_n] \\ &= \left\{ \sum_{i=1}^{n} \eta_i \kappa_i \mid \eta_i \in \mathfrak{Z}[\delta],\ i = 1, 2, 3, \ldots, n \right\}, \end{aligned}$$

where the κ_i's are *generators* of $\mathfrak{a}$ and $\kappa_i \in \mathfrak{Z}[\delta]$ $(i = 1, 2, 3, \ldots, n)$. Also there exist $\nu_1, \nu_2, \nu_3 \in \mathfrak{Z}[\delta]$ such that

$$\mathfrak{a} = \left\{ \sum_{i=1}^{3} l_i \nu_i \mid l_1, l_2, l_3 \in \mathfrak{Z} \right\}.$$

This set $\{\nu_1, \nu_2, \nu_3\}$ is said to be a *basis* of $\mathfrak{a}$. If $\mathfrak{a}$ has another basis $\{\tau_1, \tau_2, \tau_3\}$, then

$$\begin{pmatrix} \tau_1 \\ \tau_2 \\ \tau_3 \end{pmatrix} = T \begin{pmatrix} \nu_1 \\ \nu_2 \\ \nu_3 \end{pmatrix}, \tag{2.5}$$

where $T \in GL_3(\mathfrak{Z})$. Since $\nu_i, \tau_i \in \mathfrak{Z}[\delta]$ $(i = 1, 2, 3)$, by (1.2) we must have

$$\sigma \begin{pmatrix} \nu_1 \\ \nu_2 \\ \nu_3 \end{pmatrix} = M_1 \begin{pmatrix} 1 \\ \delta \\ \delta^2 \end{pmatrix}, \qquad \sigma \begin{pmatrix} \tau_1 \\ \tau_2 \\ \tau_3 \end{pmatrix} = M_2 \begin{pmatrix} 1 \\ \delta \\ \delta^2 \end{pmatrix},$$

where M_1 and M_2 are 3×3 matrices with rational integer entries. Since $1, \delta, \delta^2$ are independent over $\mathfrak{Z}$, we see that

$$M_2 = TM_1. \tag{2.6}$$

We also point out that, if the ideal $\mathfrak{a}$ has the basis $\{\nu_1, \nu_2, \nu_3\}$ and

$$\phi \begin{pmatrix} \nu_1 \\ \nu_2 \\ \nu_3 \end{pmatrix} = \psi T \begin{pmatrix} \tau_1 \\ \tau_2 \\ \tau_3 \end{pmatrix}, \tag{2.7}$$

where $\phi \in [\tau_1, \tau_2, \tau_3] = \mathfrak{b}$, $\psi \in \mathfrak{a}$, and $T \in GL_3(\mathfrak{Z})$, then $\{\tau_1, \tau_2, \tau_3\}$ is a basis of $\mathfrak{b}$. We say that two ideals $\mathfrak{a}$ and $\mathfrak{b}$ are equivalent, written $\mathfrak{a} \sim \mathfrak{b}$, when there exists two nonzero principal ideals $[\alpha]$, $[\beta]$ such that $[\alpha]\mathfrak{a} = [\beta]\mathfrak{b}$. Thus, if (2.7) is true, we see that $\mathfrak{a} \sim \mathfrak{b}$.

If $\{\omega_1, \omega_2, \omega_3\}$ is any basis of $\mathfrak{Z}[\delta]$, we know (see, for example, Landau [8, p. 117]) that any ideal $\mathfrak{a}$ of $\mathfrak{Z}[\delta]$ has a basis $\{\alpha_1, \alpha_2, \alpha_3\}$, where

$$\alpha_1 = a_{11}\omega_1, \quad \alpha_2 = a_{21}\omega_1 + a_{22}\omega_2, \quad \alpha_3 = a_{31}\omega_1 + a_{32}\omega_2 + a_{33}\omega_3.$$

Here all $a_{ij} \in \mathfrak{Z}$, and $a_{11}, a_{22}, a_{33} > 0$. Since $\mathfrak{D}[\delta]$ has a basis with $\omega_1 = 1$, we can assume that $\mathfrak{a}$ has a basis $\{\alpha_1, \alpha_2, \alpha_3\}$, where $\alpha_1 > 0$ and $\alpha_1 \in \mathfrak{Z}$. We define $L(\mathfrak{a})$ to be α_1. Furthermore, by (2.5) and the fact that $1, \omega_2, \omega_3$ must be independent over $\mathfrak{Z}$, we see that there is only one possible value of such an α_1 for any ideal $\mathfrak{a}$. In fact it is the least positive rational integer in $\mathfrak{a}$. If we let $N(\mathfrak{a})$ denote the norm of $\mathfrak{a}$, then $N(\mathfrak{a}) = a_{11}a_{22}a_{33}$, and we see that $L(\mathfrak{a}) \mid N(\mathfrak{a})$.

If we put $\mathfrak{R} = \langle 1, \alpha_2/\alpha_1, \alpha_3/\alpha_1 \rangle$, we say that $\mathfrak{R}$ is the 1-lattice which *corresponds* to the ideal $\mathfrak{a}$. In view of the above remarks there can only be one such 1-lattice. Notice that if $\mathfrak{R}$ is a 1-lattice which corresponds to $\mathfrak{a}$ and $\mathfrak{a} = [m]\mathfrak{b}$, where $m \in \mathfrak{Z}$ and $\mathfrak{b}$ is an ideal of $\mathfrak{D}[\delta]$, then $\mathfrak{R}$ also corresponds to $\mathfrak{b}$.

From the above definitions and results, it is clear that if $\mathfrak{R}$ is a 1-lattice which corresponds to an ideal $\mathfrak{a}$ and $\mathfrak{R}^*$ is a 1-lattice which corresponds to an ideal $\mathfrak{b}$, then $\mathfrak{a} \sim \mathfrak{b}$ if and only if $\mathfrak{R} \sim \mathfrak{R}^*$. We can be more specific about this in

LEMMA 2.1. *Let $\mathfrak{R}$ be a 1-lattice which corresponds to the ideal $\mathfrak{a}$ and let $\mathfrak{R}^*$ be a 1-lattice which corresponds to the ideal $\mathfrak{b}$. If $\mathfrak{R} = \gamma\mathfrak{R}^*$, then*

$$[L(\mathfrak{b})]\mathfrak{a} = [L(\mathfrak{a})\gamma]\mathfrak{b}.$$

If $\mathfrak{a} \sim \mathfrak{b}$ and $[\phi]\mathfrak{a} = [\psi]\mathfrak{b}$, where $\phi, \psi \in \mathfrak{D}[\delta]$, then

$$\mathfrak{R} = \gamma\mathfrak{R}^*,$$

where $\gamma = L(\mathfrak{b})\psi/L(\mathfrak{a})\phi$.

Proof. Follows easily from (2.3), (2.4), and (2.5). □

We also have

LEMMA 2.2. *Let $\mathfrak{R}$ and $\mathfrak{R}^*$ be 1-lattices. If $\mathfrak{R}$ corresponds to the ideal $\mathfrak{a}$ and $\mathfrak{R} \sim \mathfrak{R}^*$, then there exists an ideal $\mathfrak{b}$ such that $\mathfrak{R}^*$ corresponds to $\mathfrak{b}$.*

Proof. Since $\mathfrak{R} \sim \mathfrak{R}^*$, we have $\mathfrak{R} = \gamma\mathfrak{R}^*$, and $\Gamma\ (\approx \gamma) \in \mathfrak{R}$. Let $\mathfrak{a} = [\alpha_1, \alpha_2, \alpha_3]$, where $\{\alpha_1, \alpha_2, \alpha_3\}$ is a basis of $\mathfrak{a}$ and $\alpha_1 = L(\mathfrak{a})$. Then $\mathfrak{R} = \langle 1, \alpha_2/\alpha_1, \alpha_3/\alpha_1 \rangle$, and $\mathfrak{R}^* = \langle \gamma^{-1}, \gamma^{-1}\alpha_2/\alpha_1, \gamma^{-1}\alpha_3/\alpha_1 \rangle$. Now $\mathfrak{R}^* = \langle 1, \kappa_1, \kappa_2 \rangle$, $\kappa_1, \kappa_2 \in \mathfrak{K}$; thus, if we let $\kappa_1 = \mu_1/m$, $\kappa_2 = \mu_2/m$, where $m \in \mathfrak{Z}$ and $\mu_1, \mu_2 \in \mathfrak{D}[\delta]$, we have, by (2.3),

$$m\begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \end{pmatrix} = \alpha_1\gamma T\begin{pmatrix} m \\ \mu_1 \\ \mu_2 \end{pmatrix},$$

where $T \in GL_3(\mathfrak{Z})$. Since $\Gamma \in \mathfrak{R}$, it follows that $\alpha_1\gamma \in \mathfrak{a}$; hence, $\mathfrak{b} = \{ml_1 + \mu_1 l_2 + \mu_2 l_3 \mid l_1, l_2, l_3 \in \mathfrak{Z}\}$ is an ideal of $\mathfrak{D}[\delta]$, and $\mathfrak{R}^*$ corresponds to $\mathfrak{b}$. □

We conclude this section with a consequence of the following important definition.

Definition. Let $\mathfrak{S}_1$ and $\mathfrak{S}_2$ be 1-lattices, and suppose that $\mathfrak{S}_1$ corresponds to the ideal $\mathfrak{a}_1$ and $\mathfrak{S}_2$ corresponds to the ideal $\mathfrak{a}_2$. We define the lattice $\mathfrak{S}_1\mathfrak{S}_2$ to be the 1-lattice which corresponds to the ideal $\mathfrak{a}_1\mathfrak{a}_2$.

From this definition and Lemmas 2.1 and 2.2, it follows that, if $\mathfrak{S}_i$ $(i = 1, 2, 3, 4)$ are 1-lattices, $\mathfrak{S}_i$ corresponds to the ideal $\mathfrak{a}_i$ $(i = 1, 2)$ and $\mathfrak{S}_1 \sim \mathfrak{S}_3$, $\mathfrak{S}_2 \sim \mathfrak{S}_4$, then $\mathfrak{S}_1\mathfrak{S}_2 \sim \mathfrak{S}_3\mathfrak{S}_4$.

3. Outline of the Method. In this section, we will sketch the overall method which we will use to determine $\mathfrak{R}$ and h for $\mathfrak{Q}(\delta)$. We first require some further results concerning 1-lattices.

Let $\mathfrak{R}$ be a lattice as given by (2.1), and let $\Omega\ (\approx \omega) \in \mathfrak{R}$. We define the *normed body* of Ω, written $\mathfrak{N}(\Omega)$, to be

$$\mathfrak{N}(\Omega) = \{(x, y, z) \mid (x, y, z) \in \mathfrak{E}_3, |x| \leqslant |\omega|, y^2 + z^2 \leqslant \omega'\omega''\},$$

where $\mathfrak{E}_3$ is Euclidean 3-space. We say that $\Omega\ (\neq (0,0,0))$ is a *relative minimum* of $\mathfrak{R}$ if

$$\mathfrak{N}(\Omega) \cap \mathfrak{R} = \{(0,0,0), \Omega, -\Omega\}.$$

If $\Omega\ (\approx \omega)$ and $\Phi\ (\approx \phi)$ are relative minima of $\mathfrak{R}$ such that

$$0 < \phi < \omega, \qquad \phi'\phi'' > \omega'\omega'',$$

and there does not exist a $\Psi\ (\approx \psi) \in \mathfrak{R}$ such that

$$\phi < \psi < \omega, \qquad \psi'\psi'' < \phi'\phi'',$$

we call Ω the relative minimum *adjacent* to Φ. (Actually Voronoi [15] used the term relative minimum of the second kind adjacent to Φ.)

LEMMA 3.1 (VORONOI [15, Sections 21, 22]). *Let $\mathfrak{R}$ be a 1-lattice in which the point $(1,0,1)$ is a relative minimum, and let $\Theta\ (\approx \theta)$ be the relative minimum adjacent to $(1,0,1)$ in $\mathfrak{R}$. Then there exists $\Psi\ (\approx \psi) \in \mathfrak{R}$ such that $\mathfrak{R} = \langle 1, \theta, \psi \rangle$.*

Proof. Let $\mathfrak{R} = \langle 1, \lambda_2, \lambda_3 \rangle$, $\theta = a + b\lambda_2 + c\lambda_3$ $(a, b, c \in \mathfrak{Z})$, $d = \gcd(b, c)$. If $d > 1$, find r such that $r \equiv a \pmod{d}$ and $|r| \leqslant d/2$. Put $\phi = |(r - \theta)/d|$. Clearly, there exists $\Phi \in \mathfrak{R}$ such that $\Phi \approx \phi$. Also, $0 < \phi < |r/d| + |\theta/d| \leqslant 1/2 + \theta/2 < \theta$ and $|\phi'| \leqslant |r/d| + |\theta'/d| \leqslant 1/2 + |\theta'/2| < 1$. As this contradicts the definition of θ, we must have $d = 1$. Since $\gcd(b, c) = 1$, there exist $y, z \in \mathfrak{Z}$ such that $bz - yc = 1$. Putting $\psi = x + y\lambda_2 + z\lambda_3$ for any $x \in \mathfrak{Z}$, we see that

$$\begin{pmatrix} 1 \\ \theta \\ \psi \end{pmatrix} = T \begin{pmatrix} 1 \\ \lambda_2 \\ \lambda_3 \end{pmatrix},$$

where

$$T = \begin{pmatrix} 1 & 0 & 0 \\ a & b & c \\ x & y & z \end{pmatrix} \quad \text{and} \quad T \in GL_3(\mathfrak{Z}).$$

Hence $\{1, \theta, \psi\}$ is a basis of $\mathfrak{R}$. □

We call a 1-lattice in which $(1,0,1)$ is a relative minimum a *reduced* lattice, and we call a basis of the type $\{1, \theta, \psi\}$ in Lemma 3.1 a *reduced basis*.

Let $\mathfrak{a}$ be a primitive ideal (an ideal with no rational integer divisors). We say that $\mathfrak{a}$ is a *reduced* ideal if and only if there does not exist $\alpha \in \mathfrak{a}$ such that both $|\alpha| < L(\mathfrak{a})$ and $|\alpha'| < L(\mathfrak{a})$ hold. (This is essentially the idea of Berwick [2, pp. 418–419] and [3].) It can be easily deduced from the results in [15, Section 39] that

$$L(\mathfrak{a}) < \sqrt{|\Delta|/3}$$

when $\mathfrak{a}$ is reduced. Note that $\mathfrak{a}$ is reduced if and only if its corresponding lattice is reduced.

If $\mathfrak{R}_1$ is the lattice which has as a basis an integral basis of $\mathfrak{Q}[\delta]$, then $\mathfrak{R}_1$ is a reduced lattice, because $(1, 0, 1)$ must be a relative minimum in such a lattice. Let $\mathfrak{R}$ be any reduced lattice, and consider the sequence

$$\Theta_1 = (1, 0, 1), \Theta_2, \Theta_3, \ldots, \Theta_n, \ldots, \tag{3.1}$$

where Θ_{i+1} is the relative minimum adjacent to Θ_i for $i = 1, 2, 3, \ldots, n, \ldots$. We call this sequence the *chain* of relative minima of $\mathfrak{R}$. We know (see [6] or [18]) that such a chain will be of infinite extent. Also, if $\theta_n \approx \Theta_n$, then $\theta_1 < \theta_2 < \theta_3 < \cdots < \theta_n < \cdots$. Hence, if Φ $(\approx \phi)$ is a relative minimum of $\mathfrak{R}$ with $\phi > 1$, then $\Phi = \Theta_k$ for some $k \geqslant 2$.

If ε (> 1) is any unit of $\mathfrak{R}_1$, we see that, since $N(\varepsilon) = 1$, we must have E $(\approx \varepsilon)$ a relative minimum of $\mathfrak{R}_1$, and therefore $E = \Theta_k$ in the chain (3.1) in $\mathfrak{R}_1$. Thus, if we can find the chain (3.1) in $\mathfrak{R}_1$, we should be able to find ε_0. In [15] Voronoi described how to find the relative minimum adjacent to $(1, 0, 1)$ in a *reduced lattice*. A version of this algorithm suitable for computers is described at some length in Williams, Cormack and Seah [18]. This solves the problem of finding the elements of (3.1). For, we find $\theta_g^{(1)} = \theta_2$ by using Voronoi's algorithm and embed 1, $\theta_g^{(1)}$ in a reduced basis $\{1, \theta_g^{(1)}, \theta_h^{(1)}\}$ of $\mathfrak{R}_1$. Let $\mathfrak{R}_2 = \langle 1, 1/\theta_g^{(1)}, \theta_h^{(1)}/\theta_g^{(1)} \rangle$. Clearly $\mathfrak{R}_2$ is a reduced lattice, and we find $\theta_g^{(2)}$, the relative minimum adjacent to 1 in $\mathfrak{R}_2$. We have $\theta_3 = \theta_g^{(1)}\theta_g^{(2)}$. If $\{1, \theta_g^{(n)}, \theta_h^{(n)}\}$ is a reduced basis of $\mathfrak{R}_n$, then define $\mathfrak{R}_{n+1}$ by

$$\mathfrak{R}_{n+1} = \left\langle 1, 1/\theta_g^{(n)}, \theta_h^{(n)}/\theta_g^{(n)} \right\rangle$$

and continue the process by finding $\theta_g^{(n+1)}$, the relative minimum adjacent to $(1, 0, 1)$ in the reduced lattice $\mathfrak{R}_{n+1}$. We have

$$\theta_{n+2} = \theta_g^{(1)}\theta_g^{(2)} \cdots \theta_g^{(n+1)}.$$

Hence

$$\varepsilon_0 = \theta_k = \prod_{i=1}^{k-1} \theta_g^{(i)}$$

and

$$R = \log \varepsilon_0 = \sum_{i=1}^{k-1} \log \theta_g^{(i)}.$$

Also, $\mathfrak{R}_1 = \theta_n \mathfrak{R}_n$; hence, $\mathfrak{R}_n \sim \mathfrak{R}_1$. We further point out that if $\varepsilon_0 = \theta_k$, then $\mathfrak{R}_{k-1+m} = \mathfrak{R}_m$, $\mathfrak{R}_{s(k-1)+m} = \mathfrak{R}_m$ and $\theta_{(k-1)s+m} = \varepsilon_0^s \theta_m$.

What we now wish to do is to find, as Shanks did in the case of $\mathfrak{Q}(\sqrt{D})$, a method of getting θ_m, where θ_m is close to θ_n^2, when we know θ_n. In order to do this, we first require two results which are due essentially to Voronoi [15, Section 39]. As we will often have need of $\mathfrak{N}(1, 0, 1)$, we will denote it by $\mathcal{C}_1$. We also denote the set of points $\{(x, y, z) | (x, y, z) \in \mathfrak{E}_3, y^2 + z^2 \leqslant 1\}$ by $\mathcal{C}$.

THEOREM 3.2. *Let $\mathfrak{R}$ be any 1-lattice. There exists a reduced lattice $\mathfrak{R}^*$ such that $\mathfrak{R}^* \sim \mathfrak{R}$. Further, there exists Γ $(\approx \gamma) \in \mathfrak{R}$ such that $\gamma\mathfrak{R}^* = \mathfrak{R}$ and $0 < \gamma \leqslant 1$, $|\gamma'| \leqslant 1$.*

Proof. Let $\mathfrak{R} = \langle 1, \lambda_2, \lambda_3 \rangle$. If $(1, 0, 1)$ is a relative minimum of $\mathfrak{R}$, we are finished. If $(1, 0, 1)$ is not a relative minimum of $\mathfrak{R}$, then there must be a P $(\approx \rho) \in \mathfrak{R}$ such that

$$\rho \neq 0, \quad |\rho| < 1, \quad |\rho'| < 1. \tag{3.2}$$

Since any such ρ must be of the form $\rho = a + b\lambda_2 + c\lambda_3$, where $a, b, c \in \mathfrak{Z}$, there can only be a finite number of points P $(\approx \rho) \in \mathfrak{R}$ which satisfy (3.2). Let this number be n.

If $d = \gcd(b, c)$ and $d > 1$, let $\theta = (\rho - r)/d$, where $|r| \leqslant d/2$ and $r \equiv a \pmod{d}$. We have $\theta \neq 0$, $|\theta| \leqslant |\rho/d| + |r/d| \leqslant 1$, $|\theta'| \leqslant |\rho'/d| + |r/d| < 1$, and $\theta = (a - r)/d + (b/d)\lambda_1 + (c/d)\lambda_2$. Thus we may assume with no loss of generality that we can select a fixed Θ $(\approx \theta)$ of $\mathfrak{R}$ such that

$$\theta \neq 0, \quad |\theta| < 1, \quad |\theta'| < 1, \tag{3.3}$$

and

$$\theta = a + b\lambda_1 + c\lambda_2 \quad \text{with } \gcd(b, c) = 1.$$

By using the argument of Lemma 3.1, we see that we can embed θ in a basis of $\mathfrak{R}$. In fact, let $\mathfrak{R} = \langle 1, \theta, \psi \rangle$, and let $\mathfrak{R}' = (1/\theta)\mathfrak{R}$. Then $\mathfrak{R}'$ is a 1-lattice and $\mathfrak{R}' \sim \mathfrak{R}$. If $\mathfrak{R}'$ is a reduced lattice, $\gamma = |\theta|$ and we are finished; if $\mathfrak{R}'$ is not a reduced lattice, there must exist Φ $(\approx \phi) \in \mathfrak{R}'$ such that

$$\phi \neq 0, \quad |\phi| < 1, \quad |\phi'| < 1. \tag{3.4}$$

Again, there can only be a finite number of such elements in $\mathfrak{R}'$, and we denote this number by m. If Φ is any such element, then

$$\phi = l_1/\theta + l_2 + l_3\psi/\theta, \quad \text{where } l_1, l_2, l_3 \in \mathfrak{Z};$$

hence, X $(\approx \chi = \theta\phi = l_1 + l_2\theta + l_3\psi)$ is an element of $\mathfrak{R}$ and $\chi \neq 0$, $|\chi| = |\theta\phi| < 1$, $|\chi'| = |\theta'\phi'| < 1$ by (3.3) and (3.4). It follows that $m \leqslant n$. Since, however, $\phi\theta \neq \theta$, we see that $m \neq n$; thus, $m < n$. We can then repeat the above argument on $\mathfrak{R}'$ instead of $\mathfrak{R}$. Since, in each new 1-lattice $\mathfrak{R}^{(j)}$ $(\sim \mathfrak{R}^{(j-1)})$ that we develop, we have fewer and fewer elements P $(\approx \rho)$ such that (3.2) holds, we must eventually reach the point where we have a $\mathfrak{R}^{(k)}$ such that $\mathfrak{R}^{(k)}$ is reduced. The result of the theorem follows on putting $\mathfrak{R}^* = \mathfrak{R}^{(k)}$ and noting that $\mathfrak{R}^{(k)} \sim \mathfrak{R}$. □

COROLLARY. *If* $\mathfrak{a}$ *is any primitive ideal of* $\mathfrak{Q}[\delta]$, *there exists* $\lambda \in \mathfrak{a}$ *and a reduced ideal* $\mathfrak{b}$ *of* $\mathfrak{Q}[\delta]$ *such that*

$$[\lambda]\mathfrak{b} = [L(\mathfrak{b})]\mathfrak{a}$$

and

$$L(\mathfrak{a})^{-1} \leqslant \lambda \leqslant L(\mathfrak{a}), \qquad 1 \leqslant |\lambda'| \leqslant L(\mathfrak{a}).$$

Proof. By the theorem there exists Γ $(\approx \gamma) \in \mathfrak{R}$ and a reduced lattice $\mathfrak{R}^*$ such that $\gamma\mathfrak{R}^* = \mathfrak{R}$, $0 < \gamma \leqslant 1$, $|\gamma'| \leqslant 1$. By Lemma 2.2 there exists an ideal $\mathfrak{b}$ of $\mathfrak{Q}[\delta]$ such that $\mathfrak{R}^*$ corresponds to $\mathfrak{b}$. By Lemma 2.1

$$[L(\mathfrak{b})]\mathfrak{a} = [L(\mathfrak{a})\gamma]\mathfrak{b}.$$

Put $\lambda = L(\mathfrak{a})\gamma \in \mathfrak{a}$. We must have $0 < \lambda \leqslant L(\mathfrak{a})$, $|\lambda'| \leqslant L(\mathfrak{a})$. Since $\lambda \in \mathfrak{a}$, we have $\lambda \equiv 0 \pmod{\mathfrak{a}}$ and $N(\mathfrak{a}) | N(\lambda)$. Thus $N(\lambda) = \lambda|\lambda'|^2 \geqslant N(\mathfrak{a})$, and

$$\lambda = N(\lambda)/|\lambda'|^2 \geqslant N(\mathfrak{a})/L(\mathfrak{a})^2 \geqslant L(\mathfrak{a})^{-1}.$$

THEOREM 3.3. *Let $\mathfrak{R}$ and $\mathfrak{R}^*$ be two reduced lattices; then $\mathfrak{R} \sim \mathfrak{R}^*$ if and only if $\mathfrak{R} = \theta\mathfrak{R}^*$, where Θ ($\approx \theta$) is a relative minimum of $\mathfrak{R}$.*

Proof. Let $\mathfrak{R}$ have $\{1, \mu, \nu\}$ as a reduced basis, and let $\mathfrak{R}^*$ have $\{1, \phi, \psi\}$ as a reduced basis. If $\mathfrak{R} = \theta\mathfrak{R}^*$, then $\mathfrak{R} \sim \mathfrak{R}^*$.

If $\mathfrak{R} \sim \mathfrak{R}^*$, then $\mathfrak{R} = \theta\mathfrak{R}^*$ for some Θ ($\approx \theta$) $\in \mathfrak{R}$. If Θ is not a relative minimum of $\mathfrak{R}$, then there must exist Ω ($\approx \omega$) $\in \mathfrak{R}$ such that $\Omega \in \mathfrak{N}(\Theta)$, and $\Omega \neq (0,0,0)$, $\Theta, -\Theta$. Hence $|\omega| < |\theta|$ and $|\omega'| < |\theta'|$. Since $\omega \in \mathfrak{R}$ and $\{\theta, \theta\phi, \theta\psi\}$ is a basis of $\mathfrak{R}$, we must have $a, b, c \in \mathfrak{Z}$ such that $\omega = a\theta + b\theta\phi + c\phi\psi$. If $\rho = \omega/\theta = a + b\phi + c\psi$ and $P \approx \rho$, then $P \in \mathfrak{R}^*$. Since $|\rho| < |\omega/\theta| < 1$ and $|\rho'| = |\omega'| < 1$, we see that $P \in \mathfrak{C}_1$. Since $P \neq (0,0,0)$, this is impossible; thus, Θ is a relative minimum of $\mathfrak{R}$. □

Let $\mathfrak{a}$ be any nonzero ideal, and let $\mathfrak{R}$ be the lattice which corresponds to $\mathfrak{a}$. By Theorem 3.3 we see that Voronoi's algorithm can be used to find all the reduced ideals which are in the same ideal class as $\mathfrak{a}$. In fact, if we put $\mathfrak{R} = \mathfrak{R}_1$, $\mathfrak{a}_1 = \mathfrak{a} = \mathfrak{o}$, then with Voronoi's algorithm we can find $\mathfrak{a}_n, \mathfrak{R}_n, \theta_n \in \mathfrak{Q}[\delta]$ such that $\mathfrak{R}_n$ is the lattice which corresponds to $\mathfrak{a}_n$ and

$$[\theta_n]\mathfrak{a}_n = [L(\mathfrak{a}_n)].$$

Since $\mathfrak{R}_1$ above corresponds to the ideal $\mathfrak{o} = \mathfrak{Q}[\delta]$, we must have $\mathfrak{o}^2 = \mathfrak{o}$ and $\mathfrak{R}_1^2 = \mathfrak{R}_1$. Also, since $\mathfrak{R}_j \sim \mathfrak{R}_1$ and $\mathfrak{R}_k \sim \mathfrak{R}_1$, we have

$$\mathfrak{R}_j\mathfrak{R}_k \sim \mathfrak{R}_1^2 \sim \mathfrak{R}_1$$

by the remark at the end of Section 2. By Theorem 3.2, there exists a reduced lattice $\mathfrak{S}$ such that $\mathfrak{S} \sim \mathfrak{R}_j\mathfrak{R}_k \sim \mathfrak{R}_1$. Let Γ ($\approx \gamma$) $\in \mathfrak{R}_j\mathfrak{R}_k$ such that $\gamma\mathfrak{S} = \mathfrak{R}_j\mathfrak{R}_k$. Then by Lemma 2.2 we get

$$\mathfrak{R}_1 = t\theta_j\theta_k\mathfrak{R}_j\mathfrak{R}_k,$$

where $t = L(\mathfrak{a}_j\mathfrak{a}_k)/L(\mathfrak{a}_j)L(\mathfrak{a}_k)$; thus,

$$\mathfrak{R}_1 = \phi\mathfrak{S}, \tag{3.5}$$

where

$$\phi = \gamma t\theta_j\theta_k.$$

Also, since $|\gamma'| \leqslant 1$, $0 < \gamma \leqslant 1$, $L(\mathfrak{a}_j)L(\mathfrak{a}_k) \geqslant L(\mathfrak{a}_j\mathfrak{a}_k) > 0$, $|\theta'_j| < 1$, $|\theta'_k| < 1$, we get $|\phi'| < 1$. Thus $\phi > 1$ and $\phi \leqslant \theta_j\theta_k$.

Since $\mathfrak{S}$ and $\mathfrak{R}_1$ are both reduced lattices, we see by Theorem 3.3 that Φ ($\approx \phi$) is a relative minimum of $\mathfrak{R}_1$. Hence $\phi = \theta_m$ for some m and $\mathfrak{S} = \mathfrak{R}_m$. If $\mathfrak{a}_j\mathfrak{a}_k = [s]\mathfrak{a}$, where $\mathfrak{a}$ is a primitive ideal, we see that $sL(\mathfrak{a}) = L(\mathfrak{a}_j\mathfrak{a}_k)$. Also, since $L(\mathfrak{a})^{-1} \leqslant \gamma L(\mathfrak{a}) \leqslant L(\mathfrak{a})$ and $L(\mathfrak{a}_i)$, $L(\mathfrak{a}_j) < \sqrt{|\Delta|/3}$, we have $t\gamma = sL(\mathfrak{a})\gamma/L(\mathfrak{a}_j)L(\mathfrak{a}_k) > (3/|\Delta|)^2$. Thus, if j and k are such that θ_j and θ_k are large, then we have $\theta_m \simeq \theta_j\theta_k$

and $m \simeq j + k$. In fact, when $\delta^3 = D \in \mathfrak{Z}$, and $j = k = n$, we will see in Section 6 that

$$\theta_m = \theta_n^2 \gamma / w, \tag{3.6}$$

where $w \in \mathfrak{Z}$ and $w \mid 3g_1g_2$.

In the sections that follow, we will show how to determine $\mathfrak{R}_n^2$, γ and $\mathfrak{S}$, given $\mathfrak{R}_n$. We call our algorithm for finding γ and $\mathfrak{S}$ from $\mathfrak{R}_n$ the *doubling* procedure, as it allows us to find

$$\log \phi = 2 \log \theta_n + \log \gamma - \log w, \tag{3.7}$$

when we have $\mathfrak{R}_n$ and $\log \theta_n$. The difficulty in using the doubling idea is that, while we can now skip over many of the steps of Voronoi's algorithm, we need to know where we are going in order not to skip an important step such as the kth step when $\theta_k = \varepsilon_0$. Thus, we need to have some estimate of R, which is what we are trying to find. We can, however, estimate hR by using the Euler product method. For the pure cubic case (see, for example, Barrucand, Williams and Baniuk [1]) we have

$$hR = J\sqrt{3}\,\Phi(1)/2\pi,$$

where $\Phi(1) = \zeta_{\mathfrak{K}}(1)/\zeta(1)$ is given by the Euler product

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

Here, the product is taken over all the rational primes q and $f(q)$ is given by the following:

(i) if $q \mid J$, then $f(q) = 1$;
(ii) if $3 \nmid J$, then $f(3) = 3/2$;
(iii) if $q \equiv -1 \pmod 3$ and $q \nmid J$, then $f(q) = q^2/(q^2 - 1)$;
(iv) if $q \equiv 1 \pmod 3$ and $q \nmid J$, then

$$f(q) = \begin{cases} q^2/(q-1)^2 & \text{when } (D/q)_3 = 1, \\ q^2/q^2 + q + 1 & \text{when } (D/q)_3 \neq 1. \end{cases}$$

Since

$$c_1 = \prod_{q \equiv -1 \pmod 3} q^2/(q^2 - 1)$$

converges (approximate value 1.414064387), we can approximate $\Phi(1)$ by evaluating the product over the primes $q \equiv 1 \pmod 3$ only. The real difficulty lies in knowing how many primes to use. Put $Q > 3$,

$$F(Q) = \prod_{\substack{q \leqslant Q \\ q \equiv 1 \pmod 3}} f(q),$$

and

$$c_2 = f(3)c_1 \prod_{\substack{q \nmid J \\ q \equiv -1 \pmod 3}} (q^2 - 1)/q^2 \leqslant 3/2c_1.$$

We used $Q = 10^6$ for $D \lesssim 2 \times 10^7$, $Q = 10^7$ for $D \simeq 2 \times 10^8$, and $Q = 10^8$ for $D > 10^9$ and evaluated our estimate E of hR from

$$E = \sqrt{3}\, c_2 JF(Q)/2\pi. \tag{3.8}$$

We discuss in Section 10 how good an approximation we expect E to be of hR.

If we divide E by 2^κ, we get

$$E = 2^\kappa U.$$

Voronoi's algorithm can be used to find $\mathfrak{R}_n$ and

$$R_n = \log \theta_n = \sum_{i=1}^{n-1} \log \theta_g^{(i)},$$

where $R_n < U$ and $R_{n+1} > U$. The *doubling* process can then be used κ times to find $\mathfrak{R}_t$ and

$$R_t \simeq 2^\kappa R_n.$$

We can then resume using Voronoi's algorithm, starting at $\mathfrak{R}_t$, to find $\mathfrak{R}_{t+1}$, $\mathfrak{R}_{t+2}, \ldots$ until we find $\mathfrak{R}_k$ such that $N(\theta_k) = 1$. Then probably $R_k = \log \theta_k = hR$. What we do not know is h or R. The next step, therefore, is to find h. Since $R = \log \varepsilon_0 > R_n$ and $R \leqslant R_k$, we have $h < R_k/R_n \simeq 2^\kappa$. We now attempt to find all the primes less than R_k/R_n which divide h. If p is such a prime, then $R_s = hR/p$ for some s. If we let

$$hR/p = 2^\kappa U_p,$$

we can repeat the procedure described above to find $\mathfrak{R}_u$ and R_u such that $R_u < hR/p$ and hR/p is close in value to R_u. We can then apply Voronoi's algorithm to $\mathfrak{R}_u$ to find $\mathfrak{R}_{u+1}$, $\mathfrak{R}_{u+2}, \ldots$ until we either find $\mathfrak{R}_v$ such that $N(\theta_v) = 1$, in which case $p \mid h$, or we find $\mathfrak{R}_v$ such that $R_v > hR/p$, in which case $p \nmid h$. If we find a p which does divide h, we must replace $\mathfrak{R}_k$ by $\mathfrak{R}_v$, R_k by R_v, and repeat this procedure to determine the precise power of p that divides h. When this process has been completed for all primes less than R_k/R_n, we have the value of h and also that of $R = Rh/h$.

This has been only a brief account of the algorithm for finding h and R from an estimate E of hR. We give a much more detailed algorithm in Section 10.

4. Some Simple Properties of 1-Lattices Equivalent to $\mathfrak{R}_1$. Let $\mathfrak{R}$ be any 1-lattice such that $\mathfrak{R} \sim \mathfrak{R}_1$, and let $\mathfrak{R}_1$ have basis $\{1, \bar{\mu}, \bar{\nu}\}$, where

$$\bar{\mu} = \left(\bar{m}_1 + \bar{m}_2\delta + \bar{m}_3\delta^2\right)/\sigma, \qquad \bar{\nu} = \left(\bar{n}_1 + \bar{n}_2\delta + \bar{n}_3\delta^2\right)/\sigma, \qquad \sigma > 0,$$

$\sigma, \bar{m}_i, \bar{n}_i \in \mathfrak{Z}\ (i = 1, 2, 3)$ and $\gcd(\bar{m}_1, \bar{m}_2, \bar{m}_3, \bar{n}_1, \bar{n}_2, \bar{n}_3, \sigma) = 1$. When $\mathfrak{K}$ is a pure cubic field, values for the integers m_i, n_i, and σ here are given in Section 1. Put $e = \bar{m}_2\bar{n}_3 - \bar{n}_2\bar{m}_3$. Since $\mathfrak{R} \sim \mathfrak{R}_1$, there must exist $\psi \in \mathfrak{Q}[\delta]$ such that $\mathfrak{R}_1 = \psi\mathfrak{R}$ and

$$\begin{pmatrix} 1 \\ \mu \\ \nu \end{pmatrix} = \frac{1}{\psi} T \begin{pmatrix} 1 \\ \bar{\mu} \\ \bar{\nu} \end{pmatrix}, \tag{4.1}$$

where $\mathfrak{R} = \langle 1, \mu, \nu \rangle$ and $T \in GL_3(\mathfrak{Z})$. Let

$$\mu = \left(m_1 + m_2\delta + m_3\delta^2\right)/\rho, \quad \nu = \left(n_1 + n_2\delta + n_3\delta^2\right)/\rho,$$

where $\rho > 0$, $\rho, m_i, n_i \in \mathfrak{Z}$ $(i = 1, 2, 3)$ and $\gcd(m_1, m_2, m_3, n_1, n_2, n_3, \rho) = 1$. Put $f = m_2n_3 - n_2m_3$.

We point out that if

$$M = \begin{pmatrix} \rho & 0 & 0 \\ m_1 & m_2 & m_3 \\ n_1 & n_2 & n_3 \end{pmatrix},$$

then there exists a $U \in GL_3(\mathfrak{Z})$ such that

$$UM = \begin{pmatrix} \rho & 0 & 0 \\ m & b & 0 \\ n & n' & n'' \end{pmatrix}, \tag{4.2}$$

where $n'' = \gcd(n_3, m_3)$ and $b = f/n'' \in \mathfrak{Z}$. We call the corresponding basis

$$\left\{1, \frac{m + b\delta}{\rho}, \frac{n + n'\delta + n''\delta^2}{\rho}\right\} \tag{4.3}$$

a *canonical* basis of $\mathfrak{R}$. Note that $\gcd(m, b, n, n', n'', \rho) = 1$.

We can find U by the following procedure. We may assume that $m_3 > 0$; for, if this is not so, we can replace μ by $-\mu$. If we use the Euclidean algorithm to find

$$\begin{aligned} n_3 &= q_0m_3 + r_0 \qquad (0 < r_0 < m_3), \\ m_3 &= q_1r_0 + r_1 \qquad (0 < r_1 < r_0), \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ r_{k-2} &= q_kr_{k-1} + r_k \qquad (r_k = 0), \end{aligned}$$

then we see that $r_{k-1} = n''$ and $Q_kQ_{k-1}\cdots Q_0$, where

$$Q_i = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -q_i & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

is a suitable matrix for U.

We now prove a more general version of Theorem 3.1 of [18].

THEOREM 4.1. *In the notation above, if* $N = N(\psi)$, *then* $|N| = \rho^2|e|/\sigma^2|f|$; *also,* $f \mid \rho$.

Proof. From (4.1) we get

$$\begin{aligned} \sigma\psi &= x_{11} + x_{12}\delta + x_{13}\delta^2, \\ \sigma\psi\mu &= x_{21} + x_{22}\delta + x_{23}\delta^2, \\ \sigma\psi\nu &= x_{31} + x_{32}\delta + x_{33}\delta^2, \end{aligned}$$

where $x_{ij} \in \mathfrak{Z}$ $(i = 1, 2, 3; j = 1, 2, 3)$. If

$$\overline{M} = \begin{pmatrix} \sigma & 0 & 0 \\ \overline{m}_1 & \overline{m}_2 & \overline{m}_3 \\ \overline{n}_1 & \overline{n}_2 & \overline{n}_3 \end{pmatrix},$$

then $X = (x_{ij})_{3\times 3} = T\overline{M}$ and $|X| = \pm e\sigma$. Since $\psi \in \mathfrak{D}[\delta]$, we have $\lambda = \psi'\psi'' \in \mathfrak{D}[\delta]$, and therefore $\sigma\lambda = l_1 + l_2\delta + l_3\delta^2$, where $l_i \in \mathfrak{Z}$ $(i = 1, 2, 3)$. Thus,

$$\sigma^2\lambda\psi = \sigma^2 N,$$
$$\sigma^2\lambda\psi\mu = \sigma^2 N\mu = u_1 + u_2\delta + u_3\delta^2,$$
$$\sigma^2\lambda\psi\nu = \sigma^2 N\nu = v_1 + v_2\delta + v_3\delta^2,$$

where $u_i, v_i \in \mathfrak{Z}$ $(i = 1, 2, 3)$. Also, since $\lambda\psi\mu$ and $\lambda\psi\nu \in \mathfrak{D}[\delta]$, we must have

$$\gcd(u_1, u_2, u_3, v_1, v_2, v_3) \equiv 0 \pmod{\sigma}.$$

Now

$$\begin{pmatrix} \sigma^2 N & 0 & 0 \\ u_1 & u_2 & u_3 \\ v_1 & v_2 & v_3 \end{pmatrix} = X \begin{pmatrix} l_1 & l_2 & l_3 \\ Dl_3 & l_1 - Cl_3 & l_2 + Bl_3 \\ Dl_2 + BDl_3 & (D - BC)l_3 - l_2C & l_1 + Bl_2 + (B^2 - C)l_3 \end{pmatrix}.$$

By taking determinants of both sides of this expression, we get

$$\sigma^2(u_2v_3 - v_2u_3)N = \pm e\sigma N(\sigma\lambda)$$

by (1.3). Hence

$$u_2v_3 - v_2u_3 = \pm e\sigma^2 N. \tag{4.4}$$

If we put $d^* = \gcd(u_1, u_2, u_3, v_1, v_2, v_3, \sigma^2 N)$, then $\rho = \sigma^2|N|/d^*$ and $|f| = |e|\sigma^2|N|/(d^*)^2$ from (4.4). It follows that $|f| = |e|\rho/d^*$ and $|N| = \rho^2|e|/|f|\sigma^2$. Since $\sigma|d^*$, $d^* = \rho|e|/|f|$ and $e|\sigma$, we must also have $f|\rho$. □

THEOREM 4.2. *If* Ω $(\approx \omega) \in \mathfrak{R}$ *and* $\omega = (q_1 + q_2\delta + q_3\delta^2)/\rho$, *then* $\sigma|f|\rho$ *is a divisor of* $N(\rho\omega)$ *and* $f|q_i'$ $(i = 1, 2, 3)$, *where* $\rho^2\omega'\omega'' = q_1' + q_2'\delta + q_3'\delta^2$.

Proof. Since $\Omega \in \mathfrak{R}$, we have $a, b, c \in \mathfrak{Z}$ such that $\omega = a + b\mu + c\nu$. Also, since $\psi, \psi\mu, \psi\nu \in \mathfrak{D}[\delta]$, so is $\lambda = \psi\omega \in \mathfrak{D}[\delta]$. It follows from Theorem 4.1 that

$$|N(\rho\omega)| = |\rho^3 N(\omega)| = \rho^3|N(\lambda)/N| = \rho|f|\sigma^2|N(\lambda)|/|e|.$$

Since $e|\sigma$ and $N(\lambda) \in \mathfrak{Z}$, we have the first part of the theorem. Since

$$\omega'\omega''/N(\omega) = 1/\omega = \psi/\lambda = \lambda'\lambda''\psi/N(\lambda),$$

we have $\omega'\omega'' = \lambda'\lambda''\psi/N$. Thus

$$|\rho^2\omega'\omega''| = |q_1' + q_2'\delta + q_3'\delta^2| = \sigma^2|f||\lambda'\lambda''\psi|/|e|.$$

Since $e|\sigma$ and $\lambda'\lambda''\psi \in \mathfrak{D}[\delta]$, we must have $f|q_i'$ $(i = 1, 2, 3)$. □

Now consider the sequence $\{\gamma_i\}$ $(i = 1, 2, 3, \ldots, s)$ where $\gamma_1 = 1$ and Γ_i $(\approx \gamma_i) \in \mathfrak{R}$ $(i = 1, 2, 3, \ldots, s)$. Put $\mathfrak{S}_1 = \mathfrak{R}$, $\gamma_g^{(i-1)} = \gamma_i/\gamma_{i-1}$ $(i = 2, 3, 4, \ldots, s)$, and suppose that 1 and $\gamma_g^{(i-1)}$ can be embedded in a basis $\{1, \gamma_g^{(i-1)}, \gamma_h^{(i-1)}\}$ of $\mathfrak{S}_{i-1}$. If we define

$$\mathfrak{S}_i = \left(1/\gamma_g^{(i-1)}\right)\mathfrak{S}_{i-1},$$

then $\mathfrak{S}_t$ is a 1-lattice and $\mathfrak{S}_t \sim \mathfrak{S}_{t-1}$. Further, if $\{1, \mu_t, \nu_t\}$ is any basis of $\mathfrak{S}_t$, then

$$\begin{pmatrix} 1 \\ \mu_t \\ \nu_t \end{pmatrix} = \frac{1}{\gamma_g^{(t-1)}} T_{t-1} \begin{pmatrix} 1 \\ \mu_{t-1} \\ \nu_{t-1} \end{pmatrix},$$

where $T_{t-1} \in GL_3(\mathfrak{Z})$ and $\{1, \mu_{t-1}, \nu_{t-1}\}$ is any basis of $\mathfrak{S}_{t-1}$. Hence

$$\begin{pmatrix} 1 \\ \mu_i \\ \nu_i \end{pmatrix} = \frac{1}{\gamma_i} J_1 \begin{pmatrix} 1 \\ \mu \\ \nu \end{pmatrix} = \frac{1}{\gamma_i \psi} J_2 \begin{pmatrix} 1 \\ \bar{\mu} \\ \bar{\nu} \end{pmatrix}, \tag{4.5}$$

where $J_1, J_2 \in GL_3(\mathfrak{Z})$.

For $\mu_i = (m_1 + m_2\delta + m_3\delta^2)/\rho_i$, $\nu_i = (n_1 + n_2\delta + n_3\delta^2)/\rho_i$, such that $m_j, n_j, \rho_i \in \mathfrak{Z}$ $(j = 1, 2, 3)$, $\rho_i > 0$, $\gcd(m_1, m_2, m_3, n_1, n_2, n_3, \rho_i) = 1$, put $f_i = m_2 n_3 - m_3 n_2$. By Theorem 4.1 and (4.5), we see that $f_i \mid \rho_i$ and

$$|N(\gamma_i \psi)| = \rho_i^2 |e| / \sigma^2 |f_i| . \tag{4.6}$$

We now describe how to find a basis $\{1, \mu_r, \nu_r\}$ of $\mathfrak{S}_r$ when we know the basis $\{1, \gamma_g^{(r-1)}, \gamma_h^{(r-1)}\}$ of $\mathfrak{S}_{r-1}$.

Let

$$\gamma_g^{(r-1)} = \left(m_1 + m_2\delta + m_3\delta^2\right)/\rho_{r-1}, \qquad \gamma_h^{(r-1)} = \left(n_1 + n_2\delta + n_3\delta^2\right)/\rho_{r-1},$$

where $\rho_{r-1}, m_1, m_2, m_3, n_1, n_2, n_3 \in \mathfrak{Z}$, $\rho_{r-1} > 0$ and

$$\gcd(m_1, m_2, m_3, n_1, n_2, n_3, \rho_{r-1}) = 1.$$

Define m_1', m_2', m_3' by

$$\rho_{r-1}^2 \gamma_g^{(r-1)'} \gamma_g^{(r-1)''} = m_1' + m_2'\delta + m_3'\delta^2,$$

where $m_1', m_2', m_3' \in \mathfrak{Z}$. Put

$$d_1 = \gcd(m_1', m_2', m_3'), \quad \bar{m}_i = m_i'/d_1, \quad \bar{\rho}_r = \rho_{r-1}^3 N\left(\gamma_g^{(r-1)}\right)/d_1. \tag{4.7}$$

If $\bar{\rho}_r < 0$, replace m_1, m_2, m_3 by $-m_1, -m_2, -m_3$ and $\bar{\rho}_r$ by $-\bar{\rho}_r$. This transformation does not change the values of m_1', m_2', m_3'.

Define $\bar{n}_1, \bar{n}_2, \bar{n}_3$ by

$$\bar{n}_1 + \bar{n}_2\delta + \bar{n}_3\delta^2 = \left(\bar{m}_1 + \bar{m}_2\delta + \bar{m}_3\delta^2\right)\left(n_1 + n_2\delta + n_3\delta^2\right), \tag{4.8}$$

and put

$$d_2 = \gcd(\bar{n}_1, \bar{n}_2, \bar{n}_3), \qquad n_i^* = \bar{n}_i/d_2 \quad (i = 1, 2, 3). \tag{4.9}$$

We have

$$1/\gamma_g^{(r-1)} = \rho_{r-1}\left(\bar{m}_1 + \bar{m}_2\delta + \bar{m}_3\delta^2\right)/\bar{\rho}_r,$$

$$\gamma_h^{(r-1)}/\gamma_g^{(r-1)} = \left(\bar{n}_1 + \bar{n}_2\delta + \bar{n}_3\delta^2\right)/\bar{\rho}_r.$$

Since

$$d_1 d_2\left(n_1^* + n_2^*\delta + n_3^*\delta^2\right) = \bar{\rho}_r \frac{\gamma_h^{(r-1)}}{\gamma_g^{(r-1)}} = \bar{\rho}_r \frac{n_1 + n_2\delta + n_3\delta^2}{m_1 + m_2\delta + m_3\delta^2},$$

it follows that $d_1 d_2 \mid \bar{\rho}_r n_i$ $(i = 1, 2, 3)$. Thus $d_1 d_2$ is a divisor of the $\gcd(\bar{\rho}_r n_2, \bar{\rho}_r n_3)$ and $d_1 d_2 \mid \bar{\rho}_r f_{r-1}$. By Theorem (4.2), we have $f_{r-1}\rho_{r-1} \mid N(\rho_{r-1}\theta_g^{(r-1)})$; thus, $f_{r-1}\rho_{r-1} \mid d_1\bar{\rho}_r$. If $d = \gcd(d_2, \rho_{r-1})$, then $df_{r-1} \mid d_1\bar{\rho}_r$ and $dd_1 \mid \bar{\rho}_r f_{r-1}$; therefore, $d \mid \bar{\rho}_r$. We have now proved the following theorem.

THEOREM 4.3. *If* $\{1, \gamma_g^{(r-1)}, \gamma_h^{(r-1)}\}$ *is a basis of* $\mathfrak{S}_{r-1}$, *then* $\{1, \mu_r, \nu_r\}$ *is a basis of* $\mathfrak{S}_r$, *where*

$$\mu_r = 1/|\gamma_g^{(r-1)}| = \left(m_1^* + m_2^*\delta + m_3^*\delta^2\right)/\rho_r,$$
$$\nu_r = \gamma_h^{(r-1)}/|\gamma_g^{(r-1)}| = \left(n_1^* + n_2^*\delta + n_3^*\delta^2\right)/\rho_r,$$

$\rho_r = \bar{\rho}_r/d > 0$, $m_i^* = \rho_{r-1}m_i'/dd_1$ *and* $\gcd(m_1^*, m_2^*, m_3^*, n_1^*, n_2^*, n_3^*, \rho_r) = 1$. □

By (4.6), and the fact that $\gamma_g^{(r-1)} = \gamma_r/\gamma_{r-1}$, we find that $d_1 = N(\gamma_g^{(r-1)})\rho_{r-1}^3/\bar{\rho}_r = |f_{r-1}|\rho_r\rho_{r-1}/|f_r|d$, and therefore

$$m_1' = |f_{r-1}|\rho_r m_i^*/|f_r|. \tag{4.10}$$

We call the process of finding a basis of $\mathfrak{S}_r$ from a basis of $\mathfrak{S}_{r-1}$ the *invert* process. When $\delta^3 = D$, we have $m_1' = m_1^2 - Dm_2m_3$, $m_2' = Dm_3^2 - m_2m_1$, $m_3' = m_2^2 - m_1m_3$, $\bar{\rho}_r = m_1\bar{m}_1 + D(m_2\bar{m}_3 + m_3\bar{m}_2)$, $\bar{n}_1 = \bar{m}_1n_1 + D(\bar{m}_2n_3 + \bar{m}_3n_2)$, $\bar{n}_2 = \bar{m}_2n_1 + \bar{m}_1n_2 + D\bar{m}_3n_3$, $\bar{n}_3 = \bar{m}_3n_1 + \bar{m}_2n_2 + \bar{m}_1n_3$. In this case, if $|\gamma_r^{(r-1)}| < 1$ and $|\gamma_g^{(r-1)'}| < 1$, then by Lemma 7 of [15], we have $\delta^{i-1}|m_i| < \rho_{r-1}$ $(i = 1, 2, 3)$, and therefore $\delta^{i-1}|m_i| < 2\rho_{r-1}^2/|f_{r-1}|$ $(i = 1, 2, 3)$. From (4.10), we get $\delta^{i-1}|m_i^*| < 2\rho_{r-1}^2/|f_{r-1}|$ $(i = 1, 2, 3)$.

We conclude this section by defining, as was done in [18], what we mean when we say that we *transform a basis* $\{1, \mu, \nu\}$ of $\mathfrak{R}$ *by* K, where $K \in GL_2(\mathfrak{Z})$. When we replace the basis $\{1, \mu, \nu\}$ by the basis $\{1, \bar{\mu}, \bar{\nu}\}$, where

$$\begin{pmatrix} 1 \\ \bar{\mu} \\ \bar{\nu} \end{pmatrix} = T\begin{pmatrix} 1 \\ \mu \\ \nu \end{pmatrix},$$

$$T = \left(\begin{array}{c|cc} 1 & 0 & 0 \\ \hline t_{21} & \multicolumn{2}{c}{\multirow{2}{*}{K^T}} \\ t_{31} & & \end{array}\right),$$

K^T is the transpose of K and t_{21}, t_{31} are integers selected such that the new values $\bar{m}_1$, $\bar{n}_1$ of m_1 and n_1 satisfy $0 \leq \bar{m}_1, \bar{n}_1 < \rho$, we say that we have transformed the basis $\{1, \mu, \nu\}$ by K. Note that since $|T| = \pm 1$, the new basis is in fact a basis of $\mathfrak{R}$. Also, if $\bar{\mu} = (\bar{m}_1 + \bar{m}_2\delta + \bar{m}_3\delta^2)/\rho$, $\bar{\nu} = (\bar{n}_1 + \bar{n}_2\delta + \bar{n}_3\delta^2)/\rho$, then

$$\begin{pmatrix} m_1' & n_1' \\ \bar{m}_2 & \bar{n}_2 \\ \bar{m}_3 & \bar{n}_3 \end{pmatrix} = \begin{pmatrix} m_1 & n_1 \\ m_2 & n_2 \\ m_3 & n_3 \end{pmatrix} K$$

and

$$\bar{m}_1 \equiv m_1' \pmod{\rho}, \quad \bar{n}_1 \equiv n_1' \pmod{\rho}, \quad t_{21} = (m_1' - \bar{m}_1)/\rho, \quad t_{31} = (n_1' - \bar{n}_1)/\rho.$$

5. The Bases of the Ideals of $\mathfrak{Q}[\delta]$. In order to determine a method for finding a basis of $\mathfrak{R}_n^2$ from a basis of $\mathfrak{R}_n$, it is first necessary to discuss the integral bases of the ideals of $\mathfrak{Q}[\delta]$. The integral bases for the ideals in any cubic field were determined by Voronoi [14]. However, as this work is not easily accessible, we summarize some of his results here. There are a large number of cases, and this is one of the reasons that we will restrict our discussion, here and in the next section, to the case of the pure cubic field $\mathfrak{Q}(\sqrt[3]{D})$, where $D = g_1g_2^2$ as in Section 1.

If $\mathfrak{p}$ is a prime ideal of $\mathfrak{Q}[\delta]$, then $\mathfrak{p}$ must divide $[p]$, where p is some rational prime. It is well known (see, for example, Cassels [4]) that the principal ideals $[p]$ of $\mathfrak{Q}[\delta]$ factor as follows. We have 7 cases.

(i) $p \mid g_1$. Here $[p] = \mathfrak{p}^3$, where $\mathfrak{p} = [p, \delta]$.

(ii) $p = 3$, $3 \nmid D$, $D \not\equiv \pm 1 \pmod 9$. Here $[3] = \mathfrak{p}^3$, where

$$\mathfrak{p} = [3, 1 \mp \delta] \quad \text{when } D \equiv \pm 1 \pmod 3.$$

(iii) $p \mid g_2$. In this case $[p] = \mathfrak{p}^3$, where $\mathfrak{p} = [p, \delta^2/g_2]$.

(iv) $p = 3$, $D \equiv \pm 1 \pmod 9$. We have $[3] = \mathfrak{r}^2\mathfrak{s}$, where

$$\mathfrak{r} = [3, 1 \mp \delta, (1 \pm \delta + \delta^2)/3],$$

$$\mathfrak{s} = [3, 1 \mp \delta, (-2 \pm \delta + \delta^2)/3],$$

and the signs are determined from $D \equiv \pm 1 \pmod 9$.

(v) $p \equiv -1 \pmod 3$, $p \nmid D$. Here $[p] = \mathfrak{p}\mathfrak{q}$, and

$$\mathfrak{p} = [p, d - \delta], \qquad \mathfrak{q} = [p, d^2 + d\delta + \delta^2],$$

where d is the unique root of the congruence

$$x^3 \equiv D \pmod p. \tag{5.1}$$

(vi) $p \equiv 1 \pmod 3$, $p \nmid D$, $(D/p)_3 = 1$. In this case, $[p] = \mathfrak{p}\mathfrak{p}'\mathfrak{p}''$, where

$$\mathfrak{p} = [p, d - \delta], \quad \mathfrak{p}' = [p, d' - \delta], \quad \mathfrak{p}'' = [p, d'' - \delta],$$

and d, d', d'' are the three distinct roots of the congruence (5.1).

(vii) $p \equiv 1 \pmod 3$, $p \nmid D$, $(D/p)_3 \neq 1$. Here $[p]$ is a prime ideal of $\mathfrak{Q}[\delta]$.

Let $c \in \mathfrak{Z}$ be defined as being a solution of the system of congruences

$$\begin{cases} x^3 \equiv D & (\mathrm{mod}\ \sigma^2), \\ 3x^2 \equiv 0 & (\mathrm{mod}\ \sigma). \end{cases} \tag{5.2}$$

Also, when the system of congruences

$$\begin{cases} x^3 \equiv D & (\mathrm{mod}\ \sigma^2 p^i), \\ x \equiv c & (\mathrm{mod}\ \sigma) \end{cases} \tag{5.3}$$

has a single root (mod σp^i), denote it by d_i; when (5.3) has 3 roots (mod σp^i), denote them by d_i, d_i', d_i''. Since $3d_i^2 \not\equiv 0 \pmod{\sigma p^i}$, we may assume that none of d_i, d_i', d_i'' satisfies

$$x^3 \equiv D \pmod{\sigma p^{i+1}},$$

when $p \nmid D$.

Voronoi found the bases for the prime ideals given above, their powers, and certain products of their powers. We give his results for each of the cases (i) through (vi) below. We assume here that $i \in \mathfrak{Z}$ and $i > 0$, unless otherwise stated.

GROUP A

CASES	*IDEAL* $\mathfrak{a}$	*IDEAL BASIS OF* $\mathfrak{a}$
(i), (ii), $p \nmid \sigma$	$\mathfrak{p}$	$\{p, -d_1 + \delta, (-cd_1 - d_1^2 + c\delta + \delta^2)/\sigma\}$
	$\mathfrak{p}^2$	$\{p, p(-c + \delta), (d_1^2 + d_1\delta + \delta^2)/\sigma\}$
(iii), $p \mid \sigma$	$\mathfrak{p}$	$\{p, -c + \delta, (c^2 + c\delta + \delta^2)/\sigma\}$
	$\mathfrak{p}^2$	$\{p, -d_1 + \delta, p(c^2 + c\delta + \delta^2)/\sigma\}$

Notice that in each of these cases in Group A, we have $d_1 \equiv c \pmod{\sigma}$, $d_1 \equiv D \pmod{p}$ and $c \equiv D \pmod{\sigma}$; hence, $\mathfrak{p}$ has a basis of the form

$$\{p, -D + \delta, (D^2 + D\delta + \delta^2)/\sigma\}.$$

Also, $\mathfrak{p}^2$ has a basis of the form

$$\{p, p(-D + \delta), (D^2 + D\delta + \delta^2)/\sigma\},$$

when $p \nmid \sigma$ and $\mathfrak{p}^2$ has a basis of the form

$$\{p, -D + \delta, p(D^2 + D\delta + \delta^2)/\sigma\},$$

when $p \mid \sigma$. Thus, if $\mathfrak{t}$ is either $\mathfrak{p}$ or $\mathfrak{p}^2$ here, then $\mathfrak{t}$ has a basis of the form

$$\{P, P'(-D + \delta), P''(D^2 + D\delta + \delta^2)/\sigma\},$$

and $\mathfrak{t}^2 = [P'P'']\mathfrak{u}$, where $\mathfrak{u}$ has

$$\{P, (P/P'S)(-D + \delta), (S/P'')(D^2 + D\delta + \delta^2)/\sigma\}$$

as a basis and $S = \gcd(P, \sigma)$.

GROUP B

CASE	*IDEAL* $\mathfrak{a}$	*IDEAL BASIS OF* $\mathfrak{a}$
(iv)	$\mathfrak{r}$	$\{3, -c + \delta, (c^2 + c\delta + \delta^2)/\sigma\}$
	$\mathfrak{r}^{2i}$	$\{3^i, 3^i(-c + \delta), (d_i^2 + d_i\delta + \delta^2)/\sigma\}$
	$\mathfrak{r}^{2i+1}$ $(i \geqslant 0)$	$\{3^{i+1}, 3^i(-c + \delta), (d_i^2 + d_i\delta + \delta^2)/\sigma\}$
	$\mathfrak{s}^i$	$\{3^i, -d_i + \delta, (-cd_i - d_i^2 + c\delta + \delta^2)/\sigma\}$
	$\mathfrak{r}\mathfrak{s}$	$\{3, -c + \delta, 3(c^2 + c\delta + \delta^2)/\sigma\}$
	$\mathfrak{r}\mathfrak{s}^{i+1}$	$\{3^{i+1}, -d_i + \delta, 3(-cd_i - d_i^2 + c\delta + \delta^2)/\sigma\}$
(v)	$\mathfrak{p}^i$	$\{p^i, -d_i + \delta, (-cd_i - d_i^2 + c\delta + \delta^2)/\sigma\}$
	$\mathfrak{q}^i$	$\{p^i, p^i(-c + \delta), (d_i^2 + d_i\delta + \delta^2)/\sigma\}$
(vi)	$\mathfrak{p}^i$	$\{p^i, -d_i + \delta, (-cd_i - d_i^2 + c\delta + \delta^2)/\sigma\}$
	$\mathfrak{p}^i(\mathfrak{p}')^i$	$\{p^i, p^i(-c + \delta), (d_i''^2 + d_i''\delta + \delta^2)/\sigma\}$
	$\mathfrak{p}^{i+j}(\mathfrak{p}')^i$	$\{p^{i+j}, p^i(-d_j + \delta), ((d_i''^2 + d_i''\delta + \delta^2)/\sigma + p^iQ)\}$.

In case (vi) here, Q is determined by the congruence

$$Q(d_j - d_i'')/\sigma \equiv (d_i''^3 - D)/\sigma^2 p^i \pmod{p^j}.$$

Naturally, there are similar results for $(\mathfrak{p}'')^i, (\mathfrak{p}')^{i+j}(\mathfrak{p}'')^i$, etc. As we did not specify $\mathfrak{p}$ or $\mathfrak{p}'$ here beyond saying that they were any two of the three ideals whose product is $[p]$, these other results can be easily deduced from those given here.

Each of the several ideals described in Groups A and B here can be represented by a basis of the general form

$$\{P, P'(t + \delta), P''(u + u'\delta + \delta^2)/\sigma\},$$

where $P, P', P'', t, u, u' \in \mathfrak{Z}$, P is a prime power, $P'P'' \mid P$, and $P'' \mid \sigma$. Further, it is a simple matter to verify that for each of these ideals we have

$$\text{(5.4)} \qquad \begin{cases} u - tu' + t^2 \equiv 0 \pmod{P/P'}, \\ u \equiv u'^2 \pmod{\sigma P'/P''}, \\ u(u' + t) \equiv D + tu'^2 \pmod{\sigma P/P''}. \end{cases}$$

That this representation of these ideals is essentially unique follows from the following lemma.

LEMMA 5.1. *Let* $\mathfrak{a}$ *and* $\mathfrak{b}$ *be any two ideals of* $\mathfrak{Q}[\delta]$ *such that* $\mathfrak{a}$ *has a basis of the form* $\{P, P'(r+\delta), P''(s+s'\delta+\delta^2)/\sigma\}$ *and* $\mathfrak{b}$ *has a basis of the form* $\{Q, Q'(u+\delta), Q''(v+v'\delta+\delta^2)/\sigma\}$, *where* $P, P', P'', r, s', s, Q, Q', Q'', u, v', v \in \mathfrak{Z}$. *Then* $\mathfrak{b} \mid \mathfrak{a}$ *if and only if* $Q \mid P$, $Q' \mid P'$, $Q'' \mid P''$ *and*

$$\begin{aligned} P'r &\equiv P'u \pmod{Q}, \\ P''s' &\equiv P''v' \pmod{\sigma Q'}, \\ P''s &\equiv P''v + P''u(s'-v') \pmod{\sigma Q}. \end{aligned}$$

Proof. $\mathfrak{b} \mid \mathfrak{a}$ if and only if $\mathfrak{b} \supseteq \mathfrak{a}$; thus $\mathfrak{b} \mid \mathfrak{a}$ if and only if each of P, $P'(r+\delta)$, $P''(s+s'\delta+\delta^2)/\sigma$ is contained in $\mathfrak{b}$. If

$$M_1 = \begin{pmatrix} \sigma P & \sigma P'r & P''s \\ 0 & \sigma P' & P''s' \\ 0 & 0 & P'' \end{pmatrix}, \qquad M_2 = \begin{pmatrix} \sigma Q & \sigma Q'u & Q''v \\ 0 & \sigma Q' & Q''v' \\ 0 & 0 & Q'' \end{pmatrix},$$

then P, $P'(r+\delta)$, $P''(s+s'\delta+\delta^2)/\sigma \in \mathfrak{b}$ if and only if there exists a matrix $X = (x_{ij})_{3\times 3}$ where $x_{ij} \in \mathfrak{Z}$ $(i = 1,2,3; j = 1,2,3)$ such that $M_1 = M_2 X$. The result follows easily on multiplying M_2 by X, equating the product to M_1 and attempting to solve for the rational integers x_{ij}. □

COROLLARY. *Let* $\mathfrak{a}$ *and* $\mathfrak{b}$ *be given as above, and suppose that* $P \mid P'$, $P'' \mid \sigma$, $Q, P, Q', P', Q'', P'' > 0$; *then* $\mathfrak{a} = \mathfrak{b}$ *if and only if*

$$Q = P, \quad Q' = P', \quad Q'' = P''$$

and

$$\begin{aligned} r &\equiv u \pmod{P/P'}, \\ s' &\equiv v' \pmod{\sigma P'/P''}, \\ s &\equiv v + u(s'-v') \pmod{\sigma P/P''}. \end{aligned}$$

Proof. Follows easily from the lemma and the fact that $\mathfrak{a} = \mathfrak{b}$ if and only if $\mathfrak{a} \mid \mathfrak{b}$ and $\mathfrak{b} \mid \mathfrak{a}$. □

From these results we are now able to deduce the following lemma.

LEMMA 5.2. *Let* $\mathfrak{a}$ *and* $\mathfrak{b}$ *be ideals of* $\mathfrak{Q}[\delta]$ *such that* $\mathfrak{a}$ *has a basis of the form* $\{P, P'(r+\delta), P''(s+s'\delta+\delta^2)/\sigma\}$ *and* $\mathfrak{b}$ *has a basis of the form* $\{P, P'(t+\delta), P''(u+u'\delta+\delta^2)/\sigma\}$, *where* $r, s, s', t, u, u', P, P', P'' \in \mathfrak{Z}$, $P'P'' \mid P$, $P'' \mid \sigma$ *and* t, u, u' *satisfy the congruences* (5.4). *If* $\mathfrak{a} = \mathfrak{b}$, *then* r, s', s, P, P', P'' *must satisfy the congruences*

$$\text{(5.5)} \qquad \begin{cases} r^3 \equiv -D \pmod{P/P'}, \\ s'^3 \equiv D \pmod{\sigma P'/P''}, \\ s - rs' + r^2 \equiv 0 \pmod{P/P'}, \\ s \equiv s'^2 \pmod{\sigma P'/P''}, \\ s(s'+r) \equiv D + rs'^2 \pmod{\sigma P/P''}. \end{cases}$$

Proof. Since $\mathfrak{a} = \mathfrak{b}$, we must have

$$r \equiv t \pmod{P/P'}, \qquad s' \equiv u' \pmod{\sigma P'/P''},$$
$$s \equiv u + (s' - u)t \pmod{\sigma P/P''}$$

from the corollary of Lemma 5.1. Using these results together with the congruences (5.4), it is a routine matter to deduce the last three congruences of (5.5). The first two can be easily deduced from these last three. □

Voronoi [14, Section 44] also proved the theorem which follows.

THEOREM 5.3. *Suppose* $\mathfrak{a}$ *and* $\mathfrak{b}$ *are ideals of* $\mathfrak{D}[\delta]$ *such that* $\mathfrak{a}$ *has a basis of the form* $\{P_1, P_1'(r_1 + \delta), P_1''(s_1 + s_1'\delta + \delta^2)/\sigma\}$ *and* $\mathfrak{b}$ *has a basis of the form* $\{P_2, P_2'(r_2 + \delta), P_2''(s_2 + s_2'\delta + \delta^2)/\sigma\}$, *where* $r_i, s_i, s_i', P_i, P_i', P_i'' \in \mathfrak{Z}$, $P_i'P_i'' \mid P_i$, $P_i'' \mid \sigma$, $(i = 1, 2)$. *If* $\gcd(P_1, P_2) = 1$ *and* $\mathfrak{c} = \mathfrak{a}\mathfrak{b}$, *then* $\mathfrak{c}$ *has a basis* $\{P_3, P_3'(r_3 + \delta), P_3''(s_3 + s_3'\delta + \delta^2)/\sigma\}$, *where*

$$P_3 = P_1P_2, \quad P_3' = P_1'P_2', \quad P_3'' = P_1''P_2'',$$
$$\begin{cases} r_3 \equiv r_1 \pmod{P_1/P_1'}, \\ r_3 \equiv r_2 \pmod{P_2/P_2'}, \end{cases} \qquad \begin{cases} s_3' \equiv s_1' \pmod{\sigma P_1'/P_3''}, \\ s_3' \equiv s_2' \pmod{\sigma P_2'/P_3''}, \end{cases}$$
$$\begin{cases} s_3 \equiv s_1 + r_1(s_3' - s_1') \pmod{\sigma P_1/P_3''}, \\ s_3 \equiv s_2 + r_2(s_3' - s_2') \pmod{\sigma P_2/P_3''}. \end{cases}$$

Let $\mathfrak{a}$ be any ideal of $\mathfrak{D}[\delta]$ such that $[p]$ does not divide $\mathfrak{a}$ for any rational prime p. Then, since $\mathfrak{a}$ can be written as a product of powers of distinct prime ideals, we have

$$\mathfrak{a} = \mathfrak{t}_1\mathfrak{t}_2\mathfrak{t}_3 \cdots \mathfrak{t}_k, \tag{5.6}$$

where the $\mathfrak{t}_i$ $(i = 1, 2, 3, \ldots, k)$ are ideals of Group A or Group B above. Since $\mathfrak{t}_i$ $(i = 1, 2, 3, \ldots, k)$ has a basis

$$\{p_i^{n_i}, p_i^{m_i}(t_i + \delta), p_i^{l_i}(u_i + u_i'\delta + \delta^2)/\sigma\},$$

where $p_i^{l_i} \mid \sigma$, $n_i \geqslant m_i + l_i$, $m_il_i = 0$, and $\gcd(p_i, p_j) = 1$ for $i \neq j$, we see by Theorem 5.3 that $\mathfrak{a}$ has a basis of the form

$$\{P, P'(r + \delta), P''(s + s'\delta + \delta^2)/\sigma\}, \tag{5.7}$$

where

$$P = \prod_{i=1}^{k} p_i^{n_i}, \quad P' = \prod_{i=1}^{k} p_i^{m_i}, \quad P'' = \prod_{i=1}^{k} p_i^{l_i},$$

$r, s, s' \in \mathfrak{Z}$, $P'P'' \mid P$, $P'' \mid \sigma$, and $\gcd(P, P', P'') = 1$. Note that $P = L(\mathfrak{a})$. It is also true that the congruences (5.5) are satisfied. This follows from the theorem below.

THEOREM 5.4. *Let the ideals* $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ *be defined as in Theorem* 5.3. *If* $r_i, s_i', s_i, P_i, P_i', P_i''$ *satisfy the congruences* (5.5) *when* $i = 1$ *and* $i = 2$, *then* $r_3, s_3', s_3, P_3, P_3', P_3''$, *also satisfy* (5.5).

Proof. We will only show that

$$s_3(s_3' + r_3) \equiv D + r_3s_3'^2 \pmod{\sigma P_3/P_3''}. \tag{5.8}$$

The remaining results can be derived in a somewhat similar fashion. We first note that the congruences of Theorem 5.3 must be satisfied; hence

$$r_3 = r_1 + k_1 P_1/P_1', \qquad s_3' = s_1' + k_2 \sigma P_1'/P_3'',$$
$$s_3 \equiv s_1 + \sigma r_1 k_2 P_1'/P_3'' \pmod{\sigma P_1/P_3''},$$

where $k_1, k_2 \in \mathfrak{Z}$. From these results, we get

$$\begin{aligned}(r_3 + s_3')s_3 &\equiv (r_1 + s_1' + k_1 P_1/P_1' + k_2 \sigma P_1'/P_3'')(s_1 + \sigma r_1 k_2 P_1'/P_3'') \\ &\equiv (r_1 + s_1')s_1 + \sigma(r_1 + s_1')r_1 k_2 P_1'/P_2'' \\ &\quad + k_1 s_1 P_1/P_1' + \sigma k_2 s_1 P_1'/P_3'' + k_2^2 r_1 (\sigma P_1'/P_3'')^2 \pmod{\sigma P_1/P_3''}\end{aligned}$$

and

$$\begin{aligned}D + r_3 s_3'^2 \equiv D + r_1 s_1'^2 + 2\sigma r_1 s_1' k_2 P_1'/P_3'' + k_2^2 r_1 (\sigma P_1'/P_3'')^2 \\ + k_1 s_1'^2 P_1/P_1' \pmod{\sigma P_1/P_3''}.\end{aligned}$$

Since

$$(r_1 + s_1')s_1 \equiv D + r_1 s_1'^2 \pmod{\sigma P_1/P_1''},$$
$$s_1'^2 \equiv s \pmod{\sigma P_1'/P_1''},$$
$$s_1 \equiv r_1 s_1' - r_1^2 \pmod{P_1/P_1'},$$

we get $(r_3 + s_3')s_3 \equiv D + r_3 s_3'^2 \pmod{\sigma P_1/P_3''}$. Similarly, we also get $(r_3 + s_3')s_3 \equiv D + r_3 s_3'^2 \pmod{\sigma P_2/P_3''}$. Thus, since $\gcd(P_1, P_2) = 1$, we see that (5.8) must follow. □

COROLLARY 5.4.1. *For a basis* (5.7) *of an ideal of* $\mathfrak{Q}[\delta]$ *we must have* r, s, s', P, P', P'' *satisfying* (5.5).

COROLLARY 5.4.2. *For a basis* (5.7) *of an ideal of* $\mathfrak{Q}[\delta]$ *we must have*

$$s^2 + ss'^2 \equiv 2s'D + r(s'^3 - D) \pmod{\sigma P/P''}. \tag{5.9}$$

Proof. From the theorem we know that the congruences (5.5) must hold; hence

$$(s - s'^2)(s - rs' + r^2) \equiv 0 \pmod{\sigma P/P''}$$

and

$$(s' + r)s \equiv D + rs'^2 \pmod{\sigma P/P''}.$$

From the first of these congruences, we get

$$s^2 + s's \equiv ss'r - sr^2 + 2s's - s'^3 r + s'^2 r^2 \pmod{\sigma P/P''}.$$

Using

$$sr \equiv D + rs'^2 - ss' \pmod{\sigma P/P''}$$

to substitute for sr in the first term of the above, we get

$$\begin{aligned}s^2 + s'^2 s &\equiv s'D + s'^2 r^2 + s(s' + r)(s' - r) \\ &\equiv 2s'D + r(s'^3 - D) \pmod{\sigma P/P''}.\end{aligned}$$ □

We also require two simple lemmas.

LEMMA 5.5. *Let* $D \equiv \pm 1 \pmod 9$, *and let* $\mathfrak{a}$ *be an ideal of* $\mathfrak{Q}[\delta]$ *such that* $\mathfrak{a}$ *has a basis of the form* (5.7). *If* $3 \mid P$ *and* $3 \nmid P''$, *we have* $\mathfrak{r} \mid \mathfrak{a}$ *when* $s'^2 + 2s \equiv 3 \pmod 9$ *and* $\bar{\mathfrak{s}} \mid \mathfrak{a}$ *when* $s'^2 + 2s \equiv 6 \pmod 9$. *Here* $\mathfrak{r}$ *and* $\bar{\mathfrak{s}}$ *are the ideals of case* (iv) *in Group* B.

Proof. Clearly, since $3 \nmid P''$, we see that $\mathfrak{r}\mathfrak{s} \nmid \mathfrak{a}$. However, since $3 \mid P$, one of $\mathfrak{r}$ or $\mathfrak{s}$ must be a divisor of $\mathfrak{a}$. If $\mathfrak{r} \mid \mathfrak{a}$, by Lemma 5.1, we have

$$s' \equiv c \pmod{\sigma}, \qquad s \equiv c^2 + (s' - c)(-c) \pmod{3\sigma}.$$

Since $3 \mid \sigma$, we see that $s'^2 + 2s \equiv (s' - c)^2 + 3c^2 \equiv 3 \pmod 9$. If $\mathfrak{s} \mid \mathfrak{a}$, by Lemma 5.1, we have

$$s' \equiv c \pmod{\sigma}, \qquad s \equiv -cd_1 - d_1^2 + (s' - c)(-d_1) \pmod{3\sigma}.$$

Hence, $s \equiv -d_1^2 - d_1 s' \pmod 9$ and $s'^2 + 2s \equiv (s' - d_1)^2 - 3d_1^2 \equiv 6 \pmod 9$. □

If $\mathfrak{a}$ is an ideal of $\mathfrak{D}[\delta]$ such that $\mathfrak{a}$ has a basis of the form (5.7), define 3^{ι_0} for $\mathfrak{a}$ to be the exact power of 3 that divides $\gcd(P, \sigma)$ and define 3^{ι_1} to be the exact power of 3 that divides σ/P''. Since σ is always square free, we see that both ι_0 and ι_1 are either 0 or 1.

LEMMA 5.6. *Let $\mathfrak{a}$ be an ideal of $\mathfrak{D}[\delta]$ such that $\mathfrak{a}$ has a basis of the form* (5.7) *and* $\gcd(P, J) = 1$. *There exists $k \in \mathfrak{Z}$ such that if*

$$v' = s' + \sigma k P'/P'', \qquad v = s + kr\sigma P'/P'',$$

then $\mathfrak{a}$ also has

$$\{P, P'(r + \delta), P''(v + v'\delta + \delta^2)/\sigma\} \tag{5.10}$$

as a basis, $3^{\iota_1} \mid v'^2 + 2v$, *and* $\gcd(v'^2 + 2v, 3^{\iota_0 + \iota_1} P) = 3^{\iota_1}$.

Proof. Select k such that, for each distinct prime q which divides $3^{\iota_0}P$ but does not divide $\sigma P'/P''$, we have

$$(s' + r + k\sigma P'/P'')^2 \not\equiv 3r^2 \pmod q.$$

Certainly, we can find such a k. By Lemma 5.1, it is clear that (5.10) is a basis of $\mathfrak{a}$. Hence, by Corollary 5.3.1, we must have

$$v'^3 \equiv D, \qquad v \equiv v'^2 \pmod{\sigma P'/P''}.$$

Let p be any prime such that $p \mid 3^{\iota_0}P$. If $p \mid \sigma P'/P''$, then $v'^3 \equiv D \pmod p$. If $p \neq 3$, we see that if $p \mid v'^2 + 2v$, then $p \mid D$, which is impossible. If $p = 3$, then $\iota = 1$. Since $3 \mid \sigma P'/P''$, we have $3 \mid P'$ or $3 \mid \sigma/P''$. If $3 \mid P'$, then $3 \nmid P''$, and therefore $3 \mid \sigma/P''$. Thus $\iota_1 = 1$ and $3 \nmid P''$. Hence $3^{\iota_1} \mid (v'^2 + 2v)$ and $9 \nmid v'^2 + 2v$. Now suppose that $p \nmid \sigma P'/P''$. If $p = 3^{\iota_0}$ and $\iota_0 = 1$, then $3 \mid P'', 3 \nmid P', 3 \mid P$ and $3 \mid P/P'$. Since

$$v'^2 + 2v = (s' + r + k\sigma P'/P'')^2 + 2(s - rs' + r^2) - 3r^2$$

and $s - rs' + r^2 \equiv 0 \pmod{P/P'}$, we see that $p \nmid (v'^2 + 2v)$ by construction of k. It follows that $((v'^2 + 2v)/3^{\iota_1}, 3^{\iota_1} P) = 1$. □

Since $\mathfrak{R}$ in Section 4 is similar to $\mathfrak{R}_1$ and $\mathfrak{R}_1$ corresponds to the ideal $\mathfrak{o}$, we know by Lemma 2.2 that $\mathfrak{R}$ corresponds to some ideal $\mathfrak{a}$ of $\mathfrak{D}[\delta]$. We may assume with no loss of generality that $\mathfrak{a}$ has a basis of the form (5.7). It follows (Lemma 5.1) that a canonical basis of the form (4.3) of $\mathfrak{R}$ must have

$$\begin{cases} n'' = 1, \quad f = b = \pm\sigma P'/P'', \quad \rho = \sigma P/P'', \quad f \mid m, \\ m/f \equiv r \pmod{\rho/f}, \\ n' \equiv s \pmod f, \\ n \equiv s + r(n' - s) \pmod \rho. \end{cases} \tag{5.11}$$

Also, if q is any prime such that $q \mid P''$, then $q \mid P$ and $q \nmid P'$; hence $q \mid \sigma$ and $q \nmid f$. Further, if $q \mid \sigma$ and $q \nmid f$, then $q \mid P''$. Thus, since $P'' \mid \sigma$ and σ is square-free, we have

$$P'' = \sigma/\gcd(\sigma, f). \tag{5.12}$$

If $\mathfrak{R} = \mathfrak{R}_i$ for some i, then $|f| = |e_i|$, $\rho = \sigma_i$. Hence, $P \leqslant \sigma_i$, $P' \leqslant |e_i|$, $P'' \leqslant \sigma$ and

$$P < 3D, \quad P' < 3D, \quad P'' < \sigma \tag{5.13}$$

by (6.2) of [18]. Also, we note that since $n'^3 \equiv D \pmod f$, we must have

$$\gcd(f, n') \mid D. \tag{5.14}$$

Let $\mathfrak{R}_j$ and $\mathfrak{R}_k$ be any two reduced lattices such that $\mathfrak{R}_j \sim \mathfrak{R}_k \sim \mathfrak{R}_1$. We may assume that $\mathfrak{R}_j$ and $\mathfrak{R}_k$ have canonical bases

$$\{1, |e_j|(m_j + \delta)/\sigma_j, (n_j + n'_j\delta + \delta)/\sigma_j\},$$
$$\{1, |e_k|(m_k + \delta)/\sigma_k, (n_k + n'_k\delta + \delta^2)/\sigma_k\},$$

respectively. If $\mathfrak{a}_j$ is the ideal corresponding to $\mathfrak{R}_j$ and $\mathfrak{a}_k$ is the ideal corresponding to $\mathfrak{R}_k$, then

$$L(\mathfrak{a}_j) = \sigma_j/\gcd(\sigma, e_j), \qquad L(\mathfrak{a}_k) = \sigma_k/\gcd(\sigma, e_k)$$

by (5.11) and (5.12).

If $\gcd(L(\mathfrak{a}_j), L(\mathfrak{a}_k)) = 1$, by Theorem (5.3) we have

$$\mathfrak{R}_j\mathfrak{R}_k = \langle 1, |f|(M + \delta)/\rho, (N + N'\delta + \delta^2)/\rho \rangle, \tag{5.15}$$

where $f = e_j e_k/\sigma$, $\rho = \sigma_j\sigma_k/\sigma$,

$$\begin{cases} M \equiv m_j \pmod{\sigma_j/e_j}, \\ M \equiv m_k \pmod{\sigma_k/e_k}, \end{cases} \qquad \begin{cases} N' \equiv n'_j \pmod{\gcd(\sigma, e_k)e_j/\sigma}, \\ N' \equiv n'_k \pmod{\gcd(\sigma, e_j)e_k/\sigma}. \end{cases}$$

$$\begin{cases} N \equiv n_j + m_j(N' - n'_j) \pmod{\gcd(\sigma, e_k)\sigma_j/\sigma}, \\ N \equiv n_k + m_k(N' - n'_k) \pmod{\gcd(\sigma, e_j)\sigma_k/\sigma}. \end{cases}$$

In the next section we show how, given $\mathfrak{R}_i$, to find $\mathfrak{R}_i^2$.

6. Determination of $\mathfrak{R}_i^2$. Let

$$\mathfrak{R}_i = \langle 1, (m_1 + m_2\delta + m_3\delta^2)/\sigma_i, (n_1 + n_2\delta + n_3\delta^2)/\sigma_i \rangle,$$

where, as usual, $m_1, m_2, m_3, n_1, n_2, n_3, \sigma_i \in \mathfrak{Z}$, $\sigma_i > 0$, $e_i = m_2n_3 - m_3n_2$, $\gcd(m_1, m_2, m_3, n_1, n_2, n_3, \sigma_i) = 1$. Let

$$\mathfrak{R}_i^2 = \langle 1, (M_1 + M_2\delta + M_3\delta^2)/\rho, (N_1 + N_2\delta + N_2\delta^2)/\rho \rangle,$$

where $M_1, M_2, M_3, N_1, N_2, N_3, \rho \in \mathfrak{Z}$, $\rho > 0, f = M_2N_3 - M_3N_2$,

$$\gcd(M_1, M_2, M_3, N_1, N_2, N_3, \rho) = 1.$$

In this section, we will describe how to find $\rho, M_1, M_2, M_3, N_1, N_2, N_3$ from the values of m_j, n_j $(j = 1, 2, 3)$ and σ_i above. In order to do this, we must first show how to find a basis of $\mathfrak{a}^2$, given a basis of the type (5.7) of $\mathfrak{a}$.

From (5.6), we can write $\mathfrak{a} = \mathfrak{a}_1\mathfrak{a}_2$, where all the ideals dividing $\mathfrak{a}_1$ are from Group A and all the ideals dividing $\mathfrak{a}_2$ are from Group B. By referring to the bases of the ideals of Group A and Theorem 5.3, we deduce that $\mathfrak{a}_1^2 = [P'_1P''_1]\mathfrak{b}_1$, where

$\mathfrak{b}_1$ has basis $\{P_1, (P_1/P_1'S)(-D+\delta), (S/P_1'')(D^2+D\delta+\delta^2)/\sigma\}$. Here $P_1 = \gcd(P, J)$, $P_1' = \gcd(P', J)$, $P_1'' = \gcd(P'', J)$, $S = \gcd(\sigma, P_1)$, and $\mathfrak{a}_1$ has basis $\{P_1, P_1'(-D+\delta), P_1''(D^2+D\delta+\delta^2)/\sigma\}$.

If $P_2 = P/P_1$, $P_2' = P'/P_1'$, $P_2'' = P''/P_2''$, we have a basis $\{P_2, P_2'(r+\delta), P_2''(s+s'\delta+\delta^2)/\sigma\}$ of $\mathfrak{a}_2$.

We must now determine a basis for $\mathfrak{a}_2^2$. We first calculate ι_0, ι_1 for $\mathfrak{a}_2$ and then calculate ι_2 and ι_3 as below

$$\iota_2 = \begin{cases} 1 & \text{when } \iota_0 = 1, \quad \text{and either } 3 \mid P_2'' \text{ or } s'^2 + 2s \equiv 6 \pmod 9, \\ 0 & \text{otherwise.} \end{cases}$$

$$\iota_3 = \begin{cases} 1 & \text{when } \iota_0 = 1, \quad 3 \nmid P_2'', 3 \mid P_2/P_2', s'^2 + 2s \equiv 3 \pmod 9, \\ 0 & \text{otherwise.} \end{cases}$$

By Lemmas 5.1 and 5.5, the bases of the ideals of case (iv) in Group B and Theorem 5.3, it follows that we can have 6 possible cases.

(1) $D \not\equiv \pm 1 \pmod 9$. In this case $\iota_0 = \iota_1 = \iota_2 = \iota_3 = 0$. In the remaining cases, we assume that $D \equiv \pm 1 \pmod 9$.

(2) $\mathfrak{r} \nmid \mathfrak{a}_2$, $\mathfrak{s} \nmid \mathfrak{a}_2$. Here $3 \nmid P_2$ and $\iota_0 = \iota_1 = \iota_2 = \iota_3 = 0$.

(3) $\mathfrak{r}\mathfrak{s} \mid \mathfrak{a}_2$. We have $3 \mid P_2$, $3 \nmid P_2'$, $3 \mid P_2''$ and $\iota_0 = 1, \iota_1 = 0, \iota_2 = 1, \iota_3 = 0$.

(4) $\mathfrak{s} \mid \mathfrak{a}_2$, $\mathfrak{r} \nmid \mathfrak{a}_2$. We have $3 \mid P_2$, $3 \nmid P_2'$, $3 \nmid P_2''$, $s'^2 + 2s \equiv 6 \pmod 9$ and $\iota_0 = 1$, $\iota_1 = 1, \iota_2 = 1, \iota_3 = 0$.

(5) $\mathfrak{r}^{2J} \mid \mathfrak{a}_2$, $\mathfrak{r}^{2J+1} \nmid \mathfrak{a}_2$, $j > 0$, $\mathfrak{s} \nmid \mathfrak{a}_2$. We have $3 \mid P_2$, $3 \nmid P_2''$, $3 \nmid P_2/P_2'$, $s'^2 + 2s \equiv 3 \pmod 9$ and $\iota_0 = 1, \iota_1 = 1, \iota_2 = 0, \iota_3 = 0$.

(6) $\mathfrak{r}^{2J+1} \mid \mathfrak{a}_2$, $\mathfrak{r}^{2J+2} \nmid \mathfrak{a}_2$, $j \geqslant 0$, $\mathfrak{s} \nmid \mathfrak{a}_2$. We have $3 \mid P_2$, $3 \nmid P_2''$, $9 \nmid P_2/P_2'$, $3 \mid P_2/P_2'$, $s'^2 + 2s \equiv 3 \pmod 9$ and $\iota_0 = 1, \iota_1 = 1, \iota_2 = 0, \iota_3 = 1$.

Note that in all of these cases, we have

$$3^{\iota_3} \mid (P_2/P_2'P_2''), \qquad \gcd\left(3^{1-\iota_2}, P_2/3^{\iota_3}P_2'\right) = 1. \tag{6.1}$$

By Theorem 5.3 and the bases of the ideals in Group B, we have $\mathfrak{a}_2^2 = [P_2'']\mathfrak{b}_2$, where $\mathfrak{b}_2$ is an ideal with basis

$$\left\{P_3, P_3'(U+\delta), (V+V'\delta+\delta^2)/\sigma\right\} \tag{6.2}$$

and $P_3 = P_2^2/3^{\iota_3}P_2''$, $P_3' = 3^{\iota_3}P_2'^2$. We need now to find the values of U, V' and V in (6.2). We require the following lemma.

LEMMA 6.1. *Let $D \equiv \pm 1 \pmod 9$. If $\mathfrak{a}$ is any ideal of $\mathfrak{Q}[\delta]$ with basis of the form (5.7) such that $\mathfrak{s} \mid \mathfrak{a}$, then*

$$r^3 \equiv -D \pmod{3P/P'}.$$

If $\mathfrak{s} \nmid \mathfrak{a}$ and $\mathfrak{r} \mid \mathfrak{a}$, then

$$s'^3 \equiv D \pmod{3\sigma P'/P''}.$$

Proof. Certainly, $r^3 \equiv -D \pmod{P/P'}$ and since $\mathfrak{s} \mid \mathfrak{a}$, we must have $3 \nmid P'$. Also, if $3^k \| P$, then $k \geqslant 1$. Let d_j be a root of (5.3) with $p = 3$; then $d_j^3 \equiv D \bmod(\sigma^2 3^j)$ and since $3 \nmid P'$, by Lemma 5.1, we have $r \equiv d_j \pmod{3^k}$, where $j = k$ or $k-1$. Thus, $r^3 \equiv d_j^3 \pmod{3^{k+1}}$ and $r^3 \equiv D \pmod{3P/P'}$. The second result follows by similar reasoning. □

Since $P_2P_2'(r+\delta) \in \mathfrak{a}_2^2$, we have

$$r \equiv U \pmod{P_3P_2''/P_2P_2'}.$$

Now $P_3P_2''/P_2P_2' = P_2/3^{t_3}P_2'$ and $P_3/P_3' \mid (P_2/3^{t_3}P_2')^2$; hence,

$$U = r + kP_2/3^{t_3}P_2'$$

and

$$U^3 \equiv r^3 + 3kr^2P_2/3^{t_3}P_2' \pmod{3^{t_2}P_3/P_3'}.$$

Also, by Lemma 6.1 and the definition of t_2, we have

$$U^3 \equiv -D \pmod{3^{t_2}P_3/P_3'};$$

thus,

$$-D - r^3 \equiv 3kr^2P_2/3^{t_3}P_2' \pmod{3^{t_2}P_3/P_3'}.$$

Since

$$-D - r^3 \equiv 0 \pmod{P_2/P_2'},$$

we have

$$\frac{-(D+r^3)3^{t_3}P_2'}{3^{t_2}P_2} \equiv 3^{1-t_2}kr^2 \pmod{P_2/3^{t_3}P_2'P_2''}.$$

If x is a solution of the congruence (possible by (6.1))

$$3^{1-t_2}xr^2 \equiv 1 \mod(P_2/3^{t_3}P_2'P_2'') \tag{6.3}$$

then

$$U \equiv r - x(D+r^3)/3^{t_2} \pmod{P_3/P_3'}. \tag{6.4}$$

We must also have

$$\left(P_2''(s+s'\delta+\delta^2)/\sigma\right)^2 \in \mathfrak{a}_2^2;$$

hence, there must exist $z_1, z_2, z_3 \in \mathfrak{Z}$ such that

$$P_2''(s'^2+2s) = \sigma z_3,$$
$$P_2''(D+2ss') = \sigma z_3V' + \sigma^2 z_2P_3',$$
$$P_2''(s^2+2Ds') = \sigma z_3V + \sigma^2 z_2P_3'U + \sigma^2 z_1P_3.$$

It follows that

$$V'(s'^2+2s) \equiv D + 2ss' \pmod{\sigma^2P_3'/P_2''} \tag{6.5}$$

and

$$V(s'^2+2s) \equiv s^2 + 2Ds' - U(D+2ss') + UV'(s'^2+2s) \pmod{\sigma^2P_3/P_2''}. \tag{6.6}$$

By Lemma 5.6, we may assume that s and s' have been selected such that $(s'^2+2s, 3^{t_0+t_1}P_2) = 3^{t_1}$; hence, we can solve

$$y(s'^2+2s)/3^{t_1} \equiv 1 \pmod{3^{t_0}P_2} \tag{6.7}$$

for y. Since $D + 2ss' = s'(s'^2+2s) + D - s'^3$, we have from (6.5)

$$(V'-s')(s'^2+2s)/3^{t_1} \equiv (D-s'^3)/3^{t_1} \pmod{3^tP_3'}.$$

Now

$$D - s'^{3} \equiv 0 \pmod{\sigma P_2'/P_2''};$$

thus,

$$\frac{(V' - s')}{P_2'} \frac{(s'^2 + 2s)}{3^{t_1}} \equiv \frac{D - s'^3}{3^{t_1} p_2'} \pmod{3^{t+t_3} P_2'}.$$

Since $3^{t_3} P_2' \mid P_2$, it follows that

$$V' \equiv s' + y(D - s'^3)/3^{t_1} \pmod{3^{t_0} P_3'}. \tag{6.8}$$

From (6.6), we get

$$\begin{aligned}(s'^2 + 2s)V \equiv{}& (UV' + s - s'U)(s'^2 + 2s) \\ & - (s^2 - 2s'D + ss'^2 + U(D - s'^3)) \pmod{\sigma^2 P_3/P_2''}.\end{aligned}$$

Since $D - s'^3 \equiv 0 \pmod{3^{t_3}\sigma P_2'/P_2''}$, $r \equiv U \pmod{P_2/3^{t_3} P_2'}$ and $3^{t_1} \mid \sigma/P_2''$, we see that

$$U(D - s'^3) \equiv r(D - s'^3) \pmod{3^{t_1} P_2}.$$

By Corollary 5.4.2, we have

$$s^2 - 2s'D + rs'^2 + U(D - s'^3) \equiv 0 \pmod{3^{t_1} P_2}$$

hence,

$$\left(\frac{s'^2 + 2s}{3^{t_1}}\right)\left(\frac{V - s + s'U - UV'}{P_2}\right) \equiv \frac{-(s^2 - 2s'D + ss'^2 + U(D - s'^3))}{3^{t_1} P_2} \pmod{3^{t-t_3} P_2/P_2''}.$$

Therefore

$$V \equiv s - s'U + UV' - y(s^2 - 2s'D + ss'^2 + U(D - s'^3))/3^{t_1} \pmod{3^{t_0} P_3}. \tag{6.9}$$

Since we now have a basis for $\mathfrak{b}_1$ and one for $\mathfrak{b}_2$, we must next find a basis of $\mathfrak{b}_1\mathfrak{b}_2$. Let $\mathfrak{b}_1\mathfrak{b}_2$ have a basis $\{Q, Q'(M + \delta), Q''(N + N'\delta + \delta^2)/\sigma\}$. Since $\gcd(P_3, P_1) = 1$, we have $Q = P_3 P_1$, $Q' = P_3' P_1/P_1' S$, $Q'' = S/P_1''$,

$$\begin{aligned} M &\equiv -D \pmod{P_1' S}, \qquad N' \equiv D \pmod{\sigma P_1/Q'' P_1' S}, \\ M &\equiv U \pmod{P_3/P_3'}, \qquad N' \equiv V' \pmod{\sigma P_3'/Q''}, \\ N &\equiv D^2 - D(N' - D) \pmod{\sigma P_1'' P_1/S}, \\ N &\equiv V + U(N' - V') \pmod{\sigma P_1'' P_3/S}, \end{aligned}$$

by Theorem 5.3. Since $3^{t_0} \mid \sigma/Q''$, we have

$$N' \equiv D \pmod{\sigma P_1/(3^{t_0} Q'' P_1' S)}.$$

Further

$$N \equiv D^2 - D(N' - D) \pmod{\sigma P_1'' P_1/3^{t_0} S}$$

and

$$\begin{aligned} N &\equiv V + U(N' - V') \\ &\equiv s - s'U + UN' - y(s^2 - 2s'D + 2s'^2 + U(D - s'^3))/3^{t_1} \\ &\equiv s - s'M + MN' - y(s^2 - 2s'D + 2s'^2 + M(D - s'^3))/3^{t_1} \pmod{3^{t_0} P_3} \end{aligned}$$

by (6.9) and (6.8). Since $(3^{\iota_0}P_3, \sigma P_1''P_1/3^{\iota_0}S) = 1$, we can solve for $N' \pmod{\sigma Q'/Q''}$ and $N \pmod{\sigma Q/Q''}$ by using the Chinese Remainder Theorem.

Now since $\mathfrak{R}_\iota \sim \mathfrak{R}_1$, we know that a canonical basis of $\mathfrak{R}_\iota$ must have the form

$$\left\{1, |e_\iota| \frac{m+\delta}{\sigma_\iota}, \frac{n + n'\delta + \delta^2}{\sigma_\iota}\right\}. \tag{6.10}$$

Also $\mathfrak{R}_\iota$ corresponds to an ideal $\mathfrak{a}$ with basis $\{P, P'(m+\delta), P''(n+n'\delta+\delta^2)/\sigma\}$. Further,

$$P'' = \sigma/d, \quad P' = P''|e_\iota|/\sigma, \quad P = P''\sigma_\iota/\sigma,$$

where $d = \gcd(\sigma, e_\iota)$. Put $P_1 = \gcd(\sigma_\iota/d, J)$, $P_1' = \gcd(e_\iota/d, J)$, $P_2'' = \gcd(3, P'')$, $P_2 = P/P_1$, $P_2' = P'/P_1'$, $P_1'' = P''/P_2''$, $S = \gcd(\sigma, P_1)$,

$$\iota_0 = \begin{cases} 1, & \iota = 1 \text{ and } 3 \mid P_2, \\ 0 & \text{otherwise;} \end{cases}$$

$$\iota_1 = \begin{cases} 1, & 3 \mid \sigma/P_2'', \\ 0 & \text{otherwise;} \end{cases}$$

$$\iota_2 = \begin{cases} 1, & \iota_0 = 1, \text{ and either } P_2'' = 3 \text{ or } n'^2 + 2n \equiv 6 \pmod 9, \\ 0 & \text{otherwise;} \end{cases}$$

$$\iota_3 = \begin{cases} 1, & \iota_0 = 1, P_2'' \neq 3, 3 \mid P_2/P_2', n'^2 + 2n \equiv 3 \pmod 9, \\ 0 & \text{otherwise.} \end{cases}$$

If $\gcd(3^{\iota_0}P_2, (n'^2 + 2n)/3^{\iota_1}) \neq 1$, replace n' by $n' + \sigma k P_2'/P_2''$ and n by $n + km\sigma P_2'/P_2''$, where k is selected such that this gcd is 1.

THEOREM 6.2. *If $\mathfrak{R}_\iota$ has a canonical basis* (6.10) *such that*

$$\gcd(3^{\iota_0}P_2, (n'^2 + 2n)/3^{\iota_1}) = 1,$$

then

$$\mathfrak{R}_\iota^2 = \left\langle 1, |f|(M+\delta)/\sigma, (N + N'\delta + \delta^2)/\sigma \right\rangle,$$

where $f = \sigma Q'/Q''$, $\rho = \sigma Q/Q''$, $Q'' = S/P_1''$, $Q' = 3^{\iota_3}P_2'^2P_1/P_1'S$, $Q = P_2^2P_1/3^{\iota_3}P_2''$. *Also, M, N' and N can be determined from the congruences.*

$$M \equiv -D \pmod{P_1'S},$$

$$M \equiv m - x(D + m^3)/3^{\iota_2} \pmod{P_2^2/3^{2\iota_3}P_2'^2P_2''},$$

$$N' \equiv D \pmod{\sigma P_1/(3^{\iota_0}Q''P_1'S)},$$

$$N' \equiv n' + y(D - n'^3)/3^{\iota_1} \pmod{3^{\iota_0+\iota_3}P_2'^2},$$

$$N \equiv 2D^2 - DN' \pmod{\sigma P_1''P_1/3^{\iota_0}S},$$

$$N \equiv n - n'M + MN' - y(n^2 - 2n'D + 2n'^2 + M(D - n'^3))/3^{\iota_1} \pmod{3^{\iota_0-\iota_3}P_2^2/P_2''},$$

where

$$3^{1-\iota_2}xm^2 \equiv 1 \pmod{P_2/3^{\iota_3}P_2''P_2'}$$

and

$$y(n'^2 + 2n)/3^{\iota_1} \equiv 1 \pmod{3^{\iota_0}P_2}.$$

COROLLARY. *We have* $\mathfrak{R}_1 = (\theta_i^2/w)\mathfrak{R}_i^2$, *where* $w = 3^{t_3}P_1/P_1'P_1''$.

Proof. Follows from the above results and Lemma 2.1. □

We also point out here that

$$\sigma_i^2 = \left(3^{t_3}\sigma P_1 S/P''P_1''^2\right)\rho$$

and

$$\left(\sigma_i^2/\sigma e_i\right)^2 = \left(P_1 3^{t_3}/P_1'P_1''\right)^3\rho^2/\sigma|f|\,.$$

Hence

$$\rho \leqslant \sigma_i^2 < 9D^2, \qquad \rho^2/|f| < 9D^2 \tag{6.11}$$

by (6.1) and (6.2) of [13]. Also, if $\mathfrak{S}_1 = \mathfrak{R}_i^2$ in Section 4 and $\gamma_r\mathfrak{S}_r = \mathfrak{S}_1$, where Γ_r $(\approx \gamma_r) \in \mathcal{C}_1$, then $N(\gamma_r) < 1$ and

$$\rho_r^2/|f_r| < \rho^2/|f| < 9D^2, \tag{6.12}$$

from (4.5).

7. Reduction. Let $\mathfrak{R}$ be a lattice with basis a basis of $\mathfrak{Q}[\delta]$. In this section and the two following sections, we will show how to find a reduced lattice $\mathfrak{S}$ such that $\mathfrak{S} \sim \mathfrak{R}$. In the process of doing this, we will also show how to find $\gamma \in \mathfrak{Q}(\delta)$ such that $\gamma\mathfrak{S} = \mathfrak{R}$. In order to do this, we will make use of much of the reasoning employed in [18] and several of the results provided in that work. We begin with several simple lemmas; but we must first describe what is meant by the puncture of a point Ω $(\approx \omega) \in \mathfrak{R}$. We define the puncture of Ω as in [6] and [18]; that is, we say that it is that point $\omega_p = (\xi_\omega, \eta_\omega)$ in the $x - y$ plane such that

$$\xi_\omega = (2\omega - \omega' - \omega'')/2, \qquad \eta_\omega = (\omega' - \omega'')/2i.$$

If we put $\zeta_\omega = (\omega' + \omega'')/2$, we have $\omega = \xi_\omega + \zeta_\omega$. If

$$\delta^3 = D \quad \text{and} \quad \omega = \left(q_1 + q_2\delta + q_3\delta^2\right)/\rho, \qquad (q_1, q_2, q_3, \rho \in \mathfrak{Z}),$$

then

$$\xi_\omega = 3\delta(q_2 + q_3\delta)/2\rho, \qquad \eta_\omega = \sqrt{3}\,\delta(q_2 - q_3\delta)/2\rho, \tag{7.1}$$

$$\zeta_\omega = \left(2q_1 - \delta q_2 - \delta^2 q_3\right)/2\rho.$$

We note that there exists an infinitude of points of $\mathfrak{R}$ which have the same puncture ω_p as Ω does. Let Ω^* $(\approx \omega^*)$ be that one of this infinitude of points such that $\Omega^* \in \mathcal{C}$ and $|\omega^*|$ is minimal. Now Ω^* does not necessarily exist, but, it certainly exists if $|\eta_\omega| < \sqrt{3}/2$. In the following lemmas we will assume that Ω $(\approx \omega)$ is a point of $\mathfrak{R}$ such that $\omega \notin \mathfrak{Q}$.

LEMMA 7.1. *Suppose* $\Omega \in \mathcal{C}$ *and* $\omega < 1$. *If* Ω *has puncture* $(\xi_\omega, \eta_\omega)$ *with* $\xi_\omega > 0$, *then* $\Omega \in \mathcal{C}_1$.

Proof. If $\omega > -1$, then clearly $\Omega \in \mathcal{C}_1$. If $\omega < -1$, then, since $\omega = \xi_\omega + \zeta_\omega$ and $\xi_\omega > 0$, we must have $\zeta_\omega < -1$; by (2.2), this contradicts the fact that $\Omega \in \mathcal{C}$. □

LEMMA 7.2. *If* $\Omega \in \mathcal{C}_1$ *and* Ω *has puncture* $(\xi_\omega, \eta_\omega)$, *then* $\xi_\omega < 1 + \sqrt{1 - \eta_\omega^2}$.

Proof. Follows easily from the inequalities $\omega = \xi_\omega + \zeta_\omega < 1$ and $|\omega'|^2 = \zeta_\omega^2 + \eta_\omega^2 < 1$. □

LEMMA 7.3. *If* Ω^* *exists,* $\Omega^* \notin \mathcal{C}_1$, $(\xi_\omega, \eta_\omega)$ *is the puncture of* Ω^* *and* $\xi_\omega > 0$, *then*

$$-1 \leqslant \zeta_\omega^* < 1 - \sqrt{1 - \eta_\omega^2}\,.$$

Proof. Since $\Omega^* \in \mathcal{C}$ and $\Omega^* \notin \mathcal{C}_1$, we must have $\omega^* > 1$ by Lemma 7.1. Also, $|\zeta_\omega^*| < 1$. If $\zeta_\omega^* \geqslant 1 - \sqrt{1 - \eta_\omega^2}$, then $(\zeta_\omega^* - 1)^2 + \eta_\omega^2 \leqslant 1$ and $\Omega^* - (1, 0, 1) \in \mathcal{C}$. Since $0 < \omega^* - 1 < \omega^*$, this contradicts the definition of Ω^*. The lemma follows. □

LEMMA 7.4. *If* Ω *has puncture* $(\xi_\omega, \eta_\omega)$, Ω^* *exists and* $|\xi_\omega| < \sqrt{1 - \eta_\omega^2}$, *then* $\Omega^* \in \mathcal{C}_1$.

Proof. Since $(-\Omega)^* = -\Omega^*$, we see that if $\xi_\omega < 0$, we can replace Ω by $-\Omega$ and ξ_ω by $-\xi_\omega > 0$. Thus, we may assume $\xi_\omega > 0$. If $\Omega^* \notin \mathcal{C}_1$, by Lemma 7.3, we have $\zeta_{\omega^*} < 1 - \sqrt{1 - \eta_\omega^2}$; hence, $\omega^* = \zeta_{\omega^*} + \xi_\omega < 1$ and $\Omega^* \in \mathcal{C}_1$ by Lemma 7.1. Since this is a contradiction, the lemma follows. □

LEMMA 7.5. *Let* Ω *have puncture* $(\xi_\omega, \eta_\omega)$ *such that* $\xi_\omega > 0$ *and* $|\eta_\omega| < \sqrt{3}/2$. *Let* $T \in \mathcal{R} \cap \mathcal{C}$, *and let* T $(\approx \tau)$ *have puncture* (ξ_τ, η_τ). *If* $\Omega^* \notin \mathcal{C}_1$, $(T - \Omega)^* \notin \mathcal{C}_1$, $\xi_\tau > \xi_\omega$ *and* $\eta_\tau \eta_\omega > 0$, *then* $\tau > \omega^*$.

Proof. Follows by using Lemma 7.3 and the reasoning of Lemma 4.3 of [18]. □

LEMMA 7.6. *Let* Ω *have puncture* $(\xi_\omega, \eta_\omega)$ *with* $\xi_\omega > 0$. *If* $T \in \mathcal{C}_1 \cap \mathcal{R}$ *has puncture* (ξ_τ, η_τ) *with* $\xi_\tau = b\xi_\omega$, $\eta_\tau = b\eta_\omega$, $b \in \mathcal{Z}$, $b > 0$, *then* $\Omega^* \in \mathcal{C}_1$.

Proof. The result is certainly true for $b = 1$. Suppose it is true for $b = k$, and suppose $\xi_\tau = (k + 1)\xi_\omega$, $\eta_\tau = (k + 1)\eta_\omega$. If $(T - \Omega)^* \in \mathcal{C}_1$, then since the puncture of $(T - \Omega)^*$ is $(k\xi_\omega, k\eta_\omega)$, the result is true by the induction hypothesis. If $(T - \Omega)^* \notin \mathcal{C}_1$ and $\Omega^* \notin \mathcal{C}_1$, then since $\xi_\tau > \xi_\omega > 0$, $\eta_\tau \eta_\omega > 0$, $\eta_\omega < \eta_\tau/(k + 1) < \sqrt{3}/2$, we must have $\tau > \omega^*$ by Lemma 7.5. Since $\tau < 1$, we have $\omega^* < 1$, which, in view of Lemma 7.1, contradicts the assumption that $\Omega^* \notin \mathcal{C}_1$. The lemma is true by induction. □

Let

$$\mathfrak{L} = \{\omega_p \mid \Omega \in \mathcal{R}\}. \tag{7.2}$$

It is known (see [18, pp. 581–582]) that there exist $\phi_p, \psi_p \in \mathfrak{L}$ such that

$$\mathfrak{L} = \{a\phi_p + b\psi_p \mid a, b \in \mathcal{Z}\}$$

and

$$\begin{cases} \xi_\phi > \xi_\psi > 0, \quad |\eta_\phi| < |\eta_\psi|, \quad \eta_\phi \eta_\psi < 0, \\ |\eta_\phi| < 1 - \sqrt{3}/4, \quad |\eta_\psi| > \sqrt{3}/4, \quad |\eta_\psi| > (1 - |\eta_\phi|)/2, \end{cases} \tag{7.3}$$

where $\phi_p = (\xi_\phi, \eta_\phi)$ and $\psi_p = (\xi_\psi, \eta_\psi)$. Further, if $\{1, \mu, \nu\}$ is a basis of $\mathcal{R}$, then

$$\begin{pmatrix} \mu_p \\ \nu_p \end{pmatrix} = H \begin{pmatrix} \psi_p \\ \phi_p \end{pmatrix},$$

where $H \in GL_2(\mathfrak{Z})$. Thus, if we transform the basis $\{1, \mu, \nu\}$ by H^T, we get a new basis $\{1, \psi, \phi\}$ of $\mathfrak{R}$ such that ψ_p and ϕ_p are the punctures of Ψ ($\approx \psi$) and Φ ($\approx \phi$), respectively.

We now prove the following important theorem.

THEOREM 7.7. *If there exists* Γ ($\approx \gamma$) $\in \mathfrak{R}$ *such that* $\gamma \notin \mathfrak{Q}$ *and* $\Gamma \in \mathcal{C}_1$, *there must exist* Θ ($\approx \theta$) $\in \mathfrak{R}$ *such that* $\theta \notin \mathfrak{Q}$, $\Theta \in \mathcal{C}_1$ *and* Θ *has as its puncture one of*: $\phi_p, \psi_p, \phi_p - \psi_p, \phi_p + \psi_p$, *or* $2\phi_p + \psi_p$.

Proof. Since $\Gamma \in \mathfrak{R}$, Γ has a puncture $\gamma_p \in \mathfrak{L}$. Thus, $\gamma_p = a\phi_p + b\psi_p$ for some $a, b \in \mathfrak{Z}$. If $\xi_\gamma < 0$, we can replace Γ by $-\Gamma$; thus, we may assume, with no loss of generality, that $\xi_\gamma > 0$.

If $a < 0$, then $b > 0$ and

$$|\eta_\gamma| = |a||\eta_\phi| + b|\eta_\psi| > 1$$

for $b \geq 2$. If $b = 1$, then $\xi_\gamma < 0$, which is a contradiction; hence, we must have $a \geq 0$. If $a = 0$, we have $b > 0$ and $\gamma_p = b\psi_p$. From Lemma 7.6 we see that ψ_p is the puncture of Ψ^*, where $\Psi^* \in \mathcal{C}_1 \cap \mathfrak{R}$.

Suppose $a > 0$ and $b \leq 0$. We have

$$|\eta_\gamma| = a|\eta_\phi| + |b||\eta_\psi| > 1$$

when $|b| \geq 2$. If $b = 0$, we have $\gamma_p = a\phi_p$, and once again we see from Lemma 7.6 that ϕ_p is the puncture of Φ^*, where $\Phi^* \in \mathcal{C}_1 \cap \mathfrak{R}$. If $b = -1$ and $a \geq 3$, then $\xi_\gamma > 2\xi_\phi$ and, since $|\eta_\gamma| < 1$ and $|\eta_\psi| > \sqrt{3}/4$, we get $|\eta_\phi| < (1 - \sqrt{3}/4)/3$. Thus, $\sqrt{1 - \eta_\phi^2} > .98$ and, if $\Phi^* \notin \mathcal{C}_1$, we must have $2\xi_\phi > 1.96$ by Lemma 7.4. Now $|\eta_\gamma| > |\eta_\psi| > \sqrt{3}/4$; hence, since $\Gamma \in \mathcal{C}_1$, we must, by Lemma 7.2, have

$$\xi_\gamma < 1 + \sqrt{1 - \eta_\gamma^2} < 1 + \sqrt{13}/4 < 1.96.$$

Since this is a contradiction, we see that if $b = -1$ and $a \geq 3$, then $\Phi^* \in \mathcal{C}_1$. If $b = -1$ and $a = 2$, then $\gamma_p - \phi_p = \phi_p - \psi_p$. Also, η_γ and η_ϕ have the same sign; thus, if neither Φ^* nor $(\Phi - \Psi)^*$ is in $\mathcal{C}_1$, then by Lemma 7.5, we must have $\gamma > \phi^* > 1$. This contradicts the fact that $\Gamma \in \mathcal{C}_1$; hence, if $b = -1$ and $a = 2$, then one of Φ^* or $(\Phi - \Psi)^*$ is in $\mathcal{C}_1$. Also, if $a = 1$ and $b = -1$, then $(\Phi - \Psi)^* \in \mathcal{C}_1$.

Now suppose that $b \geq a > 0$. If $d = b - a \geq 0$, we have

$$|\eta_\gamma| = a|\eta_\phi + \eta_\psi| + d|\eta_\psi|.$$

If $d = 0$, then $(\Phi + \Psi)^* \in \mathcal{C}_1$ by Lemma 7.6. Assume that $d > 0$. If $|\eta_\phi + \eta_\psi| > 1/2$, then $|\eta_\psi| > 1/2$ and $a + d < 2$. Since $d > 0$, this is impossible. If $|\eta_\phi + \eta_\psi| < 1/2$, then $|\eta_{\phi+\psi}| = |\eta_\phi + \eta_\psi| < \sqrt{3}/2$ and $(\Phi + \Psi)^*$ exists. If $(\Phi + \Psi)^* \in \mathcal{C}_1$, we have finished the proof for this case. Suppose that $(\Phi + \Psi)^* \notin \mathcal{C}_1$. Now η_γ and $\eta_{\phi+\psi}$ have the same sign and $\xi_\gamma > \xi_{\phi+\psi}$; hence, from Lemma 7.5 it follows that if no point of $\mathfrak{R} \cap \mathcal{C}_1$ with puncture $(a - 1)(\phi_p + \psi_p) + d\psi_p$ is in $\mathcal{C}_1$, then $\gamma > (\phi + \psi)^* > 1$, a contradiction. Thus, we must assume that there exists a point of $\mathfrak{R}$ with puncture $(a - 1)(\phi_p + \psi_p) + d\psi_p$. By continuing this argument we must conclude that, since a is a finite integer, there must be a point of $\mathfrak{R}$ in $\mathcal{C}_1$ with puncture $d\psi_p$. By Lemma 7.6, we see that $\Psi^* \in \mathcal{C}_1$.

It remains to consider the case of $a > b \geq 1$. If $a \geq 3$, we have $\xi_\gamma > 3\xi_\phi$. If $\Phi^* \notin \mathcal{C}_1$, then $\xi_\phi > \sqrt{1 - \eta_\phi^2} > .8$. Also, $\xi_\gamma < 1 + \sqrt{1 - \eta_\gamma^2} < 2$. Since $\xi_\gamma > 3(.8)$, we have a contradiction; thus, if $a > b \geq 1$, we can only have $a = 2, b = 1$. □

Let $\mathcal{A}$ be a set of points $(a, b) \in \mathfrak{Z}^2$ such that if $\mathcal{R}$ is not reduced, then one of $(a\Phi + b\Psi)^* \in \mathcal{C}_1$. By Theorem 7.6, we see that we can have $\mathcal{A} \subseteq \{(1,0),(1,0),(1,-1),(1,1),(2,1)\}$. In certain cases $\mathcal{A}$ is actually a proper subset of this set.

COROLLARY 7.7.1. *If* $|\eta_\psi| < \sqrt{3}/2$, *then* $\mathcal{A} = \{(1,0),(0,1),(1,-1)\}$.

Proof. When $|\eta_\psi| < \sqrt{3}/2$, we know that Ψ^* exists. Since Φ^* also exists, $\eta_\phi \eta_\psi < 0$ and $\xi_\gamma > \xi_\psi, \xi_\phi$ when $\gamma_p = \phi_p + \psi_p$ or $\gamma_p = 2\phi_p + \psi_p$, we see that γ cannot be less than both ϕ^* and ψ^* unless one of Φ^*, Ψ^* is in $\mathcal{C}_1$. □

COROLLARY 7.7.2. *If* $|\eta_\psi| < 1.19$, *then* $\mathcal{A} = \{(1,0),(0,1),(1,-1),(1,1)\}$.

Proof. Suppose that $\Gamma \in \mathcal{C}_1$ and $\gamma_p = 2\phi_p + \psi_p$. If η_γ and η_ϕ have the same sign, then since $\xi_\gamma > \xi_\phi$, we must have Φ^* or $(\Phi + \Psi)^*$ lying in $\mathcal{C}_1$, or $\gamma > \phi^*$ by Lemma 7.5. If $\Phi^* \notin \mathcal{C}_1$, then $\gamma > \phi^* > 1$ and $\Gamma \notin \mathcal{C}_1$.

If η_γ and η_ϕ do not have the same sign, then η_γ and $\eta_{\phi+\psi}$ must have the same sign. If $|\eta_{\phi+\psi}| < \sqrt{3}/2$, then, again by Lemma 7.5, we must have Φ^* or $(\Phi + \Psi)^* \in \mathcal{C}_1$ or $\gamma > (\phi + \psi)^*$. If $\Phi^*, (\Phi + \Psi)^* \notin \mathcal{C}_1$, then $\gamma > (\phi + \psi)^* > 1$ and $\Gamma \notin \mathcal{C}_1$. Thus, we will assume that $|\eta_\phi + \eta_\psi| = |\eta_\psi| - |\eta_\phi| > \sqrt{3}/2$. We have $|\eta_\gamma| = |\eta_\psi| - 2|\eta_\phi| > \sqrt{3}/2 - |\eta_\phi|$. If $\Phi^* \notin \mathcal{C}_1$, we get $\xi_\phi > \sqrt{1 - \eta_\phi^2}$ from Lemma 7.4. Also, since $\Gamma \in \mathcal{C}_1$, we have $\xi_\gamma < 1 + \sqrt{1 - \eta_\gamma^2}$ from Lemma 7.2. Now since $|\eta_\psi| > \sqrt{3}/2 + |\eta_\phi|$ and $|\eta_\psi| < 1.19$, we find that $|\eta_\phi| < 1/3$. Further,

$$f(x) = 2\sqrt{1 - x^2} - \sqrt{1 - \left(\sqrt{3}/2 - x\right)^2}$$

is a strictly decreasing function for $0 < x < 1$ and $f(1/3) > 1.039$; hence,

$$\xi_\gamma > 2\xi_\phi > 2\sqrt{1 - \eta_\phi^2} > 1 + \sqrt{1 - \left(\sqrt{3}/2 - |\eta_\phi|\right)^2} > 1 + \sqrt{1 - \eta_\gamma^2}.$$

Since this is a contradiction, we see that we can eliminate (2, 1) from the set given above. □

With these results we are now in a position to develop an algorithm for finding a reduced lattice $\mathbb{S}$ and $\gamma \in \mathcal{K}$ such that $\mathcal{R} = \gamma\mathbb{S}$. Let $\gamma_1 = 1$, $\mathbb{S}_1 = \mathcal{R}$. We first find the points ϕ_p and ψ_p of $\mathfrak{L}$, along with the corresponding points Φ and Ψ of $\mathbb{S}_1$, for which ϕ_p and ψ_p are the respective punctures. We can then find the points $a\Phi + b\Psi$ of $\mathbb{S}_1$ with $(a, b) \in \mathcal{A}$ and then determine $(a\Phi + b\Psi)^*$. If none of these points is in $\mathcal{C}_1$, we know that $\mathbb{S}_1$ is already reduced and $\gamma = \gamma_1$. If one of them is in $\mathcal{C}_1$, let $\Gamma_g^{(1)}$ $(\approx \gamma_g^{(1)}) = (a\Phi + b\Psi)^*$ be that point such that $\Gamma_g^{(1)} \in \mathcal{C}_1$ and $|\gamma_g^{(1)}|$ is least. Put $\gamma_g^{(1)} = a\phi + b\psi$, and $\gamma_h^{(1)} = \psi$, when $(a, b) \neq (0, 1)$ or $\gamma_h^{(1)} = \phi$ when $(a, b) = (0, 1)$. Then $\{1, \gamma_g^{(1)}, \gamma_h^{(1)}\}$ is a basis of $\mathbb{S}_1$ and, if we define $\mathbb{S}_2 = |1/\gamma_g^{(1)}|\mathbb{S}_1$, we have $\mathbb{S}_2 \sim \mathbb{S}_1$. We then repeat the algorithm on $\mathbb{S}_2$ to find that either $\mathbb{S}_2$ is reduced or $\Gamma_g^{(2)}$ $(\approx \gamma_g^{(2)}) \in \mathbb{S}_2 \cap \mathcal{C}$. We repeat the above procedure to obtain $\mathbb{S}_3 = |1/\gamma_g^{(2)}|\mathbb{S}_2$ and then continue the entire process until we ultimately find $\mathbb{S}_k = |1/\gamma_g^{(k-1)}|\mathbb{S}_{k-1}$ such

that $\mathfrak{S}_k$ is reduced. That this must eventually occur follows from the fact that $\mathfrak{S}_j = (1/\gamma_j)\mathfrak{S}_1$, where

$$\gamma_j = \prod_{i=1}^{j-1} |\gamma_g^{(i)}| ;$$

hence $|\gamma_j| < 1$ and $|\gamma_j'| < 1$. Since there can only be a finite number of points in $\mathfrak{S}_1 \cap \mathfrak{C}_1$, the algorithm must terminate and $\gamma = \gamma_k$. It can also be shown that the value of k here is $O(\log|\Delta|)$.

Thus, in order to find $\mathfrak{S}$ and γ, we must know how to find $\psi_p, \phi_p, \Psi, \Phi$, $(a\Phi + b\Psi)^*$ for $(a, b) \in \mathfrak{d}$ and be able to determine whether or not $(a\Phi + b\Psi)^* \in \mathfrak{C}_1$. We will show how to solve these problems when $\delta^3 = D$ in the next two sections.

8. The Algorithm for Determining ϕ and ψ when $\delta^3 = D$ and $D > 10^5$. The problem of this section and the next is really that of developing an algorithm which determines whether or not there exists a $\gamma_g\ (> 0)$ such that $\Gamma_g\ (\approx \gamma_g) \in \mathfrak{R} \cap \mathfrak{C}_1$ and, if such a γ_g does exist, to find it. Because of the precision problems mentioned in [18], we will produce an algorithm which will require that we perform our operations on integers only.

Let $\mathfrak{R}$ have a canonical basis

$$\{1, |f|(m + \delta)/\rho, (n + n'\delta + \delta^2)/\rho\}.$$

We may certainly assume that $|m| < \rho/|f|$, $|n| < \rho$, $|n'| < |f|$. If*** $|f| \leqslant [\delta]$, transform this basis by $K = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$; if $|f| > [\delta]$ and $n' = 0$, transform this basis by $K = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$.

If $|f| > [\delta]$ and $n' \neq 0$, let

$$n'/|f| = \langle q_0, q_1, q_2, \ldots, q_k \rangle$$

be the continued fraction expansion of $n'/|f|$, and let $A_{-2} = B_{-1} = 0$, $A_{-1} = B_{-2} = 1$, $A_{r+1} = q_{r+1}A_r + A_{r-1}$, $B_{r+1} = q_{r+1}B_r + B_{r-1}$. Then $A_m/B_m = \langle q_0, q_1, q_2, \ldots, q_m \rangle$. Let $d = \gcd(n', f)$. Since $d \mid D$; we see that $Df \mid d^2$ is an integer. If $D|f|/d^2 \leqslant [\delta^2]$, put $j = k$; then $B_j = |f|/d < \sqrt{|f|/\delta}$. If $D|f|/d^2 > [\delta^2]$, find j such that

$$DB_j^2 \leqslant [\delta^2]|f| \quad \text{and} \quad DB_{j+1}^2 > [\delta^2]|f| .$$

Since Df/d^2 is an integer, we know that $B_k = |f|/d > \sqrt{|f|/\delta}$, and therefore such a j must exist. Further,

$$B_j < \sqrt{|f|/\delta} .$$

Put

$$K = \begin{pmatrix} A_j & A_{j-1} \\ -B_j & -B_{j-1} \end{pmatrix}.$$

We have $|K| = \pm 1$. Transform the canonical basis by K. If the new basis of $\mathfrak{R}$ has the form

$$\left\{1, \frac{m_1 + m_2\delta + m_3\delta^2}{\rho}, \frac{n_1 + n_2\delta + n_3\delta^2}{\rho}\right\}, \tag{8.1}$$

***We use the notation $[\alpha]$ to denote that integer which satisfies $\alpha - 1 < [\alpha] \leqslant \alpha$.

then $m_3 = -B_j$; $n_3 = -B_{j-1}$, $m_2 = A_j|f| - B_j n'$, $n_2 = A_{j-1}|f| - B_{j-1}n'$; thus $|n_3| < |m_3| < \sqrt{|f|/\delta}$. Also, if $D|f|/d^2 \leq [\delta^2]$, then $m_2 = 0$. Now it is well known that

$$\left|\frac{n'}{|f|} - \frac{A_j}{B_j}\right| < \frac{1}{B_j B_{j+1}};$$

hence, if $D|f|/d^2 > [\delta^2]$, we find that

$$|m_2| < |f|/B_{j+1} < \sqrt{\delta|f|}\left(\sqrt{\delta^2/[\delta^2]}\right) < 1.0003\sqrt{\delta|f|} \quad \text{for } D > 10^5.$$

Also, since n_2 and m_2 have different signs, $m_3 n_3 > 0$, and $|m_2 n_3 - m_3 n_2| = |f|$, we find that $|n_2| < |f/m_3|$.

Thus, after transforming our normal basis by whichever of the matrices K we select, we obtain a new basis of the form (8.1), where

$$0 < m_1, n_2 < \rho, \quad |n_2| \leq |f|, \quad |m_2| < 1.0003\sqrt{\delta|f|}, \tag{8.2}$$

$$\delta|n_3| < \sqrt{\delta|f|}, \qquad \delta|m_3| < \sqrt{\delta|f|}.$$

We call this step where we find this new basis (8.1) the *pre-reduction* step.

Incidentally, if $\mu = (m + \delta)|f|/\rho$, we see that $\xi_\mu = 3\delta|f|/2\rho$, $\eta_\mu = \sqrt{3}\,\delta|f|/2\rho$, $\xi_\mu^2 + \eta_\mu^2 = 3f^2\delta^2/\rho^2$. Thus, if $\mathfrak{R}$ is a reduced lattice, like $\mathfrak{R}_i$, then, by Lemma 7.4, $\rho/|f| < \sqrt{3}\,\delta$. This allows us to improve the result (6.3) of [18] to

$$\sigma_i/|e_i| < \sqrt{3}\,\delta. \tag{8.3}$$

Let $M \approx \mu = (m_1 + m_2\delta + m_3\delta^2)/\rho$, $\nu = (n_1 + n_2\delta + n_3\delta^2)/\rho$, where (8.2) is true. We have $|m_2| + |m_3\delta| < 3\sqrt{\delta|f|}$. Now, if $\rho^2/|f| > 9.0003D$, we have $3\sqrt{\delta|f|} < \rho/\delta$ and $|\eta_\mu| = \sqrt{3}\,\delta|m_2 - m_3\delta|/2\rho < \sqrt{3}/2$; hence, M^* exists. We also have

$$3(m_2 + m_3\delta)^2 + (m_2 - m_3\delta)^2 = 4\left(m_2^2 + m_2 m_3\delta + m_3^2\delta^2\right) < 4\rho^2/3\delta^2.$$

Hence $\eta_\mu^2 + \xi_\mu^2 < 1$. By Lemma 7.4, we see that $M^* \in \mathcal{C}_1$.

We now know that if $\rho^2/|f| > 9.0003D$, we can easily, by the pre-reduction process described above, find a basis $\{1, \mu, \nu\}$ of $\mathfrak{R}$ such that M^* $(\approx \mu^*) \in \mathcal{C}_1$ and $\mu^* > 0$. We now show, given μ and the fact that $|m_1| < \rho$, how to find λ such that $\mathfrak{R} = \langle 1, \lambda, \nu \rangle$, $\Lambda(\approx \lambda) \in \mathcal{C}_1$ and $\lambda > 0$.

Let $\lambda = (m_1^* + m_2\delta + m_3\delta^2)/\rho$. We first note that if $M^* \in \mathcal{C}_1$, then $|\lambda| < 1$, $|\lambda'| = |\lambda''| < 1$. Since $3m_i^*/\rho = \lambda + \lambda' + \lambda''$, we have $|m_i^*| < \rho$. If $m_1 < 0$, replace m_1 by $m_1 + \rho$. We now have $0 < m_1 < \rho$. Since $m_1^* \equiv m_1 \pmod{\rho}$ and $|m_1^*| < \rho$, we see that m_1^* is either m_1 or $m_1 - \rho$. Put m^* equal to that one of m_1 or $m_1 - \rho$ which has least absolute value.

Put

$$\overline{m}_1 = \left(m_1^{*2} - Dm_2m_3\right)/|f|, \qquad \overline{m}_2 = \left(Dm_3^2 - m_1^* m_2\right)/|f|,$$

$$\overline{m}_3 = \left(m_2^2 - m_1^* m_3\right)/|f|, \qquad \tau = \rho/|f|, \qquad Q = \rho\tau,$$

$$\rho\Sigma = m_1^*\overline{m}_1 + D(m_2\overline{m}_3 + m_3\overline{m}_2).$$

By using the reasoning of Section 9 of [18], we see that in order for $\Lambda \in \mathcal{C}$, we must have

$$\Sigma^2 + 3\tau(\overline{m}_1\rho - m_1^*\Sigma) < Q^2. \tag{8.4}$$

Also, if $|\lambda|<1$, we must have $N(\lambda-1)<0$ and $N(\lambda+1)>0$; hence,

$$-(Q+3\overline{m}_1)<\Sigma+3\tau m_1^*<Q+3\overline{m}_1. \tag{8.5}$$

Thus, if (8.4) and (8.5) hold, we have our value of λ. If one of them does not hold, then we can put m_1^* equal to the other of the two m_1, $m_1-\rho$, from which we made our first selection. Since we selected the value of m_1^* such that $|m_1^*|$ is minimal, we usually find that the first selected value of m_1^* works. If $\Sigma<0$, replace m_1^*, m_2, m_3, Σ by $-m_1^*$, $-m_2$, $-m_3$, and $-\Sigma$. We now have $\lambda>0$. We call this process of finding λ from μ the *find* step. Note that it is possible to show that either $\lambda<.8$ or $|\lambda'|<.8$.

When we find λ, we can put $\gamma_g=\lambda$ and $\gamma_h=\nu$ and then determine a new lattice $(1/\gamma_g)\mathfrak{R}$ by the *invert* step of Section 4. Notice that we can save some labour in the invert step if we retain some of the calculations performed in the *find* step. Note that it is possible to show that either $\lambda<.8$ or $|\lambda'|<.8$.

Thus, we have an algorithm for finding γ_g when $\rho^2/|f|>9.0003D$. When $\rho^2/|f|<9.0003D$, we make use of the results of Section 7. We can find ψ_p and ϕ_p by using algorithm A of [18]. However, we have the same problem of precision in using A as that mentioned in [18]; thus, we must modify this algorithm. We can not simply use the modification given in [18], because it was assumed throughout the discussion there that the only points of $\mathfrak{R}$ in $\mathcal{C}_1$ were $(0,0,0)$ and $(\pm1,0,\pm1)$. This need no longer be true here. We also point out that, since $\lambda|\lambda'|<.8$, no more than $O(\log D)$ pre-reduction steps need to be executed before we find that $\rho^2/|f|<9.0003D$.

Let $\{1,\mu,\nu\}$ be a basis of the form (8.1) such that (8.2) is true. Since $\rho^2/|f|<9.0003D$ and $f|\rho$, we deduce that $|f|\leqslant\rho<9.0003D$, $\rho/|f|<\sqrt{9.0003D}$ and therefore

$$|m_2|,\ \delta|n_3|,\ \delta|m_3|<\beta,\qquad |n_2|<9.0003D, \tag{8.6}$$

where $\beta=3.002\delta^2$.

For any $\Omega\in\mathfrak{R}$, where $\Omega\approx\omega=(q_1+q_2\delta+q_3\delta^2)/\rho$, $q_1,q_2,q_3\in\mathfrak{Z}$, define

$$x_\omega=q_2I_1+[I_1\delta]q_3,\qquad y_\omega=q_2I_1-[I_1\delta]q_3,$$
$$\bar{x}_\omega=[3\delta I_2]q_2+[3\delta^2I_2]q_3,\qquad \bar{y}_\omega=[\sqrt{3}\,\delta I_2]q_2-[\sqrt{3}\,\delta^2I_2]q_3,$$

where I_1, $I_2\in\mathfrak{Z}$. We will specify values for I_1 and I_2 later.

We require

LEMMA 8.1. *Suppose* $\Omega\in\mathfrak{R}$ *and* $|q_2|+|q_3|<2k$. *Let* $I_2>k/\rho(1/2-\sqrt{3}/4)$, *and let* (ξ_ω,η_ω) *be the puncture of* Ω. *If* $|\bar{y}_\omega|\geqslant I_2\rho$, *then* $|\eta_\omega|>\sqrt{3}/4$; *if* $|\bar{x}_\omega|\geqslant I_2\rho$, *then* $|\xi_\omega|>\sqrt{3}/4$.

Proof. Since

$$|\eta_\omega-\bar{y}_\omega/2\rho I_2|,\ |\xi_\omega-\bar{x}_\omega/2\rho I_2| \tag{8.7}$$
$$<(|q_2|+|q_3|)/2\rho I_2<k/\rho I_2<1/2-\sqrt{3}/4,$$

the result follows easily. □

LEMMA 8.2. *If the conditions of Lemma* 8.1 *hold, except that both* $|\bar{y}_\omega|$ *and* $|\bar{x}_\omega|$ *are now less than* $I_2\rho$, *then* $\Omega^*\in\mathcal{C}_1$.

Proof. From (8.7) we see that $|\eta_\omega|<1-\sqrt{3}/4<\sqrt{3}/2$ and $|\xi_\omega|<1-\sqrt{3}/4$. Since $\xi_\omega^2+\eta_\omega^2<1$, we must have $\Omega^*\in\mathcal{C}_1$ by Lemma 7.4. □

Lemma 8.2 is an important result for the development of our algorithm for finding γ_g; for it allows us to assume that our current basis $\{1, \mu, \nu\}$ of $\mathfrak{R}$ is such that one of $|\xi_\mu|$ or $|\eta_\mu|$ must exceed $\sqrt{3}/4$. If neither one of them, as determined by an examination of $\bar{y}_\mu$ and $\bar{x}_\mu$ exceeds $\sqrt{3}/4$, then we can immediately send μ to the *find* step for the determination of a value for γ_g. We will now present several lemmas. As the methods of proof of these lemmas are very similar or identical to the methods used in proving analogous lemmas in Sections 7 and 8 of [18], we will only state these lemmas, except in those cases where there may be some differences in the proofs. In these cases, we will sketch the proof.

LEMMA 8.3. *If* $I_1 > 3.1(2\beta)^3/\delta$, μ *and* ν *are given in* (8.1) *such that* (8.6) *holds, then* $\operatorname{sgn}(x_\mu) = \operatorname{sgn}(\xi_\mu)$, $\operatorname{sgn}(y_\mu) = \operatorname{sgn}(\eta_\mu)$, $\operatorname{sgn}(x_\nu) = \operatorname{sgn}(\xi_\nu)$, $\operatorname{sgn}(y_\nu) = \operatorname{sgn}(\eta_\nu)$, $\operatorname{sgn}(\xi_\nu - \xi_\mu) = \operatorname{sgn}(x_\nu - x_\mu)$, $\operatorname{sgn}(\eta_\nu - \eta_\mu) = \operatorname{sgn}(y_\nu - y_\mu)$.

LEMMA 8.4. *Let* (ξ_π, η_π) *be the puncture of* $\Pi \in \mathfrak{R}$ *such that* $0 < \xi_\pi < \xi_\mu$, $|\eta_\pi| < |\eta_\mu|$, *and let* $(\xi_\omega, \eta_\omega)$ *be the puncture of* $\Omega \in \mathfrak{R}$. *If* $I_1 > 3.1(4\beta)^3/\delta$ *and* $|[\xi_\omega/\xi_\pi] - [\eta_\omega/\eta_\pi]| \leqslant 3$, *then* $[\xi_\omega/\xi_\pi] = [x_\omega/x_\pi]$ *and* $[\eta_\omega/\eta_\pi] = [y_\omega/y_\pi]$.

Proof. Let $\Pi \approx \pi = (p_1 + p_2\delta + p_3\delta^2)/\rho$, $\Omega \approx \omega = (q_1 + q_2\delta + q_3\delta^2)/\rho$, $k_1 = [\xi_\omega/\xi_\pi]$, $k_2 = [\eta_\omega/\eta_\pi]$, $t_i = q_2 - k_i p_2$, $u_i = q_3 - k_i p_3$, $\xi_i = 3\delta(t_i + u_i\delta)/2\rho$, $\eta_i = \sqrt{3}\,\delta(t_i - u_i\delta)/2\rho$ $(i = 1, 2)$. By using the reasoning of Lemma 7.8 of [18], we find that

$$|\eta_1|, |\eta_1 - \eta_\pi| < 4|\eta_\pi|; \qquad |\xi_1|, |\xi_1 - \xi_\pi| < |\xi_\pi|;$$
$$|\eta_2|, |\eta_2 - \eta_\pi| < |\eta_\pi|; \qquad |\xi_2|, |\xi_2 - \xi_\pi| < 4|\xi_\pi|.$$

It follows that $|\delta u_i| < 4\beta$, $|\delta(u_i - p_3)| < 4\beta$, $\delta|p_3| < 4\beta$ $(i = 1, 2)$; hence the lemma follows from Lemma 7.5 of [18]. □

LEMMA 8.5. *Let* Π *and* Ω *be as defined in Lemma* 8.4, *and suppose that* $I_1 > 3.1\delta^2(2\sqrt{3}\,\delta + \beta/\delta)^3$. *We must have* $[x_\omega/x_\pi] = [\xi_\omega/\xi_\pi]$ *when* $\xi_\pi > \sqrt{3}/4$ *and* $[y_\omega/y_\pi] = [\eta_\omega/\eta_\pi]$ *when* $|\eta_\pi| > \sqrt{3}/4$.

LEMMA 8.6. *Let* Π *and* Ω *be defined as in Lemma* 8.4 *and suppose that* $\{1, \pi, \omega\}$ *is a basis of* $\mathfrak{R}$. *If* $I_1 > 3.1(4\beta)^3/\delta$ *and* $|[x_\omega/x_\pi] - [y_\omega/y_\pi]| \leqslant 1$, *then* $[\xi_\omega/\xi_\pi] = [x_\omega/x_\pi]$ *and* $[\eta_\omega/\eta_\pi] = [y_\omega/y_\pi]$.

Proof. We note that the Eqs. (7.2), (7.3), and (7.4) of [18] hold with e_r replaced by f. By using the facts that

$$|p_2| + |p_3|\delta < 2\beta, \quad |f| < 9.0003D \quad \text{and} \quad 4\beta(2\beta^2/\delta + 9.0003D) < 3.1(4\beta)^3/\delta,$$

we can show by the methods of Lemma 7.10 of [13] that

$$|p_2 + p_3\delta|, |p_2 - p_3\delta| > \delta|f|/3\beta; \qquad |x_\pi|, |y_\pi| > \frac{I_1\delta|f|}{3\beta} - \beta.$$

Thus, we can find that $|x_\pi||p_2 + p_3\delta|, |y_\pi||p_1 - p_3\delta| > 2|f|$, and therefore

$$|\xi_\omega/\xi_\pi - x_\omega/x_\pi|, |\eta_\omega/\eta_\pi - y_\omega/y_\pi| < 1/2.$$

Since $|[x_\omega/x_\pi] - [y_\omega/y_\pi]| \leqslant 1$, it follows that

$$|[\xi_\omega/\xi_\pi] - [\eta_\omega/\eta_\pi]| \leqslant 3,$$

and we have the result from Lemma 8.4. □

LEMMA 8.7. *Let* Π *and* Ω *be defined as in Lemma* 8.4, *and suppose that* $\{1, \pi, \omega\}$ *is a basis of* $\mathfrak{R}$ *and one of* ξ_π *or* $|\eta_\pi|$ *exceeds* $\sqrt{3}/4$. *If* $I_1 > 3.1(4\beta^3)/\delta$ *and* $j = [x_\omega/x_\pi] - [y_\omega/y_\pi]$, *then* j *and* $[\xi_\omega/\xi_\pi] - [\eta_\omega/\eta_\pi]$ *have the same sign.*

Proof. We use the result that

$$\xi_\omega\eta_\pi - \eta_\omega\xi_\pi = 3\sqrt{3}\,Df/2\rho^2$$

and the method of Lemma 7.11 of [18]. □

Let $K_1(a, b)$, $K_2(a, b)$, $K_3(a, b)$ denote, respectively, the matrices

$$\begin{pmatrix} a & 1 \\ b & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix}, \quad \begin{pmatrix} 0 & a \\ 1 & b \end{pmatrix}.$$

Let $I_1 > 3.1(4\beta)^3/\delta$, $I_2 > 2(3\beta)^3/\sqrt{3}\,\delta$. We now give that part of the reduction algorithm that we call

Algorithm R1

(i) Transform the basis $\{1, \mu, \nu\}$ of (8.1) by $\left(\begin{smallmatrix} k_1 & 0 \\ 0 & k_2 \end{smallmatrix}\right)$, where $k_1 = \operatorname{sgn}(x_\mu)$, $k_2 = \operatorname{sgn}(x_\nu)$.

(ii) If $x_\nu > x_\mu$ go to (iii); otherwise, transform the basis by $K_2(1, 1)$ and go to (iii) unless $y_\nu y_\mu < 0$ and $|y_\nu| > |y_\mu|$. If this latter case occurs, transform the basis by $K_1(0, 1)$ instead of $K_2(1, 1)$ and then go to (v).

(iii) If $y_\nu y_\mu < 0$ go to (iv); otherwise

(1) If $[y_\nu/y_\mu] = [x_\nu/x_\mu] = k$, transform the basis by $K_1(-k, 1)$ until $[y_\nu/y_\mu] \neq [x_\nu/x_\mu]$. When such a basis is found, execute one of the following steps.

(2) If $[x_\nu/x_\mu] + 1 = [y_\nu/y_\mu] = k$, transform the basis by $K_1(k, -1)$ and go to (iv).

(3) If $k = [x_\nu/x_\mu] = [y_\nu/y_\mu] + 1$, transform the basis by $K_1(-k, 1)$ and go to (iv).

(4) If $[x_\nu/x_\mu] < [y_\nu/y_\mu] - 1$, execute the *find* step and terminate R1 when $|\bar{y}_\mu|$ and $\bar{x}_\mu < I_2\rho$. If $|\bar{y}_\mu| \geqslant I_2\rho$, transform the basis by $K_2([y_\nu/y_\mu], -1)$ and go to (v); if $|\bar{y}_\mu| < I_2\rho$ and $\bar{x}_\mu \geqslant I_2\rho$ transform the basis by $K_1([x_\nu/x_\mu] + 1, -1)$ and go to (v).

(5) If $[x_\nu/x_\mu] > [y_\nu/y_\mu] + 1$, execute the *find* step and terminate R1 when $|\bar{y}_\mu|$, $\bar{x}_\mu < I_2\rho$. If $|\bar{y}_\mu| \geqslant I_2\rho$, transform the basis by $K_2(-[y_\nu/y_\mu] - 1, 1)$ and go to (v); if $|y_\mu| < I_2\rho$ and $\bar{x}_\mu \geqslant I_2\rho$, transform the basis by $K_1(-[x_\nu/x_\mu], 1)$ and go to (v).

(iv) If $|y_\mu| > |y_\nu|$, go to (v). If $|y_\mu| \leqslant |y_\nu|$ and $|\bar{y}_\mu|$, $\bar{x}_\mu < I_2\rho$, execute the *find* step and terminate R1. If $|\bar{y}_\mu| \geqslant I_2\rho$, transform the basis by $K_2([-y_\nu/y_\mu], 1)$ and go to (v); if $|\bar{y}_\mu| < I_2\rho$ and $\bar{x}_\mu \geqslant I_2\rho$, transform the basis by $K_1(-[x_\nu/x_\mu], 1)$ and go to (v).

(v) If $|\bar{y}_\nu| \leqslant I_2\rho$ and $|\bar{y}_\mu| \geqslant I_2\rho$, terminate algorithm R1. If $\bar{x}_\mu < I_2\rho$ and $|\bar{y}_\mu| < I_2\rho$, execute the *find* step and terminate R1; otherwise, go to (vi).

(vi)(1) If $|\bar{y}_\nu| > I_2\rho$, transform the basis by $K_3(1, k)$, where $k = [-y_\mu/y_\nu]$ and go to (v). If $|\bar{y}_\nu| \leqslant I_2\rho$, go to (2).

(2) If $|\bar{y}_\mu| \leqslant I_2\rho$, transform the basis by $K_1(-k, 1)$, where $k = [x_\nu/x_\mu]$ and go to (v).

THEOREM 8.8. *Suppose that we execute algorithm* R1 *up to the beginning of step* (v), *and suppose further that it was not necessary, during this process, to go to the find step. If* $\{1, \kappa, \lambda\}$ *is the basis of* $\mathfrak{R}$ *that the algorithm has produced up to the beginning of step*

(v), *then we must have*

$$\xi_\lambda > \xi_\kappa > 0, \quad |\eta_\kappa| > |\eta_\lambda|, \quad \eta_\lambda \eta_\kappa < 0,$$

where $(\xi_\lambda, \eta_\lambda)$ *and* $(\xi_\kappa, \eta_\kappa)$ *are, respectively, the punctures of* Λ $(\approx \lambda)$ *and* K $(\approx \kappa)$.

Proof. Analogous to that of Theorem 7.12 of [18]. We use ρ instead of σ_r and β instead of $(1 + \sqrt{5})\delta^2$. □

LEMMA 8.9. *Let* κ, λ *be as described in Theorem* 8.7. *We must have*

$$\xi_\lambda/3, \xi_\kappa/3, |\eta_\lambda|/\sqrt{3}, |\eta_\kappa|/\sqrt{3} < 3\beta\delta/2\rho.$$

Proof. Let $\{1, \mu, \nu\} = \{1, (m_1 + m_2\delta + m_3\delta^2)/\rho, (n_1 + n_2\delta + n_3\delta^2)/\rho\}$ be the new basis which results after step (i) of R1 has been executed. Note that (8.6) is still true. If $\{1, \bar{\mu}, \bar{\nu}\}$ is the basis produced from $\{1, \mu, \nu\}$ after step (ii) of R1 has been executed, by Lemma 8.3 we have 3 possible cases:

(1) $$\begin{cases} \bar{\mu} = \mu \\ \bar{\nu} = \nu \end{cases} \quad \text{when } \xi_\nu > \xi_\mu;$$

(2) $$\begin{cases} \bar{\mu} = \nu \\ \bar{\nu} = \mu \end{cases} \quad \text{when } \xi_\nu < \xi_\mu, |\eta_\nu| > |\eta_\mu|, \eta_\nu\eta_\mu < 0;$$

(3) $$\begin{cases} \bar{\mu} = \mu \\ \bar{\nu} = \mu + \nu \end{cases} \quad \text{when } \xi_\nu < \xi_\mu \text{ and either } \eta_\nu\eta_\mu > 0 \text{ or } |\eta_\nu| < |\eta_\mu|.$$

In the third of these cases, we see that

$$\eta_{\bar{\nu}}\eta_{\bar{\mu}} = \eta_\mu^2 + \eta_\mu\eta_\nu.$$

If $\eta_\mu\eta_\nu > 0$, then $\eta_{\bar{\nu}}\eta_{\bar{\mu}} > 0$. If $\eta_\mu\eta_\nu < 0$, then $|\eta_\nu| < |\eta_\mu|$ and

$$\eta_{\bar{\nu}}\eta_{\bar{\mu}} = |\eta_\mu|(|\eta_\mu| - |\eta_\nu|) > 0.$$

That is, in this case, one of the substeps of step (iii) of R1 will be executed next. Thus, if we arrive at the beginning of step (v) by skipping over all the substeps of (iii) and step (iv), then we must have $\lambda = \mu$, $\kappa = \nu$ or $\lambda = \nu$, $\kappa = \mu$.

Suppose that this is how we did arrive at the beginning of step (v), and suppose further that $\lambda = \mu$ and $\kappa = \nu$. Then $\xi_\kappa/3 < \xi_\lambda/3 = \xi_\mu/3 < \delta(2\beta)/2\rho$ and $|\eta_\kappa| > |\eta_\lambda|$. If $\xi_\kappa < 1/3$, then $|n_2 + n_3\delta| < 2\rho/9\delta$. Since $|n_3\delta| < \beta$ and $3\beta\delta > \rho$, we find that $|n_2 - n_3\delta| < 2\rho/9\delta + 2\beta$ and $|\eta_\kappa|/\sqrt{3} = |\eta_\nu|/\sqrt{3} < 3\delta\beta/2\rho$. If $\xi_\kappa > 1/3$, we use the result

$$|\xi_\lambda\eta_\kappa - \xi_\kappa\eta_\lambda| = 3\sqrt{3}\, D|f|/2\rho^2, \tag{8.8}$$

together with the facts $\eta_\kappa\eta_\lambda < 0$ and $\xi_\lambda > \xi_\kappa > 1/3$, to show that

$$|\eta_\kappa|/\sqrt{3} < 3Df/2\rho^2\xi_\lambda < 9D|f|/2\rho^2 < 3\beta\delta/2\rho.$$

If, instead, we have $\lambda = \nu$, $\kappa = \mu$ at the beginning of step (v), we can show the truth of the lemma by using a similar argument. The only significant change in the proof is that we first assume $|\eta_\lambda| < 1/2\sqrt{3}$ and then assume $|\eta_\lambda| > 1/2\sqrt{3}$.

If we arrive at the beginning of step (v) by executing one of the substeps of (iii) or step (iv), then we must execute one of substep 4 or substep 5 of (iii) or step (iv). Let $\{1, \bar{\kappa}, \bar{\lambda}\}$ be the basis of R1 which we have obtained from R1 just before either of

(iii)–4, (iii)–5 or (iv) is executed. If $(\xi_{\bar{\kappa}}, \eta_{\bar{\kappa}})$ is the puncture of $\bar{K}$ ($\approx \bar{\kappa}$), we certainly have

$$|\xi_{\bar{\kappa}}|/3, \qquad |\eta_{\bar{\kappa}}|/\sqrt{3} < \delta\beta/\rho.$$

If in any of the above steps ((iii)–4, (iii)–5, or (iv)), we start with $|\bar{y}_{\bar{\kappa}}| \geqslant I_2\rho$, then a transformation of the type $K_2(a, b)$ is used and $\kappa = \bar{\kappa}$. It follows that $|\eta_\kappa| > \sqrt{3}/4$ and from (8.8)

$$\xi_\lambda/3 < 2D|f|/\rho^2 < \beta\delta/\rho.$$

Also, $|\eta_\lambda|/\sqrt{3} < |\eta_\kappa|/\sqrt{3} < \delta\beta/\rho$.

If we start with $|\bar{x}_{\bar{\kappa}}| \geqslant I_2\rho$, then a transformation of the type $K_1(a, b)$ is used and we get $\lambda = \bar{\kappa}$. Thus, $\xi_\kappa > \sqrt{3}/4$ and $|\eta_\kappa|/\sqrt{3} < 3\beta\delta/2\rho$. The rest of the results follow from the facts $\lambda = \bar{\kappa}$ and $\xi_\lambda > \xi_\kappa$. □

LEMMA 8.10. *Let* $\{1, \mu, \nu\}$ *be any basis of* $\mathfrak{R}$ *such that* $\xi_\nu > \xi_\mu > 0$, $|\eta_\mu| > |\eta_\nu|$ *and* $\eta_\nu\eta_\mu < 0$. *If* $|\eta_\mu| > \sqrt{3}/4$, $|\bar{y}_\nu| \geqslant I_2\rho$, $|\eta_\nu|/\sqrt{3} < 3\beta\delta/2\rho$, *then* $|\eta_\nu| > \sqrt{3}/4$, $|n_2| + |n_3|\delta < 3\beta$ *and* $|n_2|$, $|\delta n_3| < 8\delta^2$; *if* $\xi_\nu > \sqrt{3}/4$, $\bar{x}_\mu \geqslant I_2\rho$, $\xi_\mu/3 < 3\beta\delta/2\rho$, *then* $\xi_\mu > \sqrt{3}/4$, $|m_2| + |m_3|\delta < 3\beta$ *and* $|m_2|$, $|\delta m_3| < 8\delta^2$.

Proof. We prove the last part only; the proof of the first part is similar. Since $\xi_\nu > \sqrt{3}/4$, we have

$$|\eta_\mu| < \frac{4}{\sqrt{3}} \cdot \frac{3\sqrt{3}\,D|f|}{2\rho^2} \quad \text{and} \quad |m_2 - m_3\delta| < \frac{12\delta^2}{\sqrt{3}}.$$

Since $|m_2 + m_3\delta| < (3\beta\delta/2\rho)(2\rho/\delta) = 3\beta$ $(> 12\delta^2/\sqrt{3})$, we see that $|m_2| + |m_3\delta| < 3\beta$. Also, $|m_2|$, $|\delta m_3| < 1/2(3\beta + 12\delta^2/\sqrt{3}) < 8\delta^2$. By Lemma 8.1, we have $\xi_\mu > \sqrt{3}/4$. □

We are now able to present the main result of this section.

THEOREM 8.11. *Algorithm* R1 *either executes the find step before it terminates or it terminates with a basis* $\{1, \psi, \phi\}$ *of* $\mathfrak{R}$ *such that*

$$\xi_\phi > \xi_\psi > 0, \quad |\eta_\phi| < |\eta_\psi|, \quad \eta_\phi\eta_\psi < 0,$$

$$|\eta_\phi| < 1 - \sqrt{3}/4, \quad |\eta_\psi| > \sqrt{3}/4, \quad |\eta_\psi| > (1 - |\eta_\phi|)/2.$$

Proof. Let $\{1, \mu, \nu\}$ be the basis of $\mathfrak{R}$ which algorithm R1 has produced up to the beginning of step (v), but before step (v) is ever executed. By Lemma 8.9, we have $|m_2| + |m_3|\delta < 3\beta$, $|n_2| + |n_3|\delta < 3\beta$. Thus, if $|\bar{y}_\nu| \leqslant I_2\rho$ and $|\bar{y}_\mu| \geqslant I_2\rho$, we know from Lemma 8.1 that $|\eta_\nu| < 1 - \sqrt{3}/4$ and $|\eta_\mu| > \sqrt{3}/4$. Also, if $\bar{x}_\mu < I_2\rho$ and $|\bar{y}_\mu| < I_2\rho$, then $|\xi_\mu|$, $|\eta_\nu| < 1 - \sqrt{3}/4$ and the *find* step will obtain a value of γ_g. Suppose that we have $|\bar{y}_\mu| < I_2\rho$, $\bar{x}_\mu \geqslant I_2\rho$ and $|\bar{y}_\nu| < I_2\rho$. We must go to substep (vi)–2. Since $|m_2| + |m_3\delta| < 3\beta$, we have $\xi_\nu > \xi_\mu > \sqrt{3}/4$ by Lemma 8.1 and Theorem 8.8. Hence, $|m_2 + m_3\delta| > \rho/2\sqrt{3}\,\delta$ and

$$|f|/|m_2 + m_3\delta| + |m_3| < 2\sqrt{3}\,\delta + 8\delta$$

by Lemma 8.10. Since $I_1 > 3.1\delta^2(2\sqrt{3}\,\delta + 8\delta)^3$, we must have $[x_\nu/x_\mu] = [\xi_\nu/\xi_\mu]$ by Corollary 7.5.1 of [18]. If we put $\eta_\mu^{(1)} = \eta_\nu$, $\eta_\mu^{(2)} = \eta_\mu$, $\xi_\mu^{(1)} = \xi_\nu$, $\xi_\mu^{(2)} = \xi_\mu$, $\mu^{(1)} = \nu$, $\mu^{(2)} = \mu$, $k_i = [x_\mu^{(i)}/x_\nu^{(i+1)}]$, we see, by Lemma 8.10, that as long as $\bar{x}_\mu^{(i)} \geqslant I_2\rho$ and

$|\bar{y}_\mu^{(i)}| < I_2\rho$ for $i = 1, 2, 3, \ldots, j$, substep 2 of (vi) will generate two sequences

$$\eta_\mu^{(1)}, \eta_\mu^{(2)}, \eta_\mu^{(3)}, \ldots, \eta_\mu^{(j)},$$

$$\xi_\mu^{(1)}, \xi_\mu^{(2)}, \xi_\mu^{(3)}, \ldots, \xi_\mu^{(j)},$$

such that $\eta_\mu^{(i+1)} = -k_i\eta_\mu^{(i)} + \eta_\mu^{(i-1)}$, $\xi_\mu^{(i+1)} = -k_i\xi_\mu^{(i)} + \xi_\mu^{(i-1)}$, $\mu^{(i+1)} = -k_i\mu^{(i)} + \mu^{(i-1)}$.

Also

$$|\eta_\mu^{(1)}| < |\eta_\mu^{(2)}| < |\eta_\mu^{(3)}| < \cdots < |\eta_\mu^{(j)}|,$$

$$\xi_\mu^{(1)} > \xi_\mu^{(2)} > \xi_\mu^{(3)} > \cdots > \xi_\mu^{(j)},$$

$k_i = [\xi_\mu^{(i)}/\xi_\mu^{(i+1)}]$ and $\eta_\mu^{(i)}\eta_\mu^{(i-1)} < 0$, $i = 2, 3, \ldots, j$.

We also see that if $m_2^{(i)} + m_3^{(i)}\delta = 2\rho\xi_\mu^{(i)}/3\delta$, then $|m_2^{(i)}| + \delta|m_3^{(i)}| < 3\beta$ for $i = 1, 2, 3, \ldots, j$ (Lemma 8.10). Since there are only a finite number of possibilities for $(m_2^{(i)}, m_3^{(i)})$, there must be a finite value for j such that either $\bar{x}_\mu^{(j)} < I_2\rho$ or $|\bar{y}_\mu^{(j)}| \geqslant I_2\rho$. If $\bar{x}_\mu^{(j)} < I_2\rho$ and $|\bar{y}_\mu^{(j)}| < I_2\rho$, then since $\xi_\mu^{(j)} > 0$, we have $0 < \xi_\mu^{(j)} < 1 - \sqrt{3}/4$ by (8.7) and $|\eta_\mu^{(j)}| < 1 - \sqrt{3}/4$ and we send the basis $\{1, \mu^{(j)}, \mu^{(j-1)}\}$ to the *find* step. If $|\bar{y}_\mu^{(j-1)}| < I_2\rho$ and $|\bar{y}_\mu^{(j)}| \geqslant I_2\rho$, then we have $\{1, \phi, \psi\} = \{1, \mu^{(j)}, \mu^{(j-1)}\}$. By Lemma 8.1, we have $|\eta_\psi| > \sqrt{3}/4$, $|\eta_\phi| < 1 - \sqrt{3}/4$. Also, if

$$\psi = \left(t_1 + t_2\delta + t_3\delta^2\right)/\rho, \qquad \phi = \left(s_1 + s_2\delta + s_3\delta^2\right)/\rho,$$

then

$$|\eta_\psi| = |\bar{y}_\psi|/2\rho I_2 + \alpha,$$

where $\alpha < (|t_2| + |t_3|)/2\rho I_2 < 3\beta/2\rho I_2$. Also, $|\eta_\phi|/2 = \sqrt{3}\,\delta\,|s_2 - s_3\delta|/4\rho > \sqrt{3}\,\delta/4\rho(|s_2| + |s_3|\delta)^2$ by Lemma 7.1 of [18]. Hence

$$|\eta_\phi|/2 > \sqrt{3}\,\delta/4\rho(3\beta)^2 > 3\beta/2\rho I_2 > |\alpha|$$

and

$$|\eta_\psi| > \left(1 - |\eta_\phi|\right)/2.$$

The proof of the theorem for the case in which we use substep 1 of (iv) instead of substep 2 follows by using similar reasoning. (See Theorem 8.3 of [18].) □

9. Determination of γ_g. As we have seen in Section 8, we have an algorithm R1 which either finds a value γ_g or obtains ϕ and ψ such that (7.3) holds. We will now show how we can obtain a value for γ_g (if one exists) when we know ϕ and ψ.

We first put

$$X_\psi = t_2[I_3\delta] + t_3[I_3\delta^2], \qquad Y_\psi = t_2[I_3\delta] - t_3[I_3\delta^2],$$

$$X_\phi = s_2[I_3\delta] + s_3[I_3\delta^2], \qquad Y_\phi = s_2[I_3\delta] - s_3[I_3\delta^2],$$

where $I_3 \in \mathfrak{Z}$. Since

$$-|t_2| - |t_3| + \left|\frac{2\rho}{\sqrt{3}} I_3\eta_\psi\right| < |Y_\psi| < \left|\frac{2\rho}{\sqrt{3}} I_3\eta_\psi\right| + |t_2| + |t_3|,$$

we see that $|\eta_\psi| < \sqrt{3}/2$ when $|Y_\psi| < \rho I_3 - |t_2| - |t_3|$. Also, if

$$(|t_2| + |t_3|)\sqrt{3}/2I_3\rho < .03,$$

then $|\eta_\psi| < 1.19$ when $5|Y_\psi| < 6\rho I_3$ and $|\eta_\psi| > 1$ when $5|Y_\psi| > 6\rho I_3$. Thus, if $I_3 > 100\beta$, we see by Theorem 7.7 and its corollaries that we have the possibilities shown in Table 2 for the set $\mathfrak{A}$ of Section 7.

TABLE 2

Restrictions Y_ψ	$\mathfrak{A}$
$\lvert Y_\psi\rvert < \rho I_3 - \lvert t_2\rvert - \lvert t_3\rvert$	$\{(1,0),(0,1),(1,-1)\}$
$5\lvert Y_\psi\rvert < 6\rho I_3$	$\{(1,0),(0,1),(1,-1),(1,1)\}$
$5\lvert Y_\psi\rvert > 6\rho I_3$	$\{(1,0),(1,-1),(1,1),(2,1)\}$

Let $|\mathfrak{A}| = k$, and put $q_i = a_i s_1 + b_i t_1$, $X_i = a_i X_\phi + b_i X_\psi$, $Y_i = a_i Y_\phi + b_i Y_\psi$, $d_i = |a_i s_2 + b_i t_2| + |a_i s_3 + b_i t_3| < 9\beta$, $\omega_i = a_i\phi + b_i\psi$ for $(a_i, b_i) \in \mathfrak{A}$, $1 \leqslant i \leqslant k$. If γ_g exists, by Theorem 7.7, it must have the form $l + \omega_i$, $l \in \mathfrak{L}$ and $1 \leqslant i \leqslant k$. We first note that if

$$|Y_i| > \left[\frac{2\sqrt{3}}{2}\rho I_3\right] + 1 + d_i, \tag{9.1}$$

then $|\eta_{\omega_i}| > 1$ and $\gamma_g \neq \omega_i + l$. Thus, if (9.1) is true, we can eliminate (a_i, b_i) from $\mathfrak{A}$ and decrease k by 1. Also, if (9.1) is not true, then

$$|\eta_{\omega_i}| < 2 \quad \text{when } I_3 > \sqrt{3}\,/2(d_i + 1)/\rho > 9\beta.$$

We now require

LEMMA 9.1. *Let* $\Omega\ (\approx \omega) \in \mathfrak{R}$, *where* $\omega = (q_1 + q_2\delta + q_3\delta^2)/\rho$, *and let* $\overline{\Omega}\ (\approx \overline{\omega})$, *where* $\overline{\omega} = l + \omega$ *and* $l \in \mathfrak{L}$. *Put* $I_3 > d = |q_2| + |q_3|$, $X = q_2[I_3\delta] + q_3[I_3\delta^2]$, $j = [X/I_3]$, $l_1 = [(j - 2q_1)/2\rho]$, $l_2 = l_1 + 1$. *If* $jI_3 - X > -d$ *and* $2\rho | j - 2q_1$, *put* $l_3 = l_1 - 1$ *and* $u = 3$; *if* $jI_3 - X < d - I_3$ *and* $2\rho | j + 1 - 2q_1$, *put* $l_3 = l_1 + 2$ *and* $u = 3$; *otherwise, put* $u = 2$. *If* $|\zeta_{\overline{\omega}}| < 1$, *we must have* $l \in \{l_i \mid 1 \leqslant i \leqslant u\}$. *Further, if* $l \in \{l_i \mid 1 \leqslant i \leqslant u\}$, *then* $|\zeta_{\overline{\omega}}| < 2$.

Proof. If $|\zeta_{\overline{\omega}}| < 1$, then

$$-1 < l + (2q_1 - q_2\delta - q_3\delta^2)/2\rho < 1.$$

Now $q_2\delta I_3 + q_3\delta^2 I_3 = X + \alpha$, where $|\alpha| < d$; hence,

$$-1 + (X/I_3 - 2q_1)/2\rho + \alpha/2\rho I_3 < l < 1 + (X/I_3 - 2q_1)/2\rho + \alpha/2\rho I_3.$$

Let $j - 2q_1 = 2\rho l_1 + r$, where $0 \leqslant r \leqslant 2\rho - 1$. Since $[(X/I_3 - 2q_1)/2] = [(j - 2q_i)/2\rho] = l_1$, we have

$$0 < (X - 2q_1 I_3)/2\rho I_3 - l_1 = (X - I_3 j + rI_3)/2\rho I_3 < 1$$

and

$$-1 + \alpha/2\rho I_3 + (X - I_3 j + rI_3)/2\rho I_3 < l - l_1 < 1 + \alpha/2\rho I_3 + (X - I_3 j + rI_3)/2\rho I_3.$$

Hence $-1 \leqslant l - l_1 \leqslant 2$. If $l = l_1 + 2$, we must have

$$\alpha/2\rho I_3 + (X - I_3 j + rI_3)/2\rho I_3 \geqslant 1.$$

Since $0 \leqslant (X - I_3 j)/2\rho I_3 < 1/2$, we see that this can happen only when $r = 2\rho - 1$. In this case we must also have $X - I_3 j + \alpha \geqslant I_3$ and therefore $X - I_3 j + d > I_3$. Similarly, we can show that if $l = l_1 - 1$, then $r = 0$ and $I_3 j - X > -d$.

On the other hand, if $\bar{\omega} = \omega + l_i = l_1 + \kappa + \omega$ $(1 \leqslant i \leqslant u)$, then

$$\begin{aligned}\zeta_{\bar{\omega}} &= \kappa/2\rho + \left(2\rho l_1 + 2q_1 - q_2\delta - q_3\delta^2\right)/2\rho \\ &= \kappa/2\rho - \alpha/2\rho I_3 - (X - I_3 j + rI_3)/2\rho I_3.\end{aligned}$$

Since $|\kappa/2\rho - \alpha/2\rho I_3 - (X - I_3 j + rI_3)/2\rho I_3| < 2$, we see that $|\zeta_{\bar{\omega}}| < 2$. □

We now let l_{ir} $(1 \leqslant r \leqslant u_i)$ be the values of l_r specified by Lemma 9.1 for each ω_i defined above. Put $q_{ir} = q_i + \rho l_{ir}$, $\Omega_{ir} \approx \omega_{ir} = l_{ir} + \omega_i$, where $1 \leqslant i \leqslant k$, $1 \leqslant r \leqslant u_i$ and let

$$\mathfrak{W} = \{I_3 q_{ir} + X_i \mid 1 \leqslant i \leqslant k, 1 \leqslant r \leqslant u_i\},$$
$$\mathfrak{P} = \{\Omega_{ir} \mid 1 \leqslant i \leqslant k, 1 \leqslant r \leqslant u_i\}.$$

We prove

LEMMA 9.2. *If $I_3 > 487\beta\sqrt{D}$ and W_{ir} is the least element of $\mathfrak{W}$ such that $\Omega_{ir} \in \mathcal{C}$, then either $\Omega_{ir} \in \mathcal{C}_1$ or there does not exist a value for γ_g in $\mathfrak{R}$.*

Proof. Certainly, in view of the remark made earlier in this section and Lemma 9.1, if there exists a value of γ_g in $\mathfrak{R}$, then one of the elements of $\mathfrak{P}$ must lie in $\mathcal{C}_1$. Since $\xi_{\omega_{ir}} > 0$, we see that if $\Omega_{ir} \in \mathcal{C}$ and $\omega_{ir} < 1$, then $\Omega_{ir} \in \mathcal{C}_1$ by Lemma 7.1. Let Θ $(\approx \theta) \in \mathfrak{P}$ such that $\Theta \in \mathcal{C}_1$ and $\Theta \neq \Omega_{ir}$. Let W_1 be the value in $\mathfrak{W}$ corresponding to Θ, and let W_2 be the value in $\mathfrak{W}$ corresponding to Ω_{ir}. If $\Omega_{ir} \notin \mathcal{C}_1$, then $\omega_{ir} > 1 > \theta$. Let $\chi = \theta - \omega_{ir} < 0$, where $\chi = (x_1 + x_2\delta + x_3\delta^2)/\rho$. We have $|x_2| + |x_3\delta| < 3(3\beta) = 9\beta$ since $|s_2| + |s_3|\delta$ and $|t_2| + |t_3|\delta$ are both less than 3β. If $\chi_p = (\xi_\chi, \eta_\chi)$, we have $|\zeta_\chi|, |\eta_\chi| < 3$ since $|\eta_\theta| < 1$, $|\eta_{\omega_{ir}}| < 1$ and $|\zeta_\theta| < 1$, $|\zeta_{\omega_{ir}}| < 2$. If $X \approx \chi$, then $X \in \mathfrak{R}$ and $\sigma\rho|f|$ must divide $N(\rho\chi)$ by Theorem 4.2; hence

$$|N(\chi)| = |\chi|\left(\eta_\chi^2 + \zeta_\chi^2\right) \geqslant \sigma|f|/\rho^2.$$

Since $\eta_\chi^2 + \zeta_\chi^2 < 18$, we have

$$|\chi| > \sigma|f|/18\rho^2$$

and

$$\begin{aligned}I_3\rho|\chi| &> I_3\sigma|f|/18\rho > I_3/18\sqrt{9.0003D} \\ &> 9\beta > |x_2| + |x_3|\delta > |I_3\rho\chi - W_1 + W_2|.\end{aligned}$$

Thus, $\operatorname{sgn}(\chi) = \operatorname{sgn}(W_1 - W_2)$. Since $\chi < 0$ and $W_1 - W_2 \geqslant 0$, we have a contradiction. □

Our algorithm to find a value of γ_g, given ϕ and ψ, can now be given as Algorithm R2 below.

Algorithm R2. Put $I_3 > 487\beta\sqrt{D}$.

(i) Put $\tau = \rho/|f|$, $Q = \tau\rho$. Calculate X_ϕ, Y_ϕ, X_ψ, Y_ψ, as above.

(ii) If $|Y_\psi| < \rho I_3 - |t_2| - |t_3|$, put $k = 3$ and $(a_1, b_1) = (1, 0)$, $(a_2, b_2) = (0, 1)$, $(a_3, b_3) = (1, -1)$. When $5|Y_\psi| < 6\rho I_3$, increase k to 4 and put $(a_4, b_4) = (1, 1)$. When $5|Y_\psi| > 6\rho I_3$, put $k = 4$ and $(a_1, b_1) = (1, 0)$, $(a_2, b_2) = (1, -1)$, $(a_3, b_3) = (1, 1)$, $(a_4, b_4) = (2, 1)$.

(iii) For each pair (a_i, b_i) $(i = 1, 2, \ldots, k)$, calculate $Y_i = a_i Y_\phi + b_i Y_\psi$. If

$$|Y_i| > \left[\frac{2\sqrt{3}}{3}\rho I_3\right] + d_i + 1,$$

where $d_i = |a_i s_2 + b_i t_2| + |a_i s_3 + b_i t_3|$, eliminate the corresponding pair (a_i, b_i) and decrease k by 1. For the remaining pairs (a_i, b_i), calculate $q_i = a_i s_1 + b_i t_1$, $X_i = a_i X_\phi + b_i X_\psi$, put

$$l_{i1} = \left[\left(\left[X_i/I_3\right] - 2q_i\right)/2\rho\right],$$
$$l_{i2} = l_{i1} + 1.$$

If $[X_i/I_3]I_3 - X_i > -d_i$ and $2\rho | [X_i/I_3] - 2q_i$; put $u_i = 3$ and $l_{i3} = l_{i1} - 1$; if $[X_i/I_3]I_3 < d_i - I_3$ and $2\rho | [X_i/I_3] - 2q_i + 1$, put $u_i = 3$ and $l_{i3} = l_{i1} + 2$; otherwise, put $u_i = 2$. Compute $q_{ir} = q_i + \rho l_{ir}$ $(1 \leqslant i \leqslant k;\ 1 \leqslant r \leqslant u_i)$.

(iv) Put $\mathfrak{W} = \{I_3 q_{ir} + X_i \mid 1 \leqslant i \leqslant k,\ 1 \leqslant r \leqslant u_i\}$, and find the minimum $|I_3 q_{\kappa\lambda} + X_\kappa|$ of $\mathfrak{W}$. Put $m_1 = q_{\kappa\lambda}$, $m_2 = a_\kappa s_2 + b_\kappa t_2$, $m_3 = a_\kappa s_3 + b_\kappa t_3$, and calculate the integers

$$\overline{m}_1 = \left(m_1^2 - D m_2 m_3\right)/|f|, \quad \overline{m}_2 = \left(D m_3^2 - m_1 m_2\right)/|f|,$$
$$\overline{m}_3 = \left(m_2^2 - m_1 m_3\right)/|f|, \qquad \Sigma = \left(m_1 \overline{m}_1 + D(m_2 \overline{m}_3 + m_3 \overline{m}_2)\right)/\rho.$$

If $\Sigma < 0$, replace m_i by $-m_i$ $(i = 1, 2, 3)$ and Σ by $-\Sigma$. If

$$\Sigma + 3\tau(\overline{m}_1 \rho - m_1 \Sigma) \geqslant Q^2, \tag{9.2}$$

we cannot have $M \approx \mu = (m_1 + m_2\delta + m_3\delta^2)/\rho$ in $\mathcal{C}$ (Theorem 9.4 of [18]). Thus, we eliminate $I_3 q_{\kappa\lambda} + X_\kappa$ from $\mathfrak{W}$ and return to the beginning of this step. If (9.2) is not true, check that

$$\Sigma + 3\tau m_1 < Q + 3\overline{m}_1. \tag{9.3}$$

If this is not so, then $\mu > 1$ and $M \notin \mathcal{C}_1$. Thus, $\mathfrak{R}$ must be a reduced lattice by Lemma 9.2. If (9.3) holds, then $M \in \mathcal{C}_1$, and we put $n_1 = t_1$, $n_2 = t_2$, $n_3 = t_3$ when $\kappa = 1$; otherwise, put $n_1 = s_1$, $n_2 = s_2$, $n_3 = s_3$. We have a new basis of $\{1, \mu, \nu\}$ of $\mathfrak{R}$, where $\nu = (n_1 + n_2\delta + n_3\delta^2)/\rho$ and $M\ (\approx \mu) \in \mathcal{C}_1$. Thus, we find that $\gamma_g = \mu$ and $\gamma_h = \nu$.

With this algorithm, we are now able to conclude this section by presenting our complete *reduction algorithm*. This algorithm finds, from a given basis of a 1-lattice $\mathfrak{R}$, a reduced lattice $\mathfrak{S}$ such that $\mathfrak{R} \sim \mathfrak{S}$. It also calculates $G = -\log \gamma$, where $\mathfrak{R} = \gamma\mathfrak{S}$ and $\gamma \in \mathfrak{K}$. This algorithm terminates in $O((\log D)^2)$ operations.

Reduction Algorithm

(i) Initialization. Put $j = 1$, $\mathfrak{S}_1 = \mathfrak{R}$, $G = -\log \gamma = 0$.

(ii) Find a *canonical* basis of $\mathfrak{S}_j$ (see Section 4).

(iii) Execute the *pre-reduction step* of Section 8 on this canonical basis of $\mathfrak{S}_j$. If possible, use the *find* step to determine a basis $\{1, \gamma_g^{(j)}, \gamma_h^{(j)}\}$ of $\mathfrak{S}_j$ and go to (v). If this is not possible, go to (iv).

(iv) Execute the algorithm R1 and, if necessary, R2.

(1) If $\mathfrak{S}_j$ is not reduced, then we will find a basis $\{1, \gamma_g^{(j)}, \gamma_h^{(j)}\}$ of $\mathfrak{S}_j$. After doing this, go to (v).

(2) If $\mathfrak{S}_j$ is reduced, terminate the reduction algorithm. We have $\mathfrak{S} = \mathfrak{S}_j$ and $G = -\log \gamma$.

(v) Perform the *invert* step of Section 4 on the basis $\{1, \gamma_g^{(j)}, \gamma_h^{(j)}\}$ of $\mathfrak{S}_j$ to find a basis of the lattice $\mathfrak{S}_{j+1} = |\gamma_g^{(j)}|^{-1}\mathfrak{S}_j$. Replace G by $G + \log(1/|\gamma_g^{(j)}|)$, increase j by 1 and return to (ii).

10. Implementation and Computational Results. We call the process by which we obtain a basis $\{1, \theta_g^{(r+1)}, \theta_h^{(r+1)}\}$ of $\mathfrak{R}_{r+1}$ from a basis $\{1, \theta_g^{(r)}, \theta_h^{(r)}\}$ of $\mathfrak{R}_r$ (see Section 3) a *simple step*. One means of doing this has been fully described in [18]. When this algorithm was implemented for values of $D > 10^6$ it was found that the amount of precision needed by Algorithm II of [18] was large enough to slow the program's running time significantly. To overcome this difficulty we modified Algorithm II along the lines of Algorithm R2 of Section 9.

We replaced step (ii) of Algorithm II by the step

(ii′) If $|Y_\psi| < \sigma_r I_3 - |t_2| - |t_3|$, put $k = 3$ and $(a_1, b_1) = (1,0)$, $(a_2, b_2) = (0,1)$, $(a_3, b_3) = (1,-1)$. When $|Y_\psi| \geqslant \sigma I_3 - |t_2| - |t_3|$ and $4|X_\psi| > \sigma_r I_3$, put $k = 4$ and $(a_1, b_1) = (1,0)$, $(a_2, b_2) = (0,1)$ $(a_3, b_3) = (1,-1)$, $(a_4, b_4) = (1,1)$. When $|Y_\psi| \geqslant \sigma I_3 - |t_2| - |t_3|$ and $4|X_\psi| < \sigma_r I_3$, put $k = 4$ and $(a_1, b_1) = (1,0)$, $(a_2, b_2) = (1,-1)$, $(a_3, b_3) = (1,1)$, $(a_4, b_4) = (2,1)$. Let $\mathfrak{A} = \{(a_i, b_i) \mid 1 \leqslant i \leqslant k\}$.

We also replaced step (iii) by the step

(iii′) For each pair $(a_i, b_i) \in \mathfrak{A}$ calculate $Y_i = a_i Y_\phi + b_i Y_\psi$, $d_i = |a_i s_2 + b_i t_2| + |a_i s_3 + b_i t_3|$. If

$$|Y_i| > \left[\frac{2\sqrt{3}}{3}\sigma_r I_3\right] + d_i + 1,$$

eliminate the corresponding pair (a_i, b_i) from $\mathfrak{A}$ and decrease k by 1. For the remaining pairs in $\mathfrak{A}$ calculate $q_i = a_i s_1 + b_i t_1$, $X_i = a_i X_\phi + b_i Y_\psi$. Put

$$l_{i1} = \left[\left([X_i/I_3] - 2q_i\right)/2\sigma_r\right], \qquad l_{i2} = l_{i1} + 1.$$

If $[X_i/I_3]I_3 - X_i > -d_i$ and $2\sigma_r | [X_i/I_3] - 2q_i$, put $u_i = 3$ and $l_{i3} = l_{i1} - 1$; if

$$[X_i/I_3]I_3 - X_i < d_i - I_3 \quad \text{and} \quad 2\sigma_r | [X_i/I_3] - 2q_i + 1,$$

put $u_i = 3$ and $l_{i3} = l_{i1} + 2$; otherwise, put $u_i = 2$. Compute $q_{ij} = q_i + \sigma_r l_{ij}$ $(1 \leqslant i \leqslant k, 1 \leqslant j \leqslant u_i)$ and $\mathfrak{W} = \{I_3 q_{ij} + X_i \mid 1 \leqslant i \leqslant k, 1 \leqslant j \leqslant u_i\}$.

This new version of Algorithm II is valid for $I_3 > 18^2\sqrt{3}\,\delta^3$, a much smaller value for I_3 than that needed in the old version. This follows from the methods used in Section 9 here, especially Lemma 9.1. We must also make use of the methods of Lemma 9.2 of this work, Lemma 9.3 of [18] and (8.3).

Let $\mathfrak{R}_r$ have $\{1, (m_1 + m_2\delta + m_3\delta^2)/\sigma_r, (n_1 + n_2\delta + n_3\delta^2)/\sigma_r\}$ as a basis, and suppose $R_r = \sum_{i=1}^{r-1} \log \theta_g^{(i)}$. The complete algorithm for a *doubling* step when $\delta^3 = D$ is given below.

Doubling Algorithm

(i) Find a canonical basis of $\mathfrak{R}_r$ as described in Section 4.

(ii) Find a basis of $\mathfrak{R}_r^2$ by using the method of Theorem 6.2. Also, calculate w by the corollary of Theorem 6.2.

(iii) Apply the reduction algorithm of Section 9 to $\mathfrak{R}_r^2$ to find a basis $\{1, \mu, \nu\}$ of a reduced lattice $\mathfrak{S}$ $(\sim \mathfrak{R}_r^2)$, together with $G = -\log \gamma$, where $\gamma\mathfrak{S} = \mathfrak{R}_r^2$. Compute $\overline{R}_r = 2R_r - G - \log w$.

After we have performed this algorithm, we have a new reduced lattice $\mathfrak{S} = \mathfrak{R}_m = \langle 1, \mu, \nu \rangle$ such that $m \simeq 2r$. Further $R_m = \overline{R}_r$.

We will also require an algorithm which, given some lattice $\mathfrak{R}_r$ and another lattice $\mathfrak{R}_k$, finds a lattice $\mathfrak{R}^* = \mathfrak{R}_n$ with $R^* = R_n$, where $n \simeq k + r$. We call this the *large step algorithm*. We first put $P_i = \sigma_i/\gcd(\sigma, e_i)$; this is $L(\mathfrak{a}_i)$ for the ideal $\mathfrak{a}_i$ corresponding to $\mathfrak{R}_i$.

Large Step Algorithm

(i) Find $\mathfrak{R}_j$ such that $\gcd(P_r, P_j) = 1$ and $R_j \leqslant R_k$.

(ii) Find canonical bases for $\mathfrak{R}_r$ and $\mathfrak{R}_j$.

(iii) Use formulas (5.15) to find a basis of $\mathfrak{R} = \mathfrak{R}_j\mathfrak{R}_r$.

(iv) Apply the reduction algorithm of Section 9 to $\mathfrak{R}$ to find a basis of a reduced lattice $\mathfrak{R}^*$ $(\sim \mathfrak{R})$ together with $G = -\log \gamma$, where $\gamma\mathfrak{R}^* = \mathfrak{R}$. Since $\gcd(L(\mathfrak{a}_i), L(\mathfrak{a}_j)) = 1$, we have $t = 1$ in (3.5) and $R^* = R_r + R_j - G$. (Note that $R^* \leqslant R_r + R_j$.)

Remark. In order to accomplish step (i), it is often convenient to have a pre-computed list of lattices $\mathfrak{R}_{k-i}$ $(i = 1, 2, 3, \ldots, m)$. Since the probability that two randomly selected integers be relatively prime is $6/\pi^2$, m need not be very large. Of course, one could dispense entirely with this search step by using the formulas in Section 5 to obtain a general composition algorithm for finding $\mathfrak{R}_k\mathfrak{R}_r$. Such an algorithm would execute in $O(\log D)$ operations. However, in practice, the search for $\mathfrak{R}_j$ here is usually very brief. In fact, we found that most often $j = k$ or $k - 1$.

We will also need the following simple lemma.

LEMMA 10.1. *Suppose we are given t lattices*

$$\mathfrak{R}_b, \mathfrak{R}_{2b}, \mathfrak{R}_{3b}, \ldots, \mathfrak{R}_{tb}, \tag{10.1}$$

together with the values of $R_b, R_{2b}, R_{3b}, \ldots, R_{tb}$. *Suppose further that* $R_{tb} \leqslant R$ *and* $\overline{\mathfrak{R}}$ *is a lattice such that* $\overline{R} = mR$, *where* $m \in \mathfrak{Z}$ *and* $m \geqslant 1$. *If* $R_r < \overline{R} \leqslant R_n$, *where* $R_n - R_r \leqslant R_{b(t-1)}$, *then one of the lattices*

$$\mathfrak{R}_n, \mathfrak{R}_{n+1}, \mathfrak{R}_{n+2}, \ldots, \mathfrak{R}_{n+b-1}$$

must be one of the lattices in (10.1).

Proof. Let $\theta_n = \varepsilon_0^{q_1}\theta_u$, $\theta_r = \varepsilon_0^{q_2}\theta_v$, where $1 \leqslant \theta_u, \theta_v < \varepsilon_0$. Then $\mathfrak{R}_u = \mathfrak{R}_n$, $\mathfrak{R}_v = \mathfrak{R}_r$ and $R_u, R_v < R$. Since $R_n - R_r < R$, we get

$$0 < R_r - (m-1)R < R \leqslant R_n - (m-1)R < 2R.$$

Thus,

$$R_v = R_r - (m-1)R, \quad R_u = R_n - mR \quad \text{and} \quad R_u + R - R_v \leqslant R_{b(t-1)}.$$

Since $R - R_v > 0$, we have $R_u < R_{t(b-1)}$. It follows that one of the b lattices $\mathfrak{R}_n, \mathfrak{R}_{n+1}, \mathfrak{R}_{n+2}, \ldots, \mathfrak{R}_{n+b-1}$ must be one of the lattices in (10.1). □

By using this lemma we can develop the *search algorithm*. We assume that the sequence of lattices (10.1) has been pre-computed and that $\mathfrak{R}_k = \mathfrak{R}_{(t-1)b}$. Given a lattice $\mathfrak{R}_r$ and an upper bound B, this algorithm finds (if it exists) the value of $\bar{R}$ for a lattice $\bar{\mathfrak{R}}$ such that

$$R_r < \bar{R} \leqslant B \quad \text{and} \quad \bar{R} = mR \qquad (m \in \mathfrak{Z},\ m \geqslant 1).$$

It does this by searching the range between R_r and B in large steps of size R_k.

The Search Algorithm

(i) Use $\mathfrak{R}_r$ and $\mathfrak{R}_k$ with the large step algorithm above to find $\mathfrak{R}^*$ and R^*.

(ii) Assuming $\mathfrak{R}_n = \mathfrak{R}^*$, perform simple steps on $\mathfrak{R}_n$ to find

$$\mathfrak{R}_n, \mathfrak{R}_{n+1}, \mathfrak{R}_{n+2}, \ldots, \mathfrak{R}_{n+b-1}. \tag{10.2}$$

(iii) Compare each of the lattices of (10.2) with the t lattices of (10.1). This is most rapidly accomplished if the σ_{bi} values for the lattices in (10.1) have been pre-sorted. If any $\sigma_{bi} = \sigma_{n+j}$, compare $|e_{bi}|$ and $|e_{n+j}|$. If they are not equal, we do not have a match; if they are equal, then compare $\mathfrak{R}_{bi}$ and $\mathfrak{R}_{n+j}$ by finding a canonical basis for both and comparing coefficients. (If the search routine is to be used frequently, it is a good idea to pre-compute canonical bases for the lattices in (10.1).) If we get a match $\mathfrak{R}_{bi} = \mathfrak{R}_{n+j}$, then $\bar{R} = R_{n+j} - R_{bi}$, and we terminate the algorithm. If we do not find a match, go to (iv).

(iv) If $B \leqslant R^*$, the algorithm terminates, and we know that $\bar{\mathfrak{R}}$ does not exist. If $B > R^*$, put $\mathfrak{R}_r = \mathfrak{R}^*$, $R_r = R^*$ and return to (i).

If we know in advance that there are two elements $\Theta_i\ (\approx \theta_i)$, $\Theta_j\ (\approx \theta_j)$ in the chain (3.1) such that $\theta_i < \theta_j < \varepsilon_0$ and $N(\theta_i) | J^2$, $N(\theta_j) | J^2$ (see [15], [16] for some simple criteria), put $p = 1$; otherwise, put $p = 0$. When $p = 1$, we have $\varepsilon_0 = \theta_i^3 / N(\theta_i)$ and $R = 3R_i - \log N(\theta_i)$.

We are now ready to give the algorithm for finding R and h. We assume that $E = \sqrt{3}\, c_2 J F(Q)/2\pi$ has been pre-computed and that we have values for input parameters, D, E, L, b, t, x, k.

The Main Algorithm

(i) By using simple steps starting from $\mathfrak{R}_1$ calculate and store in memory a table of lattices each of which is represented by the set of integers

$$\{m_1^{(i)}, m_2^{(i)}, m_3^{(i)}, n_1^{(i)}, n_2^{(i)}, n_3^{(i)}, \sigma_i\},$$

where the corresponding lattice $\mathfrak{R}_i$ has basis

$$\{1, (m_1^{(i)} + m_2^{(i)}\delta + m_3^{(i)}\delta^2)/\sigma_i, (n_1^{(i)} + n_2^{(i)}\delta + n_3^{(i)}\delta^2)/\sigma_i\}.$$

We also store the corresponding value of R_i. The lattices we store are $\mathfrak{R}_{jb}$ $(j = 1, 2, 3, \ldots, t)$. It is also convenient when performing large steps to have a table of lattices $\mathfrak{R}_{tb-j}$ $(j = 0, 1, 2, 3, \ldots, 2b)$. If in the process of creating these tables, we find R, that is, $R \leqslant 3R_{bt} - \log J^2$ when $p = 1$ or $R \leqslant R_{bt}$ when $p = 0$, then we can usually calculate h from E without much trouble (see [1]), and we are done. We may assume that $R_{bt} < R$ for the rest of this algorithm.

(ii) Put $L_1 = R_{bt}$, and find that value of κ such that $E/2^\kappa < L_1$ and $E/2^{\kappa-1} > L_1$. Put $U = E/2^\kappa$, and find in the table produced in step (i) that lattice $\mathfrak{R}_{iu}$ such that

$R_{iu} < U$ and $R_{i(u+1)} > U$. Perform simple steps starting with $\mathfrak{R}_{iu}$ to find that lattice $\mathfrak{R}_n$ such that $R_n < U$ and $R_{n+1} > U$. Put $\lambda = 1$.

(iii) Perform the *Doubling* step on $\mathfrak{R}_n$ to produce $\mathfrak{R}_m$ and R_m. Perform simple steps, starting with $\mathfrak{R}_m$ to obtain $\mathfrak{R}_b$ and R_b, where $R_b < 2^\lambda U$ and $R_{b+1} > 2^\lambda U$. Increment λ by 1, and replace $\mathfrak{R}_n$ and R_n by $\mathfrak{R}_b$ and R_b, respectively, If $\lambda \leqslant \kappa$, return to the beginning of step (iii); otherwise go to (iv).

(iv) We now have a lattice $\mathfrak{R}_n$ where $R_n \simeq E$. Use the search algorithm to find R starting at R_n and going up to $B = E + L$. If this is unsuccessful, replace E by $E - L$ and go to (ii). If this fails to find $\bar{R}$, we say that the algorithm fails and we either increase L or terminate the algorithm; otherwise, we now have $\bar{R} = hR$. Put $E = \bar{R}$.

(v) We now determine h. We first put $i = h^* = 1$, $H = E$.

(vi) Find v and all primes q_a $(a = 1, 2, 3, \ldots, v)$ such that $q_1 = 2$, $q_a > q_{a-1}$, and $q_a < \sqrt{E/kL_1}$ $(a = 1, 2, 3, \ldots, v)$.

(vii) If $i \leqslant v$ go to (1); otherwise, go to (2).

(1) By using the methods of (ii) and (iii), find $\mathfrak{R}_n$ and R_n such that $R_n < E/q_i - x$ and $R_{n+1} > E/q_i - x$. That is, we use $E/q_i - x$ for E in (ii) and (iii) in order to find $\mathfrak{R}_n$. Perform simple steps starting with $\mathfrak{R}_n$ until we find some $\mathfrak{R}_k$ such that $\sigma_k = 1$ or $R_k > E/q_i + x$. If the former case occurs, we know that $q_i | h$. We replace the value of h^* by that of $q_i h^*$, the value of E by that of E/q_i and return to (vi). If the latter case occurs, we know that $q_i \nmid h$. We increment i by 1, and we return to the beginning of step (vii).

(2) Starting with $\mathfrak{R}_r = \mathfrak{R}_{bt}$, use the search algorithm to find $\bar{R}$ with $B = \sqrt{kL_1 E} + x$.

(viii) If, in executing (2) we find $\bar{R}$, then $R = \bar{R}$ and $h = h^*(E/R)$. If we do not find $\bar{R}$, then $R > \sqrt{kL_1 E}$. Hence, $h/h^* < E/\sqrt{kL_1 E} = \sqrt{E/kL_1}$. Thus, if $q | (h/h^*)$, then $q < \sqrt{E/kL_1}$ and, since all such q's have been examined, it follows that $h = h^*$ and $R = H/h$.

Remarks. (1) We could have stored all of the lattices computed in step (i) instead of $1/b$ of them; but, if we wish L_1 to be large, this may require more storage than the computer is capable of handling.

(2) We make use of x in substeps (vii)–1, and (vii)–2 in order to ensure that we do not skip over any lattices that should be examined. This could happen because of round off or truncation errors in the evaluation of R_n or $\bar{R}$. For example, the computer's estimate of R_n might be less than E or E/q_i, but the actual value of R_n might not be. The value of x need not be very large but must be large enough to overcome this possibility.

(3) It is difficult to find what value to use for L here. We give below a theoretic estimate which requires the truth of a certain Generalized Riemann Hypothesis (GRH). However, a glance at the results in Table 3 will show that this estimate for L will often be much larger than that needed in practice. In the range of values of D used here we found that L between 50000 and 300000 would usually work.

(4) Because we cannot be sure of how good our approximation $F(Q)$ is to $\Phi(1)$, we cannot prove with full mathematical rigour that the value we get here for h is correct. From the results given below we would expect that $F(Q)$ should give a reasonable approximation to $\Phi(1)$ when Q is fairly large. Hence, when h is small, our method is

very likely to find it correctly. In spite of our slight lack of confidence in h, however, the value that we obtain for R is correct. This is simply because we get a value of $\bar{h}R$ in step (iv), and then we find $\bar{h}$ in step (viii). Nowhere in the process of finding $\bar{h}$ did we really have to assume that it was actually h.

As indicated in Remark (3) above, a problem in running this algorithm is knowing what value to give L. We now discuss a theoretic estimate of a value for L which ensures that $\bar{R}$ will be found. This requires an analysis of how good an approximation E is to hR. Of course we will find $\bar{R}$ when

$$L > |E - hR| .$$

Let $\prod'_x$ (Σ'_x) represent the product (sum) over all primes q such that $q > x$, $q \equiv 1 \pmod 3$ and $q \nmid J$. Let $Q > 3$, and put $T(Q) = \prod'_Q f(q)$. Then

$$\Phi(1) = c_2 F(Q) T(Q)$$

and

$$|E - hR| < c_2\sqrt{3}\, JF(Q)\,|1 - T(Q)|/2\pi.$$

In order to estimate $T(Q)$, we will use a method very similar to that employed by Cornell and Washington [5].

We have

$$T(Q) = \prod_Q{}' q^2/(q^2 + \varepsilon(q)q + 1),$$

where

$$\varepsilon(q) = \begin{cases} -2 & \text{when } (D/q)_3 = 1, \\ 1 & \text{when } (D/q)_3 \neq 1. \end{cases}$$

Hence,

$$\log T(Q) = -\sum_Q{}' \varepsilon(q)/q + \gamma,$$

where $|\gamma| < 3/Q$. Put $B(Q) = \Sigma'_Q \varepsilon(q)/q$ and $A(t) = \Sigma_{q \leq t} \varepsilon(q)$. We now require the effective version of the Chebotarev Density Theorem of Lagarias and Odlyzko [7] with constants given by Oesterlé [10]. This requires further that we assume the truth of the GRH for the zeta function $\zeta_{\mathfrak{S}}$, where $\mathfrak{S} = \mathfrak{Q}(\sqrt[3]{D}, \rho)$ and $\rho^2 + \rho + 1 = 0$.

We note that $n_{\mathfrak{S}} = [\mathfrak{S}: \mathfrak{Q}] = 6$ and $d_{\mathfrak{S}}$, the discriminant of $\mathfrak{S}$, is $27J^4$. Further, if G is the Galois group of $\mathfrak{S}$, then $|G| = 6$. Now $A(t) = -2\pi_{C_1}(t) + \pi_{C_2}(t)$, where the symbols C and π_C are defined in [10]; also, $|C_1| = 1$, $|C_2| = 2$. Thus, by [10]

$$A(t) = -2\pi_{C_1}(t) + \frac{2|C_1|}{|G|}\mathrm{Li}(t) + \pi_{C_2}(t) - \frac{|C_2|}{|G|}\mathrm{Li}(t)$$

and

$$\begin{aligned} |A(t)| &\leq \frac{2}{3}\sqrt{t}\left[\left(\frac{1}{\pi} + \frac{5.3}{\log t}\right)\log 27J^4 + 6\left(\frac{\log t}{2\pi} + 2\right)\right] \\ &= \sqrt{t}\,(\log t)C(t), \end{aligned}$$

where $C(t)$ is a monotone decreasing function of t. By using the reasoning of [5] we find that

$$|B(Q)| < \left(\frac{4 + 3\log Q}{\sqrt{Q}}\right) C(Q).$$

When $Q^5 > \max(10^{30}, 27J^4)$, $J > 10^6$, then

$$|1 - T(Q)| < \frac{6\log(27J^4Q)}{\sqrt{Q}}$$

and

$$|E - hR| < \frac{3\sqrt{3}\,c_2}{\pi\sqrt{Q}} J\log(27J^4Q)F(Q).$$

Since evaluating E requires $O(Q)$ operations and, by Mertens' Theorem,

$$F(Q) < \prod_{q \leq Q}\left(\frac{q}{q-1}\right)^2 = \left[\prod_{q \leq Q}(1 - 1/q)\right]^{-2} \sim (e^{\gamma}\log Q)^2,$$

we see that if $L_1 \simeq D^{2/5}$, then in order to evaluate E and $\bar{R}$ we require (putting $Q = D^{2/5}$) $O(D^{2/5+\varepsilon})$ operations. Further, since $\sqrt{kEL_1}/L_1 = O(D^{3/10+\varepsilon})$, we see that we require $O(D^{2/5+\varepsilon})$ operations to find R and h by the above algorithm under the GRH for $\zeta_{\mathfrak{S}}$.

Let r be the number of steps required by Voronoi's algorithm to find R. Since $R = \sum_1^r \log \theta_g^{(t)}$ and $1 < \theta_g^{(t)} < 1 + \xi_\theta$, where $(\xi_\theta, \eta_\theta)$ is the puncture of $\Theta_g^{(t)}$, we have $R < r\log(1 + (3\sqrt{3} + 3)D)$ by formula 6.8 of [18]. In fact, it seems by empirical results that $R \simeq 1.12r$. From the results developed above, we see that we have $Rh = O(D^{1-\varepsilon})$. Thus, we expect Voronoi's algorithm to take about $O(D/h)$ steps to find R. Even if we do not assume the GRH, we can use the well-known result that $\Phi(1) = O((\log|\Delta|)^{1+\varepsilon})$. With this we can show that our ideas will provide a method which executes in $O(D^{1/2+\varepsilon})$ operations. Thus, if h is small our new method is faster than that which uses a straight application of Voronoi's algorithm.

The algorithm described above was implemented in FORTRAN-*H* (extended) for an AMDAHL 470-*V*7 computer. The extended precision feature allowed us to operate on numbers of up to 33 decimal digits. For values of $D < 2^{31}$, this amount of precision is sufficient except for the *find* step and the *invert* step. For these steps we obtained more precision by using special purpose multi-precision assembler language subroutines. This program was usually run with $L = 50000$, $b = 15$, $k = 10$, $t = 1500$. On running the program, we found that the amount of time taken to perform a simple step was about 4.3 milliseconds. The time required to perform a doubling step or a large step was usually between 100 and 400 milliseconds, the average time being 250 milliseconds. Most of this time was consumed by the multi-precision *find* and *invert* sections of the reduction algorithm. In Table 3 below, we give some results of running our program for large values of D. These values were selected with an eye to obtaining large values of R; hence, the values of D are primes congruent to 2 or 5 (mod 9) such that $\Phi(1)$ is large.

TABLE 3

D	E	hR	R	h
1079021	2734906.136341	2733739.063036	341717.382879	8
2609069	7400272.677097	7399896.890644	3699948.445321	2
2961713	7665950.516997	7663248.163765	7663248.163765	1
3650249	9782563.073006	9781303.600000	4890651.800000	2
4248551	11409669.209399	11408545.752473	2852136.438118	4
7191911	19018244.808396	19012522.349931	9506261.174966	2
8688161	23904403.372750	23896176.735251	5974044.183831	4
9488513	26068028.870131	26068015.858615	2606801.585862	10
14613773	39788531.398671	39783254.555210	4972906.819401	8
16477553	43721343.379590	43716350.599929	63541.207267	688
17353643	44095839.633036	44116470.280843	8823294.056169	5
18209801	52783288.770296	52790989.627523	13197747.406881	4
19196813	52633382.613328	52632827.706395	26316413.853197	2
19446881	51387164.594867	51375468.466817	51375468.446817	1
19914539	54729047.586607	54736734.178735	5473673.417873	10
20281169	53486260.159788	53488442.838074	53488442.838074	1
21745121	57252172.105084	57258743.313504	57258743.313504	1
23301797	61614171.225781	61611468.798065	12322293.759613	5
23444777	61469132.178084	61462434.613230	61462434.613230	1
20006741	46521260.090157	46524073.006668	46524073.006668	1
20007749	49446137.483399	49428982.133678	24714491.066839	2
20015087	47763949.503176	47766835.229026	23883417.614513	2
20022059	44039595.529345	44048511.873016	3146322.276644	14
20025923	50081813.840435	50049413.717038	25024706.858519	2
20040509	47040758.406428	47029680.710366	47029680.710366	1
20045297	46484105.511038	46493930.428174	46493930.428174	1
20046053	45782490.090580	45787613.586821	22893806.793410	2
20054273	44847449.611742	44843516.182618	44843516.182618	1
20058611	47780427.920252	47760659.269566	47760569.269566	1
20060321	49219975.499996	49221641.419518	12305410.354880	4
20092379	46866613.196961	46861161.134179	5857645.141772	8
20096231	44069991.510614	44055464.985446	22027732.492723	2
20103329	45663222.588792	45666190.521819	22833095.260910	2
20131229	44263821.181251	44265315.438814	44265315.438814	1
20141939	47544122.638427	47526507.556002	4752650.755600	10
20150411	49432033.465649	49407063.942000	24703531.971000	2
20155169	45910007.981908	45925409.600054	22962704.800027	2
20156681	49108786.477367	49115714.187083	49115714.187083	1
200003987	488445524.404758	488441550.471778	122110387.617945	4
200014823	506589820.204984	506559571.011469	253279785.505735	2
200021333	431868738.397306	431848126.981261	431848126.981261	1
200050859	459913063.601063	459866668.037712	459866668.037712	1
200085059	480458216.172594	480409066.144472	240204533.072236	2
200087861	537372949.701100	537332554.388950	134333138.597237	4
200089163	437965734.284523	437975996.332267	437975996.332267	1

TABLE 3 (*continued*)

D	E	hR	R	h
200099381	497603952.415591	497590195.640789	124397548.910197	4
200100389	424196870.367996	424203442.573298	424203442.573298	1
200100503	451182094.347744	451197215.352740	451197215.352740	1
200107571	480433899.513446	480444645.440266	480444645.440266	1
200112401	472253194.115455	472167872.629630	118041968.157408	4
200114699	404492099.980046	404488912.856795	202244456.428397	2
200122889	464342463.344755	464299134.881723	58037391.860215	8
200164271	441701163.856313	441705327.026624	220852663.513312	2
200171999	518597740.739617	518594546.969083	518594546.969083	1
200182403	440166276.950028	440210372.576431	220105186.288216	2
200182529	447398884.585019	447390972.406384	22369548.620319	20
200237591	458593160.418426	458631734.208582	229315867.104291	2
1000002821	2224268272.85790	2224244048.137217	2224244048.137217	1
1000021079	2415725386.65008	2415802816.494235	603950704.123559	4
1000022213	2176263035.09785	2176209325.109052	272026165.638631	8
1000027001	2378191472.68543	2378124348.205241	1189062174.102620	2
1000050017	2131249352.94466	2131259056.681105	2131259056.681105	1
1000069643	2178195190.70341	2178254057.347236	544563514.336809	4
1000091399	2235417592.91327	2235363727.828276	1117681863.914138	2
1000115579	2340780764.18363	2340733780.230313	37753770.648876	62
2000001359	5097379160.99403	5097475496.226634	1274368874.056659	4
2000009129	4675237416.61298	4675293317.830901	4675293317.830901	1
2000012477	4148134404.14319	4148034373.232793	4148034373.232793	1
2000029403	4826616791.70067	4826399013.912892	2413199506.956446	2
2000052137	4983495105.51258	4983602513.601523	4983602513.601523	1
2000108111	4605978642.80285	4606048408.531975	1151512102.132994	4
2000131223	4840963289.88280	4840696491.272803	121017412.281820	40
2000145629	4937983529.32301	4937740516.447692	4937740516.447692	1

For $D = 2000145629$, we found the value of hR in 3.6 minutes of CPU time. To test the primes up to 151 as possible divisors of h required 1.8 minutes, and a further 8.6 minutes was needed for the search routine in step (vii)–2 to execute. The total time required to find R and h was 14 minutes. Probably these times could be reduced by careful tuning of the values of the input parameters b, t, k. To find R using Voronoi's algorithm alone would probably require about $(1/3)(4.3 \times 10^{-3})R/1.12$ seconds or 73 CPU days.

11. Acknowledgements. The authors gratefully acknowledge suggestions of H. W. Lenstra, Jr., and R. Schoof for improving the speed of this algorithm. These suggestions led to the development of the search algorithm. They also wish to thank Daniel Shanks for originally suggesting this problem and for his continued interest and encouragement.

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

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

2. W. E. H. BERWICK, "The classification of ideal numbers that depend on a cubic irrationality," *Proc. London Math. Soc.*, v. 12, 1913, pp. 393–429.

3. W. E. H. BERWICK, "The arithmetic of quadratic number fields," *Math. Gazette*, v. 14, 1928, pp. 1–11.

4. J. W. S. CASSELS, "The rational solutions of the diophantine equation $Y^2 = X^3 - D$," *Acta Math.*, v. 82, 1950, pp. 243–273.

5. G. CORNELL & L. WASHINGTON, "Class numbers of cyclotomic fields," *J. Number Theory*. (To appear.)

6. 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.

7. J. C. LAGARIAS & A. M. ODLYZKO, "Effective versions of the Chebotarev density theorem," *Algebraic Number Fields*, Academic Press, New York, 1977, pp. 409–464.

8. E. LANDAU, *Vorlesungen über Zahlentheorie*, Vol. II, Chelsea, New York, 1955.

9. H. W. LENSTRA, JR., *On the Calculation of Regulators and Class Numbers of Quadratic Fields*, Report 80-08, Mathematisch Instituut, Amsterdam, 1980.

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

11. R. J. SCHOOF, *Quadratic fields and factorization*, Studie Week Getaltheorie en Computers, Math. Centrum, Amsterdam, 1980, pp. 165–206.

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

13. D. SHANKS, "A survey of quadratic, cubic and quartic algebraic number fields (from a computational point of view)," *Congressus Numerantium*, v. 17, 1976, pp. 15–40.

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

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

16. H. C. WILLIAMS, "Improving the speed of calculating the regulator of certain pure cubic fields," *Math. Comp.*, v. 34, 1980, pp. 1423–1434.

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

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

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