MATHEMATICS OF COMPUTATION, VOLUME 34, NUMBER 150
APRIL 1980, PAGES 567–611

Calculation of the Regulator of a Pure Cubic Field

By H. C. Williams, G. Cormack and E. Seah

Abstract. A description is given of a modified version of Voronoi's algorithm for obtaining the regulator of a pure cubic field $\mathcal{Q}(\sqrt[3]{D})$. This new algorithm has the advantage of executing relatively rapidly for large values of D. It also eliminates a computational problem which occurs in almost all algorithms for finding units in algebraic number fields. This is the problem of performing calculations involving algebraic irrationals by using only approximations of these numbers.

The algorithm was implemented on a computer and run on all values of D ($\leqslant 10^5$) such that the class number of $\mathcal{Q}(\sqrt[3]{D})$ is not divisible by 3. Several tables summarizing the results of this computation are also presented.

1. Introduction. Let δ be the real root of

$$x^3 - Bx^2 + Cx - D = 0,$$

an irreducible cubic equation with rational integer coefficients B, C, D and negative discriminant Δ. Let $\mathcal{Q}(\delta)$ be the cubic field formed by adjoining δ to the rationals, and let $\mathcal{Q}[\delta]$ be the ring of integers in $\mathcal{Q}(\delta)$. The regulator of $\mathcal{Q}(\delta)$ is $R = \log \epsilon_0$, where ϵ_0 (>1) is the fundamental unit of $\mathcal{Q}(\delta)$.

When $B = C = 0$, we say that $\mathcal{Q}(\delta)$ is a pure cubic field. In Williams [8] an attempt was made to tabulate several pure cubic fields $\mathcal{Q}(\sqrt[3]{D})$ which have D a prime $\equiv -1 \pmod 3$ and class number 1. In doing this it was necessary to evaluate the value of R for each $\mathcal{Q}(\sqrt[3]{D})$. This was done by using the algorithm of Voronoi [6] as described in Delone and Faddeev [3, pp. 282–290] and Beach, Williams and Zarnke [2].

Calculations had to be terminated when $D > 35100$ for two reasons. The first reason was the immense amount of time needed (up to 10 minutes of C.P.U. time on an IBM 370-168 computer) to calculate an individual R value; the second, and more important reason, was that the values of D were getting too large for the precision available to the computer, even using double-precision arithmetic. All methods of evaluating R known to the authors, with one exception, require that it be possible to determine when an algebraic irrational $\alpha \in \mathcal{Q}(\delta)$ exceeds zero. The computer can only calculate an approximation A to α, and when D is large it is not always true that if $A > 0$, then $\alpha > 0$.

Received January 15, 1979; revised September 12, 1979.
AMS (MOS) subject classifications (1970). Primary 12A30, 12A50; Secondary 12–04.

The purpose of this paper is to describe a modification of Voronoi's technique for calculating R in $Q(\sqrt[3]{D})$ which (1) executes rapidly and (2) minimizes the number of calculations which have to be done with irrational numbers. The method of [3, pp. 290 ff.] satisfies (2) but requires large precision when D is large and executes rather slowly. We also present, in the last section, some results of running the programs which were written to implement our algorithm.

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

TABLE 1

Symbol	Description
Z	The set of rational integers
δ	The real zero of an irreducible (over the rationals) cubic polynomial with negative discriminant Δ
$Q(\delta)$	The cubic field formed by adjoining δ to the rationals
$Q[\delta]$	The ring of integers in $Q[\delta]$
M, N	$M = (m_1 + m_2\delta + m_3\delta^2)/\sigma$, $N = (n_1 + n_2\delta + n_3\delta^2)/\sigma$, where $m_1, m_2, m_3, n_1, n_2, n_3, \sigma \in Z$, $\sigma > 0$, and g.c.d.$(m_1, m_2, m_3, n_1, n_2, n_3, \sigma) = 1$
$\mathcal{O}$	A lattice with basis $[1, M, N]$
$\mathcal{R}$	The real lattice derived from $\mathcal{O}$
θ_g	Relative minimum of the second kind adjacent to 1 in a lattice which has 1 as a relative minimum
$\mathcal{R}_1$	Real lattice which has as a basis an integral basis of $Q[\delta]$
$\theta_g^{(r)}$ (θ_g)	Relative minimum of the second kind adjacent to 1 in $\mathcal{R}_r$ $(\mathcal{R})$
$\theta_h^{(r)}$	An element of $\mathcal{R}_r$ such that $[1, \theta_g^{(r)}, \theta_h^{(r)}]$ is a basis of $\mathcal{R}_r$
$\mathcal{R}_{r+1}$	Real lattice with basis $[1, 1/\theta_g^{(r)}, \theta_h^{(r)}/\theta_g^{(r)}]$
Θ_r	$\Theta_r = \prod_{i=1}^{r-1} \theta_g^{(i)}$
Q_r	$Q_r = N(\Theta_r)$, the norm of Θ_r

Symbol	Description
M_r, N_r, e_r	$M_r = (m_1 + m_2\delta + m_3\delta^2)/\sigma_r$, $N_r = (n_1 + n_2\delta + n_3\delta^2)/\sigma_r$ where $m_1, m_2, m_3, n_1, n_2, n_3, \sigma_r \in Z$, $\sigma_r > 0$, g.c.d.$(m_1, m_2, m_3, n_1, n_2, n_3, \sigma_r) = 1$ and $[1, M_r, N_r]$ is a basis of $\mathcal{R}_r$. $e_r = m_2n_3 - n_2m_3$
m_1^*, m_2^*, m_3^*, n_1^*, n_2^*, n_3^*	$(m_1^* + m_2^*\delta + m_3^*\delta^2)/\sigma_r = 1/\theta_g^{(r-1)}$ $(n_1^* + n_2^*\delta + n_3^*\delta^2)/\sigma_r = \theta_h^{(r-1)}/\theta_g^{(r-1)}$ here $m_1^*, m_2^*, m_3^*, n_1^*, n_2^*, n_3^* \in Z$ and g.c.d.$(m_1^*, m_2^*, m_3^*, n_1^*, n_2^*, n_3^*, \sigma_r) = 1$
$\Omega, \Omega', \Omega''$	Ω is an element of $\mathcal{R}_r$, i.e. $\Omega = aM_r + bN_r + c$ $(a, b, c \in Z)$. Also $\Omega = (q_1 + q_2\delta + q_3\delta^2)/\sigma_r$, where $q_1, q_2, q_3 \in Z$. Ω' and Ω'' are the conjugates of Ω.
E_3	Euclidean 3-space
C_Ω	C_Ω is the normed body of Ω; that is $C_\Omega = \{(x, y, z) \mid (x, y, z) \in E_3, \lvert x\rvert \leqslant \lvert\Omega\rvert, y^2 + z^2 \leqslant \Omega'\Omega''\}$
ω $(\xi_\omega, \eta_\omega)$ ζ_Ω	ω is the puncture $(\xi_\omega, \eta_\omega)$ of Ω. Here $\xi_\omega = (2\Omega - \Omega' - \Omega'')/2$, $\eta_\omega = (\Omega' - \Omega'')/2i \quad (i^2 = -1)$, $\zeta_\Omega = (\Omega' + \Omega'')/2$ when $\delta^3 = D$ $(D \in Z)$, $\xi_\omega = 3\delta(q_2 + q_3\delta)/2\sigma_r$, $\eta_\omega = \sqrt{3}\delta(q_2 - q_3\delta)/2\sigma_r$, $\zeta_\Omega = (2q_1 - q_2\delta - q_3\delta^2)/2\sigma_r$.
q_1', q_2', q_3'	$q_1' = q_1^2 - Dq_2q_3$, $q_2' = Dq_3^2 - q_1q_2$, $q_3' = q_2^2 - q_1q_3$
μ, ν	The punctures of M_r and N_r respectively
$g(\kappa)$	$g(\kappa) = (\sqrt{3}(\kappa + 1/2) - \sqrt{1 - (\kappa + 1/2)^2})/2$
β	$\beta = (2 - \sqrt{3})/4$

Symbol	Description
$K_1(a, b)$ $K_2(a, b)$ $K_3(a, b)$	$K_1(a, b) = \begin{pmatrix} a & 1 \\ b & 0 \end{pmatrix}, K_2(a, b) = \begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix}, K_3(a, b) = \begin{pmatrix} 0 & a \\ 1 & b \end{pmatrix}$
E_r	$E_r = \lvert \xi_\mu \eta_\nu - \xi_\nu \eta_\mu \rvert$
$f(x, y)$	$f(x, y) = x^2 + \lvert xy \rvert + y^2$
x_ω, y_ω	$x_\omega = I_1 q_2 + q_3 [I_1 \delta], y_\omega = I_1 q_2 - q_3 [I_1 \delta]$
$\bar{y}_\omega$	$\bar{y}_\omega = [I_2 \sqrt{3} \delta] q_2 - q_3 [I_2 \sqrt{3} \delta^2]$
X_ω, Y_ω	$X_\omega = [I_3 \delta] q_2 + q_3 [I_3 \delta^2], Y_\omega = [I_3 \delta] q_2 - q_3 [I_3 \delta^2]$

2. **Preliminary Observations and Definitions.** For a more general discussion of the ideas presented below see [3] and Steiner [5].

Let $\mathcal{O}$ be a lattice [3] with basis $[1, M, N]$, where

$$M = (m_1 + m_2\delta + m_3\delta^2)/\sigma, \qquad N = (n_1 + n_2\delta + n_3\delta^2)/\sigma,$$

$\sigma, m_1, m_2, m_3, n_1, n_2, n_3 \in Z$ (the set of rational integers), $\sigma > 0$, g.c.d.$(\sigma, m_1, m_2, m_3, n_1, n_2, n_3) = 1$, and δ is defined as in the first paragraph of Section 1. Then $\mathcal{O}$ is made up of the collection of ordered triples $(\Omega, \Omega', \Omega'')$, where

$$\Omega = x + yM + zN, \qquad x, y, z \in Z,$$

and Ω', Ω'' are the conjugate roots of Ω. Since Ω' and Ω'' are complex, we often discuss the real lattice $\mathcal{R}$ which is the collection of points $(\Omega, (\Omega' - \Omega'')/2i, (\Omega' + \Omega'')/2)$ of $\mathcal{E}_3$ (Euclidean 3-space). Here $i^2 = -1$. Since, to each Ω, there corresponds a unique point of $\mathcal{R}$, we often identify this point of $\mathcal{R}$ by using the symbol Ω only and writing

$$\Omega \approx (\Omega, (\Omega' - \Omega'')/2i, (\Omega' + \Omega'')/2).$$

We define the value of e for $\mathcal{R}$ (or $\mathcal{O}$) as

$$e = m_2 n_3 - m_3 n_2.$$

If $\Omega \in \mathcal{R}$, we define its *parameters* to be $|\Omega|$ and

$$\Omega'\Omega'' = ((\Omega' - \Omega'')/2i)^2 + ((\Omega' + \Omega'')/2)^2.$$

We also define the *norm* of Ω, written $N(\Omega)$, to be $\Omega\Omega'\Omega''$ and the *trace* of Ω to be

$\mathrm{Tr}(\Omega) = \Omega + \Omega' + \Omega''$. Note that since $\Omega'\Omega'' = |\Omega'|^2 \geqslant 0$, then Ω and $N(\Omega)$ have the same sign. It should also be noted that [3, p. 274] if Ω and Φ are two points of R such that $\Phi'\Phi'' = \Omega'\Omega''$, then $\Phi = \pm\Omega$.

If $\Omega \in R$, we call the collection of all points $(x, y, z) \in E_3$ such that $|x| \leqslant |\Omega|$ and $y^2 + z^2 \leqslant \Omega'\Omega''$ the *normed body* C_Ω of Ω. That is, the normed body of Ω is a right circular cylinder of radius $\sqrt{\Omega'\Omega''}$ and length $2|\Omega|$. It is oriented in E_3 as illustrated in Figure 1.

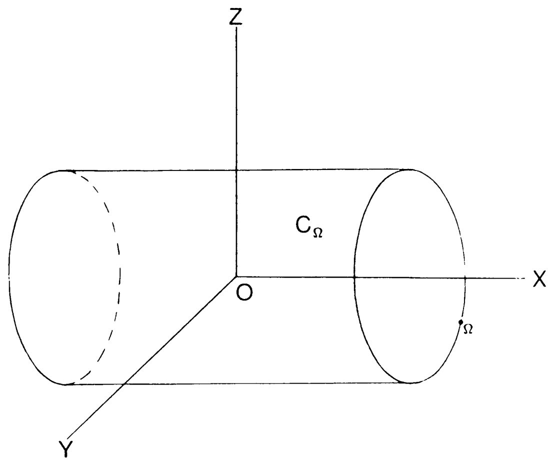

FIGURE 1

We say that Ω $(\neq 0)$ is a *relative minimum* of R (or O) if the only points of R which are in the normed body of Ω are Ω, $-\Omega$ and 0. For example, if $[1, M, N]$ is an integral basis of $Q[\delta]$, then the point $1 \approx (1, 0, 1)$ is a relative minimum of R. For the norm of 1 is 1 and the value of $\Omega\Omega'\Omega''$ for any $\Omega \in R$ is a rational integer; consequently, no point of R except 0, 1 and -1 can lie in the normed body of 1. For the same reason we see that any unit ϵ of $Q(\delta)$ must also be a relative minimum of R.

If Ω, Φ are relative minima of R such that

$$0 < \Phi < \Omega, \qquad \Phi'\Phi'' > \Omega'\Omega''$$

and there does not exist a $\Psi \in R$ such that $\Phi < \Psi < \Omega$ and $\Psi'\Psi'' < \Phi'\Phi''$, we call Φ *the relative minimum of the first kind adjacent* to Ω; and we call Ω *the relative minimum of the second kind adjacent to* Φ. See Figure 2 below.

Geometrically, we see that, given Φ, we find Ω by increasing the length of the cylinder C_Φ until it includes a nonzero point of R. The first such point encountered is Ω. That Ω must exist is guaranteed by the lemma of Minkowski [3, p. 80]. For a given Ω, we find Φ by increasing the radius of the cylinder C_Ω until it includes a point Φ of R such that $\Phi > 0$.

Consider now the sequence

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

where Θ_1 is a relative minimum of R and Θ_{i+1} is the relative minimum of the first kind adjacent to Θ_i for $i = 1, 2, 3, \ldots$. We call such a sequence a *chain* of relative minima of the first kind.

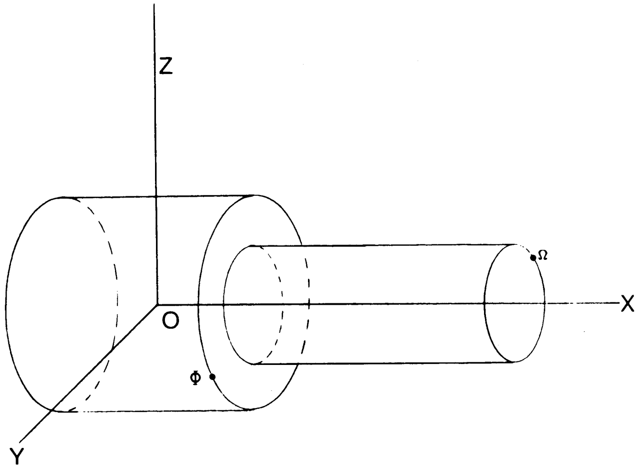

FIGURE 2

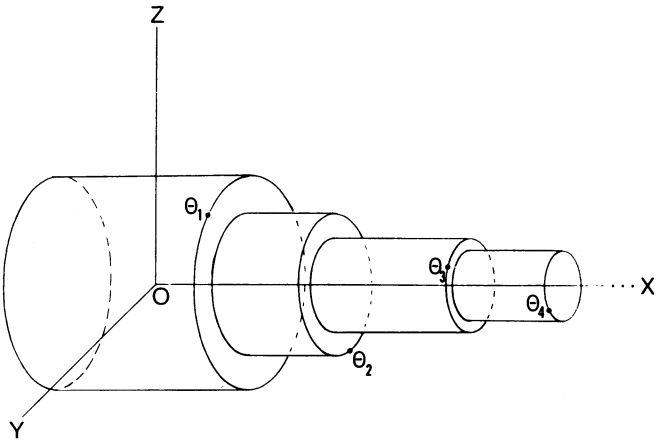

FIGURE 3

If Θ_{i+1} is the relative minimum of the second kind adjacent to Θ_i, we call (2.1) a chain of relative minima of the second kind (see Figure 3). Voronoi's algorithm for determining $\epsilon_0^{-1}(\epsilon_0)$ consists of a method for obtaining a chain of relative minima of the first (second) kind for R when R has as a basis an integral basis of $Q[\delta]$ and $\Theta_1 = 1$, together with a method for determining which member of the chain is $\epsilon_0^{-1}(\epsilon_0)$.

Suppose the basis of $R = R_1$ is $[1, M, N]$, where $[1, M, N]$ is an integral basis of $Q[\delta]$; and suppose we have found the relative minimum of the second kind Θ_2 adjacent to $\Theta_1 = 1$. Put $\theta_g^{(1)} = \Theta_2$ and suppose $[1, \theta_g^{(1)}, \theta_h^{(1)}]$ is a basis of R_1. We let R_2 be the real lattice with basis $[1, 1/\theta_g^{(1)}, \theta_h^{(1)}/\theta_g^{(1)}]$. Clearly 1 is a relative minimum of R_2, and we find $\theta_g^{(2)}$, the relative minimum of the second kind adjacent to 1 in R_2 and $\Theta_3 = \theta_g^{(1)}\theta_g^{(2)}$. We continue in this way finding $[1, \theta_g^{(n)}, \theta_h^{(n)}]$ a basis of R_n and then defining R_{n+1} as having a basis $[1, 1/\theta_g^{(n)}, \theta_h^{(n)}/\theta_g^{(n)}]$ and determining $\theta_g^{(n+1)}$, the relative minimum of the second kind adjacent to 1 in R_{n+1}. We have $\Theta_{n+2} = \theta_g^{(1)}\theta_g^{(2)} \cdots \theta_g^{(n+1)}$. When for some k (>1), $\mathcal{R}_k$ and $\mathcal{R}_1$ are the same lattice or, equivalently, $N(\Theta_k) = 1$ (and k is the least integer (>1) such that this is so), then

$$\epsilon_0 = \Theta_k = \theta_g^{(1)}\theta_g^{(2)} \cdots \theta_g^{(k-1)}$$

and

$$R = \log \epsilon_0 = \sum_{i=1}^{k-1} \log \theta_g^{(i)}.$$

In a later section we shall require the following theorem concerning $\theta_g^{(r)}$.

THEOREM 2.1. *If $\theta_g^{(r)}$ is the relative minimum of the second kind adjacent to 1 in $\mathcal{R}_r$, then $1/\theta_g^{(r)}$ is the relative minimum of the first kind adjacent to 1 in $\mathcal{R}_{r+1}$.*

Proof. Let $[1, \theta_g^{(r)}, \theta_h^{(r)}]$ be a basis of $\mathcal{R}_r$; then $[1, 1/\theta_g^{(r)}, \theta_h^{(r)}/\theta_g^{(r)}]$ is a basis of $\mathcal{R}_{r+1}$. Also, since $\theta_g^{(r)}$ is the relative minimum of the second kind adjacent to 1 in $\mathcal{R}_{r+1}$, we have $1/\theta_g^{(r)} < 1$ and $1/\theta_g^{(r)'}\theta_g^{(r)''} > 1$.

Let Ψ be the relative minimum of the first kind adjacent to 1 in R_{r+1}. Now if $\Theta \in \mathcal{R}_{r+1}$, $\Theta \neq \Psi$ and $0 < \Theta < 1$, we must have $\Theta'\Theta'' > \Psi'\Psi''$; for, if $0 < \Theta < \Psi$, then since C_Ψ contains no points of $\mathcal{R}_{r+1}$ except for 0, Ψ and $-\Psi$, we get $\Theta'\Theta'' > \Psi'\Psi''$. On the other hand, if $\Psi < \Theta < 1$, then $\Theta'\Theta'' > \Psi'\Psi''$ by definition of the relative minimum of the first kind adjacent to 1. Thus, if $\Theta = 1/\theta_g^{(r)}$, we see that

$$0 < \Psi < 1 \quad \text{and} \quad \Psi'\Psi'' < 1/\theta_g^{(r)'}\theta_g^{(r)''}.$$

Since $\Psi = a + b/\theta_g^{(r)} + c\theta_h^{(r)}/\theta_g^{(r)}$ ($a, b, c \in Z$), we have

$$\Omega = \theta_g^{(r)}\Psi = a\theta_g^{(r)} + b + c\theta_h^{(r)} \in \mathcal{R}_r, \qquad 0 < \Omega < \theta_g^{(r)},$$

and $\Omega'\Omega'' < 1$. This contradicts the fact that $\theta_g^{(r)}$ is the relative minimum of the second kind adjacent to 1 in $\mathcal{R}_r$. □

We conclude this section with some simple results concerning the points of $\mathcal{R}_r$ when $\delta^3 = D$ ($D \in Z$). Note that when we deal with the case $\delta^3 = D$, we assume that D is not a perfect integral cube.

If $\Omega \in \mathcal{R}_r$ and $\delta^3 = D$, then

$$\Omega = aM_r + bN_r + c,$$

where $a, b, c \in Z$, $[1, M_r, N_r]$ is a basis of $\mathcal{R}_r$, and

$$M_r = (m_1 + m_2\delta + m_3\delta^2)/\sigma_r, \qquad N_r = (n_1 + n_2\delta + n_3\delta^2)/\sigma_r.$$

Hence $\Omega = (q_1 + q_2\delta + q_3\delta^2)/\sigma_r$, where $q_1, q_2, q_3 \in Z$. If $\Omega \approx (u, v, w)$ in $\mathcal{R}_r$, then

$$u = \Omega, \quad v = \frac{\sqrt{3}}{2\sigma_r}(q_2\delta - q_3\delta^2), \quad w = (2q_1 - q_2\delta - q_3\delta^2)/2\sigma_r.$$

Also,

$$\mathrm{Tr}(\Omega) = 3q_1/\sigma_r, \quad N(\Omega) = (q_1^3 + Dq_2^3 + D^2q_3^3 - 3Dq_1q_2q_3)/\sigma_r^3,$$

and

$$\Omega'\Omega'' = (q_1' + q_2'\delta + q_3'\delta^2)/\sigma_r^2,$$

where

$$q_1' = q_1^2 - Dq_2q_3, \quad q_2' = Dq_3^2 - q_1q_2, \quad q_3' = q_2^2 - q_1q_3.$$

We also have $e_r = m_2n_3 - m_3n_2$. Now an integral basis of $Q[\delta]$ is given by $[1, \delta, \delta^2/g_2]$ when $D \not\equiv \pm 1 \pmod 9$ and by $[1, \delta, (\delta^2 \pm g_2^2\delta + g_2^2)/3g_2]$ when $D \equiv \pm 1 \pmod 9$. Here we assume $D = g_1g_2^2$, where g_1 and g_2 are square free and $(g_1, g_2) = 1$. Thus, $\sigma_1 = e_1$.

3. Some Results Concerning the Bases of R_r. If $[1, M_r, N_r]$ is any basis of R_r, then

$$\begin{pmatrix} 1 \\ M_r \\ N_r \end{pmatrix} = \frac{1}{\theta_g^{(r-1)}} J_{r-1} \begin{pmatrix} 1 \\ M_{r-1} \\ N_{r-1} \end{pmatrix},$$

where $[1, M_{r-1}, N_{r-1}]$ is any basis of R_{r-1} and J_{r-1} is a 3×3 matrix with integer coefficients and $|J_{r-1}| = \pm 1$. From this we get the result

$$\begin{pmatrix} 1 \\ M_r \\ N_r \end{pmatrix} = \frac{1}{\Theta_r} J \begin{pmatrix} 1 \\ M_1 \\ N_1 \end{pmatrix},$$

where J is a 3×3 matrix with integer coefficients such that $|J| = \pm 1$. It follows that $\Theta_r, \Theta_r M_r, \Theta_r N_r \in R_1$. In this section we restrict ourselves to the case in which the basis of R_1 is an integral basis for $Q[\delta]$, when $Q(\delta)$ is a pure cubic field, i.e. $\delta^3 = D$. Put $\sigma = \sigma_1$ and $Q_r = N(\Theta_r)$. The proof of the following theorem makes use of the methods of Section 36 of Voronoi [6].

THEOREM 3.1. *If $\delta^3 = D$ and $Q_r = N(\Theta_r)$, then $e_r | \sigma_r$ and*

$$Q_r = \sigma_r^2 / |e_r| \sigma. \tag{3.1}$$

Proof. Since $\Theta_r, \Theta_r M_r, \Theta_r N_r \in R_1$, we have

$$\sigma\Theta_r = t_{11} + t_{12}\delta + t_{13}\delta^2, \qquad \sigma\Theta_r M_r = t_{21} + t_{22}\delta + t_{23}\delta^2,$$
$$\sigma\Theta_r N_r = t_{31} + t_{32}\delta + t_{33}\delta^2 \qquad (t_{ij} \in Z).$$

If

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

where $\sigma M_1 = \bar{m}_1 + \bar{m}_2\delta + \bar{m}_3\delta^2$, $\sigma N_1 = \bar{n}_1 + \bar{n}_2\delta + \bar{n}_3\delta^2$, then $T = JS$, where $T = (t_{ij})_{3\times 3}$. It follows that $|T| = \pm e\sigma$ $(e = e_1)$.

Let $\Gamma = \Theta_r'\Theta_r''$. Since $\Theta_r \in Q[\delta]$, we see that $\Gamma \in Q[\delta]$ and, therefore, $\sigma\Gamma = g_1 + g_2\delta + g_3\delta^2$ ($g_1, g_2, g_3 \in Z$). Thus, we find that

$$\sigma^2 Q_r = (g_1 + g_2\delta + g_3\delta^2)(t_{11} + t_{12}\delta + t_{13}\delta^2),$$
$$\sigma^2 Q_r M_r = (g_1 + g_2\delta + g_3\delta^2)(t_{21} + t_{22}\delta + t_{23}\delta^2) = u_1 + u_2\delta + u_3\delta^2,$$
$$\sigma^2 Q_r N_r = (g_1 + g_2\delta + g_3\delta^2)(t_{31} + t_{32}\delta + t_{33}\delta^2) = v_1 + v_2\delta + v_3\delta^2,$$

and

$$\begin{pmatrix} \sigma^2 Q_r & 0 & 0 \\ u_1 & u_2 & u_3 \\ v_1 & v_2 & v_3 \end{pmatrix} = T \begin{pmatrix} g_1 & g_2 & g_3 \\ Dg_3 & g_1 & g_2 \\ Dg_2 & Dg_3 & g_1 \end{pmatrix}.$$

Thus, by taking determinants of both sides, we find that

$$\sigma^2 Q_r(u_2v_3 - v_2u_3) = \pm e\sigma^4 N(\Gamma) = \pm e\sigma^4 Q_r^2 \quad \text{and} \quad u_2v_3 - v_2u_3 = \pm e\sigma^2 Q_r.$$

If we put $d^* = \text{g.c.d.}(u_1, u_2, u_3, v_1, v_2, v_3, Q_r\sigma^2)$, we get $\sigma_r = Q_r\sigma^2/d^*$ and $e_r = m_2n_3 - n_2m_3 = \pm e\sigma^2 Q_r/(d^*)^2 = \pm e\sigma_r/d^*$.

Since Γ and $\Theta_r M_r$, $\Theta_r N_r \in Q[\delta]$, we have

$$\Theta_r\Gamma M_r = (u_1 + u_2\delta + u_3\delta^2)/\sigma^2 \in Q[\delta]$$

and

$$\Theta_r\Gamma N_r = (v_1 + v_2\delta + v_3\delta^2)/\sigma^2 \in Q[\delta];$$

therefore, σ is a factor of $\text{g.c.d.}(u_1, u_2, u_3, v_1, v_2, v_3)$ and $\sigma | d^*$. Since $d^* = \pm e\sigma_r/e_r$ and $\sigma = e$, we have the theorem. □

COROLLARY 3.1.1. $\sigma | \sigma_r$.

COROLLARY 3.1.2. $Q_r = 1$ *if and only if* $|e_r| = \sigma_r = \sigma$.

THEOREM 3.2. *If* $\Omega \in R_r$ *and* $\Omega = (q_1 + q_2\delta + q_3\delta^2)/\sigma_r$, *then* $\sigma|e_r|\sigma_r$ is a *factor of* $N(\sigma_r\Omega)$ *and* $e_r | q_i'$ $(i = 1, 2, 3)$, *where* $q_1' = q_1^2 - Dq_2q_3$, $q_2' = Dq_3^2 - q_1q_2$, $q_3' = q_2^2 - q_1q_3$.

Proof. Since $\Omega \in R_r$, we have $\Omega = aM_r + bN_r + c$ ($a, b, c \in Z$); also, since Θ_r, $\Theta_r M_r$ and $\Theta_r N_r \in Q[\delta]$ so is $\Lambda = \Theta_r\Omega \in Q[\delta]$. It follows from (3.1) that

$$N(\sigma_r\Omega) = \sigma_r^3 N(\Omega) = \sigma_r^3 N(\Lambda)/Q_r = \sigma|e_r|\sigma_r N(\Lambda).$$

Since $N(\Lambda)$ is an integer, we have the first part of the theorem.

Now $\Omega'\Omega''/N(\Omega) = 1/\Omega = \Theta_r/\Lambda = \Lambda'\Lambda''\Theta_r/N(\Lambda)$ and consequently $\Omega'\Omega'' = \Lambda'\Lambda''\Theta_r/N(\Theta_r)$. Using the fact that $\sigma_r^2\Omega'\Omega'' = q_1' + q_2'\delta + q_3'\delta^2$, we have

$$q_1' + q_2'\delta + q_3'\delta^2 = \sigma|e_r|\Lambda'\Lambda''\Theta_r.$$

Since Θ, $\Lambda'\Lambda'' \in Q[\delta]$, we have $\Lambda'\Lambda''\Theta \in Q[\delta]$; and, therefore, $e_r | q_i'$ $(i = 1, 2, 3)$. □

In the remainder of this section we discuss a method of finding the basis $[1, 1/\theta_g^{(r-1)}, \theta_h^{(r-1)}/\theta_g^{(r-1)}]$ of R_r when we have the basis $[1, \theta_g^{(r-1)}, \theta_h^{(r-1)}]$ of R_{r-1}.

Let $m_1' = m_1^2 - Dm_2m_3$, $m_2' = Dm_3^2 - m_2m_1$, $m_3' = m_2^2 - m_1m_3$, where $\theta_g^{(r-1)} = (m_1 + m_2\delta + m_3\delta^2)/\sigma_{r-1}$; we have

$$\sigma_{r-1}^2\theta_g^{(r-1)'}\theta_g^{(r-1)''} = m_1' + m_2'\delta + m_3'\delta^2$$

and

$$\sigma_{r-1}^3 N(\theta_g^{(r-1)}) = m_1m_1' + D(m_2m_3' + m_3m_2').$$

Put $d_1 = \text{g.c.d.}(m_1', m_2', m_3')$, $\bar{m}_i = m_i'/d_1$ $(i = 1, 2, 3)$ and $\bar{\sigma}_r = m_1\bar{m}_1 + D(m_2\bar{m}_3 + m_3\bar{m}_2)$. We have

$$1/\theta_g^{(r-1)} = \sigma_{r-1}(\bar{m}_1 + \bar{m}_2\delta + \bar{m}_3\delta^2)/\bar{\sigma}_r$$

and

$$\theta_h^{(r-1)}/\theta_g^{(r-1)} = (n_1' + n_2'\delta + n_3'\delta^2)/\bar{\sigma}_r,$$

where

$$n_1' = \bar{m}_1n_1 + D(\bar{m}_2n_3 + \bar{m}_3n_2), \quad n_2' = \bar{m}_2n_1 + \bar{m}_1n_2 + D\bar{m}_3n_3,$$

$$n_3' = \bar{m}_3n_1 + \bar{m}_2n_2 + \bar{m}_1n_3.$$

If $d_2 = (n_1', n_2', n_3')$, we get

$$n_2(\bar{m}_2^2 - \bar{m}_3\bar{m}_1) \equiv n_3(D\bar{m}_3 - \bar{m}_1\bar{m}_2) \pmod{d_2}$$

from the last two equations. Now

$$\bar{m}_2^2 - \bar{m}_3\bar{m}_1 = m_3\bar{\sigma}_r/d_1, \quad D\bar{m}_3^2 - \bar{m}_1\bar{m}_2 = m_2\bar{\sigma}_r/d_1;$$

hence, $d_2d_1 | \bar{\sigma}_re_{r-1}$. Also, since $\Theta_r = \Theta_{r-1}\theta_g^{(r-1)}$, we have $Q_{r-1}N(\theta_g^{(r-1)}) = Q_r$. From (3.1), we have $Q_{r-1} = \sigma_{r-1}^2/|e_{r-1}|\sigma$; thus, since $N(\theta_g^{(r-1)}) = d_1\bar{\sigma}_r/\sigma_{r-1}^3$, we get $d_1\bar{\sigma}_r = \sigma|e_{r-1}|\sigma_{r-1}Q_r$. If $d = (d_2, \sigma_{r-1}) = (n_1', n_2', n_3', \sigma_{r-1})$, then $e_{r-1}d | d_1\bar{\sigma}_r$ and $dd_1 | \bar{\sigma}_re_{r-1}$; therefore, $d | \bar{\sigma}_r$. We have proved

THEOREM 3.3. *If* $[1, \theta_g^{(r-1)}, \theta_h^{(r-1)}]$ *is a basis of* R_{r-1}, *then* $[1, M_r, N_r]$ *is a basis of* R_r, *where*

$$M_r = 1/\theta_g^{(r-1)} = (m_1^* + m_2^*\delta + m_3^*\delta^2)/\sigma_r,$$
$$N_r = \theta_h^{(r-1)}/\theta_g^{(r-1)} = (n_1^* + n_2^*\delta + n_3^*\delta^2)/\sigma_r,$$

$\sigma_r = \bar{\sigma}_r/d$, $m_i^* = \sigma_{r-1}m_i'/dd_1$, $n_i^* = n_i'/d$ $(i = 1, 2, 3)$.

It should be noted here that since $d_1 = |e_{r-1}|\sigma_r\sigma_{r-1}/|e_r|d$, we have

$$m_i' = |e_{r-1}|\sigma_r m_i^*/|e_r| \quad (i = 1, 2, 3). \tag{3.2}$$

Let $B = [1, M, N]$ be any basis of the lattice R, and let $K = (k_{ij})_{2\times 2}$ be a matrix with integer entries such that $|K| = \pm 1$. We say that we *transform* the basis B by K when we *replace* $[1, M, N]$ by $[1, \bar{M}, \bar{N}]$, where

$$\bar{M} = (\bar{m}_1 + \bar{m}_2\delta + \bar{m}_3\delta^2)/\sigma_r, \quad \bar{N} = (\bar{n}_1 + \bar{n}_2 + \bar{n}_3\delta^2)/\sigma_r$$

and

$$\begin{pmatrix} \bar{m}_1 & \bar{n}_1 \\ \bar{m}_2 & \bar{n}_2 \\ \bar{m}_3 & \bar{n}_3 \end{pmatrix} = \begin{pmatrix} m_1 & n_1 \\ m_2 & n_2 \\ m_3 & n_3 \end{pmatrix} K.$$

Since $|K| = \pm 1$, we see that the transformed basis is also a basis of $\mathcal{R}$. Now, if $m_3 \neq 0$ and

$$K = \begin{pmatrix} 1 & -k \\ 0 & 1 \end{pmatrix},$$

where* $k = [n_3/m_3]$, then $\bar{m}_2 = m_2, \bar{m}_3 = m_3, \bar{n}_2 = n_2 - km_2$, and $\bar{n}_3 = n_3 - km_3$; thus, $|\bar{n}_3/\bar{m}_3| < 1$. Also, since $e_r = \bar{m}_2\bar{n}_3 - \bar{m}_3\bar{n}_2$, we get $|\bar{n}_2| < |e_r|/|m_3| + |m_2|$. If $m_3 = 0$ and $k = [n_2/m_2]$, we have $|\bar{n}_2/\bar{m}_2| < 1$. Thus, if $[1, M, N]$ is a basis of $\mathcal{R}$, we know that there exists a basis $[1, \bar{M}, \bar{N}]$ of $\mathcal{R}$ such that if $m_3 \neq 0$, then

(3.3) $$\bar{m}_2 = m_2, \quad \bar{m}_3 = m_3, \quad |\bar{n}_3| < |\bar{m}_3|, \quad |\bar{n}_2| < |e_r|/|m_3| + |m_2|;$$

or, if $m_3 = 0$, then

(3.4) $$\bar{m}_2 = m_2, \quad \bar{m}_3 = 0, \quad |\bar{n}_2| < |\bar{m}_2|.$$

4. Some Lemmas Concerning the Lattice $\mathcal{R}$. As in Section 2 we let $\mathcal{R}$ be any lattice with basis $[1, M, N]$. Suppose further that $\mathcal{R}$ has 1 as a relative minimum. In Section 5 we show how to determine a small set of possible values for θ_g, the relative minimum of the second kind adjacent to 1 in $\mathcal{R}$; however, in order to do this we must first prove a number of lemmas concerning $\mathcal{R}$.

We define the *puncture* of any $\Omega \in \mathcal{R}$ to be a point $\omega = (\xi_\omega, \eta_\omega)$ in the x-y plane of E_3, where

$$\xi_\omega = (2\Omega - \Omega' - \Omega'')/2, \quad \eta_\omega = \frac{\Omega' - \Omega''}{2i} \qquad (i^2 = -1).$$

That is, if $\Omega \approx (u, v, w)$, then $\omega = F(u, v, w)$, where $F(u, v, w) = (u - w, v)$. Thus, ω is simply the point at which a line passing through Ω and parallel to the line joining the origin of E_3 to $(1, 0, 1)$ meets the x-y plane. We denote the set of all these punctures by L. We also denote by ζ_Ω the value of $(\Omega' + \Omega'')/2$; hence, $\Omega = \xi_\omega + \zeta_\Omega$. When $\delta^3 = D$, we see that if $\Omega = (q_1 + q_2\delta + q_3\delta^2)/\sigma$, then

$$\xi_\omega = 3\delta(q_2 + q_3\delta)/2\sigma, \quad \eta_\omega = \sqrt{3}\delta(q_1 - q_2\delta)/2\sigma,$$

$$\zeta_\Omega = (2q_1 - q_2\delta - q_3\delta^2)/2\sigma.$$

We note here that, if

$$W = \begin{pmatrix} \xi_\mu & \xi_\nu \\ \eta_\mu & \eta_\nu \end{pmatrix},$$

where (ξ_μ, η_μ) and (ξ_ν, η_ν) are, respectively, the punctures of M and N, then when we transform the basis by K, we replace W by WK.

---

*We denote by $[\alpha]$ that rational integer such that $0 < \alpha - [\alpha] < 1$; we also denote by $\{\alpha\}$ the value of $\alpha - [\alpha]$.

Since F is a linear mapping, we see that L is additive; thus, if Φ and Ψ are any two points of $\mathcal{R}$ and $\Omega = a\Phi + b\Psi + c$ $(a, b, c \in Z)$, then the puncture $\omega = (\xi_\omega, \eta_\omega)$ of Ω is given by $\xi_\omega = a\xi_\phi + b\xi_\psi$ and $\eta_\omega = a\eta_\phi + b\eta_\psi$, where $\phi = (\xi_\phi, \eta_\phi)$, $\psi = (\xi_\psi, \eta_\psi)$ are the punctures of Φ and Ψ, respectively. Also, $\zeta_\Omega = a\zeta_\Phi + b\zeta_\Psi + c$. It follows that L is a two-dimensional lattice with basis the punctures of M and N. Thus, if $\Omega_1 = a_1M + b_1N + c_1$, $\Omega_2 = a_2M + b_2N + c_2$ $(a_1, a_2, b_1, b_2, c_1, c_2 \in Z)$, then Ω_1 and Ω_2 have the same puncture if and only if $a_1 = a_2$, and $b_1 = b_2$. Let $\Omega = aM + bN + c$ $(a, b, c \in Z)$ have ω as its puncture. We say that Ω *belongs* to ω if $-1 < \zeta_\Omega < 1$. That is, Ω belongs to ω if it is one of the two points on either side of the x-y plane of $\mathcal{E}_3$ which has ω as a puncture and is closest to the x-y plane. In Figure 4 below both Ω_1 and Ω_2 belong to ω.

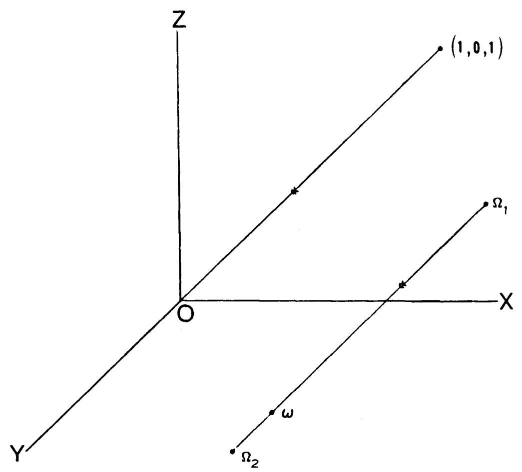

FIGURE 4

We have $\Omega_1 - \Omega_2 = 1$ and $c_1 = [-a\zeta_M - b\zeta_N] + 1$.

Let C be the set $\{(x, y, z) | (x, y, z) \in \mathcal{E}_3$ and $z^2 + y^2 \leqslant 1\}$, i.e. the set of all points of $\mathcal{E}_3$ in or on the cylinder $z^2 + y^2 = 1$, and let C_1 be the normed body of 1. Note that only two points (± 1) of $\mathcal{R}$ lie on the surface of C and no points of $\mathcal{R}$ except 0 and ± 1 are contained in C_1. Note also that $\theta_g \in C$. We have the following

Definition of Ω^*. Let Ω_1 and Ω_2 be the two points which belong to ω. If just one of these is in C, denote it by Ω^*. If both are in C, put $\Omega^* = \Omega_1$ if $|\Omega_1| < |\Omega_2|$; else put $\Omega^* = \Omega_2$. If neither Ω_1 nor Ω_2 is in C, Ω^* is not defined.

Note that in order for $\Omega \in C$, we must have $\zeta_\Omega^2 + \eta_\omega^2 < 1$; hence, if $|\eta_\omega| > 1$, Ω^* does not exist. On the other hand, if $|\eta_\omega| < \sqrt{3}/2$, then Ω^* must exist. Further, if $|\eta_\omega| > \sqrt{3}/2$ and Ω^* exists, then $|\zeta_{\Omega^*}| < 1/2$ and $\Omega^* = c + aM + bN$, where $c = [1/2 - a\zeta_M - b\zeta_N]$. If $|\eta_\omega| < \sqrt{3}/2$ and $\zeta_{\Omega_2} > -1/2$, then $\Omega_2 \in C$ and since $\Omega_1 = \Omega_2 + 1$, we must have $\Omega_2 = \Omega^*$.

We are now able to present several lemmas. These results are analogous to results given in [3] for the case $\Delta > 0$. Wada also made use of results of this type to produce his table [7].

LEMMA 4.1. *If* $\omega = (\xi_\omega, \eta_\omega)$ *is a puncture such that* Ω^* ($> 0, \neq 1$) *exists, then*

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

Proof. Since $\Omega^* \in C$ and $\Omega^* > 0$, we must have $\Omega^* > 1$; also, by definition $|\zeta_{\Omega^*}| < 1$. If $\zeta_{\Omega^*} \geqslant 1 - \sqrt{1 - \eta_\omega^2}$, then $(\zeta_{\Omega^*} - 1)^2 + \eta_\omega^2 \leqslant 1$ and, consequently, $\Omega^* - 1 \in C$. Since $0 < \Omega^* - 1 < \Omega^*$, this contradicts the definition of Ω^*. □

LEMMA 4.2. *If* $\omega = (\xi_\omega, \eta_\omega)$ *is the puncture of* Ω, $\xi_\omega > 0$, *and* $|\eta_\omega| < \sqrt{3}/2$, *then* $\xi_\omega > \sqrt{1 - \eta_\omega^2}$.

Proof. Since $|\eta_\omega| < \sqrt{3}/2$, there must exist $\Omega^* \in R$ with puncture ω. Since $\xi_\omega > 0$ and no point of R except 0 exists within C_1, we must have $\Omega^* > 1$; thus, since $\Omega^* = \xi_\omega + \zeta_{\Omega^*}$ and $\zeta_{\Omega^*} < 1 - \sqrt{1 - \eta_\omega^2}$, we get $\xi_\omega > \sqrt{1 - \eta_\omega^2}$. □

LEMMA 4.3. *Let* $\omega = (\xi_\omega, \eta_\omega)$ *be the puncture of a point* Ω *such that* $\xi_\omega > 0$, $|\eta_\omega| < \sqrt{3}/2$ *and let* $\tau = (\xi_\tau, \eta_\tau)$ *be the puncture of a point* $T \in C$. *If* $\xi_\tau > \xi_\omega$ *and* $\eta_\tau \eta_\omega > 0$, *then* $T > \Omega^*$.

Proof. Suppose $T < \Omega^*$. Since $\xi_\tau > \xi_\omega$ and $T = \xi_\tau + \zeta_T < \xi_\omega + \zeta_{\Omega^*} = \Omega^*$, we see that $\zeta_T < \zeta_{\Omega^*}$. Since $\zeta_T > -1$ and $-\zeta_{\Omega^*} > -1/2$, we have $-3/2 < \zeta_T - \zeta_{\Omega^*} < 0$. Thus, the absolute value of one of $\zeta_T - \zeta_{\Omega^*}$ or $\zeta_T - \zeta_{\Omega^*} + 1$ must be less than $1/2$. If $|\eta_\tau - \eta_\omega| < \sqrt{3}/2$, one of $T - \Omega^*$ or $T - \Omega^* + 1 \in C$.

Since η_τ and η_ω have the same sign, $|\eta_\tau - \eta_\omega| = ||\eta_\tau| - |\eta_\omega||$. If $|\eta_\tau - \eta_\omega| = |\eta_\omega| - |\eta_\tau|$, then $|\eta_\tau - \eta_\omega| < |\eta_\omega| < \sqrt{3}/2$. Suppose that $|\eta_\tau - \eta_\omega| = |\eta_\tau| - |\eta_\omega| > \sqrt{3}/2$; then $|\eta_\tau| > \sqrt{3}/2$. We now assume without loss of generality that $\eta_\omega > 0$ and consider Figure 5 below.

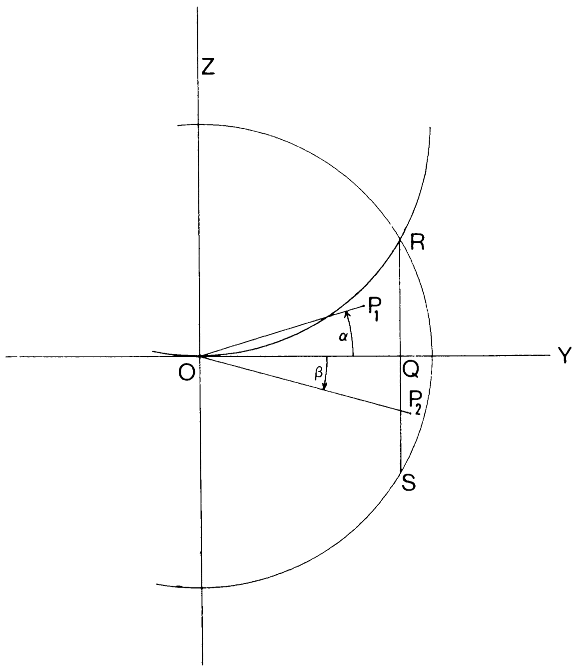

FIGURE 5

Here $P_1 = (\eta_\omega, \zeta_{\Omega^*})$, $P_2 = (\eta_\tau, \zeta_T)$. If we let $d_1 = \overline{OP_1}$, $d_2 = \overline{OP_2}$, $d_3 = \overline{P_1P_2}$, then

$$(\eta_\tau - \eta_\omega)^2 + (\zeta_T - \zeta_{\Omega^*})^2 = d_3^2 = d_1^2 + d_2^2 - 2d_1d_2 \cos(\alpha + \beta).$$

Now $\overline{OQ} = \sqrt{3}/2$ and $\overline{QR} = \overline{QS} = 1/2$; thus, if P_1 lies above the line OP_2 or if P_1 lies below OP_2 and $\zeta_T > 0$, then $\alpha + \beta < \pi/3$ and $\cos(\alpha + \beta) > 1/2$. It follows that

$$d_3^2 < d_1^2 + d_2^2 - d_1d_2 \leqslant \max(d_1^2, d_2^2) \qquad (d_1, d_2 > 0).$$

Since d_1 and $d_2 < 1$, we have $d_3^2 < 1$. If P_1 lies below OP_2 and $\zeta_T < 0$, then since $\zeta_{\Omega^*} > \zeta_T$, the angle between OP_1 and P_1P_2 exceeds $\pi/2$; hence, $d_3 < d_2 < 1$. In each of the cases above we find $d_3 < 1$ and, thus, $(\eta_\tau - \eta_\omega)^2 + (\zeta_T - \zeta_{\Omega^*})^2 < 1$ or $T - \Omega^* \in C$.

Thus, under the assumption that $T < \Omega^*$, we see that either $T - \Omega^* + 1$ or $T - \Omega^* \in C$. If, however, $T - \Omega^* \in C$, then $\zeta_T - \zeta_{\Omega^*} > -1$ and, consequently, $T - \Omega^* > \zeta_T - \zeta_{\Omega^*} > -1$. Since $T - \Omega^* < 0$, we have $T - \Omega^* \in C_1$, which is impossible. If $T - \Omega^* \notin C_1$, then $-3/2 < \zeta_T - \zeta_{\Omega^*} < -1/2$ or $T - \Omega^* + 1 > -1/2$; also, $T - \Omega^* + 1 < 1$; and we have $T - \Omega^* + 1 \in C_1$, which is also impossible. It follows that $T > \Omega^*$. □

LEMMA 4.4. *Let $g(\kappa) = (\sqrt{3}(\kappa + 1/2) - \sqrt{1 - (\kappa + 1/2)^2})/2$. If $0 \leqslant \kappa \leqslant (\sqrt{3} - 1)/2$ and $g(\kappa) \leqslant \lambda \leqslant 1$, then*

$$(\kappa + 1/2)\sqrt{1 - \lambda^2} - \lambda\sqrt{1 - (\kappa + 1/2)^2} \leqslant 1/2.$$

Proof. If $\lambda \geqslant (\sqrt{3}(\kappa + 1/2) - \sqrt{1 - (\kappa + 1/2)^2})/2$, then

$$\lambda^2 + \lambda\sqrt{1 - (\kappa + 1/2)^2} + 1/4 - (\kappa + 1/2)^2 \geqslant 0;$$

consequently,

$$(\kappa + 1/2)^2(1 - \lambda^2) \leqslant \lambda^2(1 - (\kappa + 1/2)^2) + \lambda\sqrt{1 - (\kappa + 1/2)^2} + 1/4,$$

and

$$(\kappa + 1/2)\sqrt{1 - \lambda^2} \leqslant \lambda\sqrt{1 - (\kappa + 1/2)^2} + 1/2. \ \square$$

LEMMA 4.5. *Let $\omega = (\xi_\omega, \eta_\omega)$ be a puncture of a point Ω such that $|\eta_\omega| < 1/2 + \kappa$ $(0 \leqslant \kappa < (\sqrt{3} - 1)/2)$, and let $\tau = (\xi_\tau, \eta_\tau)$ be the puncture of a point $T \in C$. Suppose further that $\xi_\tau = 1 + \lambda + \xi_\omega$, where $\lambda \geqslant 0$. If $\lambda \geqslant g(\kappa)$, we must have $\Omega^* < T$.*

Proof. Suppose $\Omega^* > T$; since $\xi_\tau = 1 + \lambda + \xi_\omega$, we have $1 + \lambda - \zeta_{\Omega^*} + \zeta_T < 0$. From this we see that, since $\zeta_T > -1$, we get $\zeta_{\Omega^*} > \lambda \geqslant 0$. Also, $\zeta_{\Omega^*} < 1/2$ (Lemma 4.1) and $\zeta_T - \zeta_{\Omega^*} > -3/2$; thus,

$$-3/2 < \zeta_T - \zeta_{\Omega^*} < -\lambda - 1 \quad \text{and} \quad \lambda < \zeta < 1/2,$$

where $\zeta = \zeta_{\Omega^*} - \zeta_T - 1$. Now $|\eta_\omega| < 1/2 + \kappa < \sqrt{3}/2$ and (Lemma 4.1)

$$0 < \zeta_{\Omega^*} < 1 - \sqrt{1 - \eta_\omega^2} < 1 - \sqrt{1 - (1/2 + \kappa)^2};$$

hence,

$$|\zeta_T| \geq \zeta_{\Omega^*} - \zeta_T - \zeta_{\Omega^*} > \zeta + \sqrt{1 - (1/2 + \kappa)^2}.$$

If $T - \Omega^* + 1$ is not in C, then

$$(\zeta_T - \zeta_{\Omega^*} + 1)^2 + (\eta_\tau - \eta_\omega)^2 > 1 \quad \text{and} \quad |\eta_\tau - \eta_\omega| > \sqrt{1 - \zeta^2}.$$

Hence,

$$|\eta_\tau| \geq |\eta_\tau - \eta_\omega| - |\eta_\omega| > \sqrt{1 - \zeta^2} - \kappa - 1/2$$

and

$$\begin{aligned}\zeta_T^2 + \eta_\tau^2 &> (\zeta + \sqrt{1 - (1/2 + \kappa)^2})^2 + (\sqrt{1 - \zeta^2} - \kappa - 1/2)^2 \\ &= 2 - 2(\kappa + 1/2)\sqrt{1 - \zeta^2} + 2\zeta\sqrt{1 - (\kappa + 1/2)^2} \\ &> 2 - 2(\kappa + 1/2)\sqrt{1 - \lambda^2} + 2\lambda\sqrt{1 - (\kappa + 1/2)^2} \\ &\geq 1 \quad \text{(by Lemma 4.4)}.\end{aligned}$$

Since $T \in C$, it follows that we must have $T - \Omega^* + 1 \in C$.

Since $\Omega^* > T$, we have $T - \Omega^* + 1 < 1$ and since

$$T - \Omega^* + 1 = \xi_\tau + \zeta_T - \xi_\omega - \zeta_{\Omega^*} + 1 = 2 + \zeta_T - \zeta_{\Omega^*} + \lambda,$$

we have $T - \Omega^* + 1 > 1/2$. Hence, $T - \Omega^* + 1 \in C_1$, i.e. $T - \Omega^* + 1 = 0$; this, however, is impossible since $\xi_\tau > \xi_\omega$. □

5. Determination of θ_g. We now consider the following algorithm [3, p. 453 ff.], which we refer to as Algorithm A. We perform the steps in the indicated order; and we denote by $K_1(a, b)$ a matrix of the form $\begin{pmatrix} a & 1 \\ b & 0 \end{pmatrix}$, by $K_2(a, b)$ a matrix of the form $\begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix}$ and by $K_3(a, b)$ a matrix of the form $\begin{pmatrix} 0 & a \\ 1 & b \end{pmatrix}$.

(i) Transform the basis by $K = \begin{pmatrix} k_1 & 0 \\ 0 & k_2 \end{pmatrix}$, where $k_1 = \operatorname{sgn}(\xi_\mu)$, $k_2 = \operatorname{sgn}(\xi_\nu)$.

(ii) If $\xi_\nu < \xi_\mu$, transform the basis by $K_2(1, 1)$ and go to (iii) unless $\eta_\nu\eta_\mu < 0$ and $|\eta_\nu| > |\eta_\mu|$. If this latter case occurs, transform the basis by $K_1(0, 1)$ and go to (v).

(iii) If $\eta_\mu\eta_\nu < 0$, omit the rest of step (iii) and perform step (iv).

  (a) If $[\xi_\nu/\xi_\mu] = [\eta_\nu/\eta_\mu] = k$, transform the basis by $K_1(-k, 1)$ and continue to perform this step until $[\xi_\nu/\xi_\mu] \neq [\eta_\nu/\eta_\mu]$.

  (b) If $[\xi_\nu/\xi_\mu] + 1 = [\eta_\nu/\eta_\mu] = k$, transform the basis by $K_1(k, -1)$ and go to step (iv).

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

  (d) If $[\xi_\nu/\xi_\mu] < [\eta_\nu/\eta_\mu] - 1$, transform the basis by either of $K_1(k_1, -1)$ or $K_2(k_2, -1)$, where $k_1 = [\xi_\nu/\xi_\mu] + 1$, $k_2 = [\eta_\nu/\eta_\mu]$. Go to step (v).

  (e) If $[\xi_\nu/\xi_\mu] > [\eta_\nu/\eta_\mu] + 1$, transform the basis by either of $K_1(-k_1, 1)$ or $K_2(-k_2, 1)$, where $k_1 = [\xi_\nu/\xi_\mu]$, $k_2 = [\eta_\nu/\eta_\mu] + 1$. Go to step (v).

(iv) If $|\eta_\mu| > |\eta_\nu|$ go to (v); otherwise, transform the basis by either of $K_1(-k_1, 1)$ or $K_2(k_2, 1)$, where $k_1 = [\xi_\nu/\xi_\mu]$, $k_2 = [|\eta_\nu/\eta_\mu|]$.

(v) At this point $\xi_\nu > \xi_\mu > 0$, $\eta_\mu\eta_\nu < 0$, and $|\eta_\nu| < |\eta_\mu|$.

(a) If $|\eta_\nu| > 1/2$ and $|\eta_\mu| < 1/2$, terminate the algorithm.

(b) If $|\eta_\mu| < 1/2$, transform the basis by $K_1(-k_1, 1)$, where $k_1 = [\xi_\nu/\xi_\mu]$ until $|\eta_\mu| > 1/2$. At this point the algorithm terminates.

(c) If $|\eta_\nu| > 1/2$, transform the basis by $K_3(1, k_2)$, where $k_2 = [|\eta_\mu/\eta_\nu|]$, until $|\eta_\nu| < 1/2$. At this point the algorithm terminates.

After this algorithm has terminated we have a new basis $[1, M, N]$ of $\mathcal{R}$ and for this basis it is not difficult to show that μ, ν form a basis for L, $\xi_\nu > \xi_\mu > 0$, $\eta_\mu\eta_\nu < 0$, $|\eta_\nu| < 1/2$, $|\eta_\mu| > 1/2$. In the following theorem we assume the existence of Φ and $\Psi \in \mathcal{R}$ such that $[1, \Phi, \Psi]$ is a basis of $\mathcal{R}$ and $\xi_\phi > \xi_\psi > 0$, $\eta_\phi\eta_\psi < 0$, $|\eta_\phi| < |\eta_\psi|$, $|\eta_\phi| < 1/2 + \beta$, $|\eta_\psi| > 1/3$. Certainly, in view of Algorithm A, such a pair exists. The difficulty occurs in attempting to find them by using an algorithm which uses only a finite amount of precision. We discuss such an algorithm in a later section.

THEOREM 5.1. *If θ is the puncture of θ_g, then*

$$\theta = a\phi + b\psi,$$

where $(a, b) \in S = \{(-1, 2), (1, -2), (1, 0), (0, 1), (1, 1), (1, -1), (2, 1)\}$.

Proof. Clearly, $\theta = a\phi + b\psi$ for some $(a, b) \in Z^2$; also $\theta_g \in \mathcal{C}$ and, therefore, $|\eta_\theta| < 1$.

If $a < 0$, then $b > 0$; also, $|\eta_\theta| = |a||\eta_\phi| + b|\eta_\psi| < 1$. Since $|\eta_\psi| > 1/3$, it follows that $b \leqslant 2$. Since $\xi_\theta = b\xi_\psi - |a|\xi_\phi > 0$, we have $|a| < b$ and, therefore, $(a, b) = (-1, 2)$.

If $a = 0$, then since $\xi_\theta = b\xi_\psi$ and $|\eta_\theta| = b|\eta_\psi|$, we see that $0 < b < 3$. If $b = 2$, then $|\eta_\psi| < 1/2$, and η_θ and η_ψ have the same sign. Also, since $\theta_g < \Psi^*$ we have a contradiction to Lemma 4.3. Thus, if $a = 0$, we can only have $b = 1$.

If $a \geqslant 1$ and $b \leqslant 0$, then $|\eta_\theta| = a|\eta_\phi| + |b||\eta_\psi| < 1$; hence, $|b| \leqslant 2$. Suppose $b = -2$; we have η_ϕ and $\eta_\phi - \eta_\psi$ with the same sign and since $\eta_\theta = 2(\eta_\phi - \eta_\psi) + (a - 2)\eta_\phi$, we see that, if $a \geqslant 2$, η_θ has the same sign as $\eta_\phi - \eta_\psi$ and $|\eta_\phi - \eta_\psi| < 1/2$. But $\xi_\theta > \xi_{\phi-\psi}$ and $\theta_g < (\Phi - \Psi)^*$ contradicts Lemma 4.3; thus, $(a, b) = (1, -2)$. Suppose next that $b = -1$; then η_θ and η_ϕ have the same sign, $|\eta_\phi| < \sqrt{3}/2$ and, if $a \geqslant 2$, $\xi_\theta > \xi_\phi$. This also contradicts Lemma 4.3; hence, $(a, b) = (1, -1)$. If $b = 0$, then $a = 1$; for, otherwise, we would again contradict Lemma 4.3.

We are left to consider the case of $a, b \geqslant 1$. If $b \geqslant a$, let $b = a + c$, where $c \geqslant 0$. Now $\eta_{\phi+\psi}$ and η_ψ have the same sign and if $|\eta_{\phi+\psi}| > 1/2$, we have $|\eta_\psi| > 1/2$ and $|\eta_\theta| = a|\eta_{\phi+\psi}| + c|\eta_\psi| > (a + c)/2 \geqslant 1$ when $c, a \geqslant 2$ or $a = c = 1$. As η_θ and $\eta_{\phi+\psi}$ have the same sign and $\xi_\theta > \xi_{\phi+\psi}$, we cannot have $|\eta_{\phi+\psi}| < 1/2$ by Lemma 4.3. We see that $(a, b) = (1, 1)$. Finally, we note that if $a > b \geqslant 1$ and $a \geqslant 3$, then

$$\xi_\theta = \xi_\phi + (a-1)\xi_\phi + b\xi_\psi = \xi_\phi + \lambda + 1,$$
$$\lambda = (a-1)\xi_\phi + b\xi_\psi - 1 > 2\xi_\phi - 1 > 2\sqrt{1-(1/2+\beta)^2} - 1 \quad \text{(Lemma 4.2)}$$
$$\geqslant g(\beta).$$

From Lemma 4.5 we must have $a \leqslant 2$ and $(a, b) = (2, 1)$. □

COROLLARY 5.1.1. *If* $|\eta_\psi| > (1 - |\eta_\phi|)/2$, *then* $(a, b) \neq (-1, 2)$ *or* $(1, -2)$.

Proof. If $\theta = \pm(\phi - 2\psi)$, then $|\eta_\theta| > 1$. □

COROLLARY 5.1.2. *If* $\xi_\psi > .256$, *then* $(a, b) \neq (2, 1)$.

Proof. If $\xi_\psi > .256$ and $(a, b) = (2, 1)$, then

$$\xi_\theta = 2\xi_\phi + \xi_\psi = \xi_\phi + \lambda + 1,$$

where

$$\lambda = \xi_\phi + \xi_\psi - 1 > .256 + \sqrt{1-(1/2+\beta)^2} - 1 \geqslant g(\beta).$$

Since $|\eta_\phi| < \sqrt{3}/2$, we cannot have $\theta_g < \Phi^*$ by Lemma 4.5. □

COROLLARY 5.1.3. *If* $|\eta_\psi| < \sqrt{3}/2$, *then* $(a, b) \neq (1, 1), (2, 1)$; *if* $|\eta_\psi| > 3/2$ *and* $\xi_\psi < 1/2$, *then* $(a, b) \neq (0, 1)$.

Proof. If $|\eta_\psi| < \sqrt{3}/2$, then Ψ^* exists. Since Φ^* also exists, $\eta_\phi\eta_\psi < 0$, and $\xi_\theta > \xi_\psi, \xi_\phi$ when $\theta = \phi + \psi$ or $\theta = 2\phi + \psi$, we see that θ_g cannot be less than both Ψ^* and Φ^* by Lemma 4.3.

If $|\eta_\psi| > \sqrt{3}/2$ and Ψ^* exists, then $\zeta_{\Psi^*} < 1/2$; hence, if $\xi_\psi < 1/2$, we get $\Psi^* = \zeta_{\Psi^*} + \xi_\psi < 1$, which is impossible as 1 is a relative minimum. □

The corollaries of Theorem 5.1 allow us to restrict even further the set S from which the possible value of (a, b) can be obtained such that $\theta = a\phi + b\psi$. We summarize these results in Table 2 below. It is assumed in this table that $|\eta_\psi| > (1 - |\eta_\phi|)/2$.

TABLE 2

Restrictions on ϕ and ψ	S
$\lvert\eta_\psi\rvert < \sqrt{3}/2$	$\{(1, 0), (0, 1), (1, -1)\}$
$\xi_\psi > .256$	$\{(1, 0), (0, 1), (1, -1), (1, 1)\}$
$\lvert\eta_\psi\rvert > \sqrt{3}/2$, $\xi_\psi < 1/2$	$\{(1, 0), (1, -1), (1, 1), (2, 1)\}$

We now have an algorithm to find θ_g. We first determine Φ and Ψ, then create the subset made up of those members of the set $\{a\Phi + b\Psi | (a, b) \in S\}$ such that $(a\Phi + b\Psi)^*$ exists. Since $|\eta_\phi| < \sqrt{3}/2$, this subset is not empty. Put θ_g equal to that element of this subset such that $(a\Phi + b\Psi)^*$ is least. If $\theta_g = \Phi^*$, put θ_h equal to one of the points which belong to Ψ; if $\theta_g \neq \Phi^*$, put $\theta_h = \Phi^*$. Since $[1, \Phi, \Psi]$ is a basis of R, so is $[1, \theta_g, \theta_h]$.

6. Some Useful Inequalities. If $[1, M_r, N_r]$ is a basis of R_r and $\mu = (\xi_\mu, \eta_\mu)$, $\nu = (\xi_\nu, \eta_\nu)$ are, respectively, the punctures of M_r and N_r, put $E_r = |\xi_\mu \eta_\nu - \xi_\nu \eta_\mu|$. It is a simple matter [6, Section 29] to show that $E_r = |e_r|\sqrt{|\Delta|}/2\sigma_r^2$. Since the value of $|e_r|$ is the same for any basis of R_r, so is the value of E_r. Voronoi [6, Section 30] also showed that $E_r > \sqrt{3}/2$ and that if Θ is a relative minimum of the first kind adjacent to 1 in R_r, then $\Theta'\Theta'' < P + 1/4$, where P is the minimum of a certain quadratic form $Ax^2 + 2Bxy + Cy^2$, with $AC - B^2 = E_r^2$ [6, Sections 27, 28]. In this section we make use of these results to find inequalities which will be useful in the following sections.

We first note that when we are dealing with pure cubic fields, $|\Delta| = 27D^2$. Since $E_r > \sqrt{3}/2$, we have

$$\sigma_r^2/|e_r| < 3D; \tag{6.1}$$

and consequently, (Theorem 3.1)

$$|e_r| \leqslant \sigma_r < 3D, \tag{6.2}$$

$$\sigma_r/|e_r| < \sqrt{3D}, \tag{6.3}$$

$$\sigma_1 Q_r < 3D. \tag{6.4}$$

In several of the following sections we shall be concerned about developing a means of finding a *β-basis* of R_r. This is a basis $[1, \Phi, \Psi]$ of R_r such that the punctures $\phi = (\xi_\phi, \eta_\phi)$ and $\psi = (\xi_\psi, \eta_\psi)$ (of Φ and Ψ, respectively) possess the following properties:

(1) $\xi_\phi > \xi_\psi > 0$,
(2) $|\eta_\phi| < |\eta_\psi|$, $\eta_\phi \eta_\psi < 0$,
(3) $|\eta_\phi| < 1/2 + \beta = 1 - \sqrt{3}/4$, $|\eta_\psi| > 1/2 - \beta = \sqrt{3}/4$.
(4) $|\eta_\psi| > (1 - |\eta_\phi|)/2$.

It follows that, since $|\eta_\phi| < \sqrt{3}/2$, Φ^* as defined in Section 2 must exist. Further, since $1/2 - \beta > 1/3$, by Theorem 5.1 and Corollary 5.1.1, we see that if θ is the puncture of $\theta_g^{(r)}$, then $\theta = a\phi + b\psi$, where (a, b) is one of the elements of the set $\{(1, 0), (0, 1), (1, 1), (1, -1), (2, 1)\}$.

In Lemma 6.1 we derive some important inequalities concerning β-bases when $\delta^3 = D$ $(D \in Z)$. Indeed, in all the remaining sections of this paper we shall confine our discussion to lattices R, where $\delta^3 = D$ $(D \in Z)$.

LEMMA 6.1. *Let $\Phi = (\xi_\phi, \eta_\phi)$, $\Psi = (\xi_\psi, \eta_\psi)$ be the punctures of Φ and Ψ respectively, where $[1, \Phi, \Psi]$ is a β-basis of R_r. If $\Phi^* = (\overline{s}_1 + s_2\delta + s_3\delta^2)/\sigma_r$ and $\Psi_i = (\overline{t}_1 + t_2\delta + t_3\delta^2)/\sigma_r$ $(i = 1$ or $2)$ is either of the two points of R_r which belongs* *to* Ψ, *then*

$$0 < t_2 + t_3\delta < s_2 + \delta s_3 < 4\delta^2, \quad |s_2 - \delta s_3| < 2\delta^2, \quad |t_2 - t_3\delta| < 3.65\delta^2$$

and

$$|s_2|, |\delta s_3| < 3\delta^2, \quad |t_2|, |\delta t_3| < 3.83\delta^2; \quad |\bar{s}_1|, |\bar{t}_1| < 5D.$$

Proof. We first notice that

$$E_r = \xi_\phi |\eta_\psi| + |\eta_\phi| \xi_\psi;$$

hence, $\xi_\phi |\eta_\psi|$, $|\eta_\phi| \xi_\psi < E_r$. Also, since $|\eta_\phi| < \sqrt{3}/2$, we must have $\xi_\phi > \sqrt{1 - \eta_\phi^2}$ by Lemma 4.2. Thus,

$$\sqrt{1 - \eta_\phi^2} < \xi_\phi < E_r/|\eta_\psi|, \quad 0 < \xi_\psi < \xi_\phi,$$

and

$$|\eta_\phi| < |\eta_\psi| < E_r/|\xi_\phi| < E_r/\sqrt{1 - \eta_\phi^2}.$$

Now $|\eta_\psi| > \sqrt{3}/4$; hence,

$$\xi_\phi = \frac{3\delta(s_2 + s_3\delta)}{2\sigma_r} < \frac{4}{\sqrt{3}} E_r = \frac{6|e_r|D}{\sigma_r^2}$$

and

$$0 < s_2 + s_3\delta < 4|e_r|D/\sigma_r\delta \leqslant 4\delta^2 \quad \text{(by (6.2))}.$$

Also,

$$|\eta_\phi| = \frac{\sqrt{3}\delta|s_2 - s_3\delta|}{2\sigma_r} < 1 - \sqrt{3}/4;$$

consequently,

$$|s_2 - s_3\delta| < \frac{2(1 - \sqrt{3}/4)\sigma_r}{\sqrt{3}\delta} < 2\delta^2.$$

It follows from the results on $s_2 + s_3\delta$ and $|s_2 - s_3\delta|$ that $|s_2|$, $|\delta s_3| < 3\delta^2$.

Since $\eta_\phi < 1 - \sqrt{3}/4$, we have $\sqrt{1 - \eta_\phi^2} > \sqrt{\sqrt{3}/2 - 3/16}$. The results involving t_2 and t_3 can be easily derived from the inequalities

$$\xi_\psi < \xi_\phi \quad \text{and} \quad |\eta_\psi| < E_r/\sqrt{\sqrt{3}/2 - 3/16}.$$

Clearly, $|\zeta_{\Psi_i}|$, $|\zeta_{\Phi^*}| < 1$ and $0 < \xi_\psi, \xi_\phi < 2$; thus, since $\bar{s}_1/\sigma_r = \zeta_{\Phi^*} + \xi_\phi/3$, we get $|\bar{s}_1| < 5D$. Similarly, $|\bar{t}_1| < 5D$. $\square$

LEMMA 6.2. *If* $\Theta = \theta_g^{(r)} = (m_1 + m_2\delta + m_3\delta^2)/\sigma_r$ *is the relative minimum of the second kind adjacent to* 1 *in* $\mathcal{R}_r$, *then*

$$|m_2| + |m_3|\delta < (2 + 2\sqrt{3})\delta^2$$

and

$$-3D < m_1 < (\sqrt{3} + 5/2)D; \quad |m_2|, |\delta m_3| < (1 + 2\sqrt{3})\delta^2.$$

Proof. By the construction technique of Algorithm A we know there exists a β-basis $[1, \Phi, \Psi]$ such that $|\eta_\phi| < 1/2$ and $|\eta_\psi| > 1/2$. If we refer to Lemma 4.5 with $\kappa = 0 = g(0)$, we see that $\xi_\theta < \xi_\phi + 1$. For, if $\xi_\theta \geqslant \xi_\phi + 1$, then $\xi_\theta = 1 + \lambda + \xi_\phi$, where $\lambda = \xi_\theta - \xi_\phi - 1 \geqslant 0 = g(0)$. Hence, from Lemma 6.1 we get

$$0 < \frac{3\delta(m_2 + m_3\delta)}{2\sigma_r} < 2E_r + 1 = \frac{3\sqrt{3}|e_r|D}{\sigma_r^2} + 1;$$

and since $|\eta_\theta| < 1$, we also get

$$\left|\frac{\sqrt{3}\delta(m_2 - m_3\delta)}{2\sigma_r}\right| < 1.$$

Thus, $|m_2 + m_3\delta| < 2(\sqrt{3} + 1)\delta^2$ and $|m_2 - m_3\delta| < 2\sqrt{3}\delta^2$. It follows that $|m_2| + |m_3|\delta < (2 + 2\sqrt{3})\delta^2$ and $|m_2|, |\delta m_3| < (1 + 2\sqrt{3})\delta^2$. Since (Lemma 4.1) $-1 < \zeta_\Theta < 1/2$, we have $-1 + \xi_\theta/3 < m_1/\sigma_r < 1/2 + \xi_\theta/3$; thus $-\sigma_r < m_1 < 5\sigma_r/6 + \sqrt{3}|e_r|D/\sigma_r$ and the result for m_1 follows. □

We now give two very simple lemmas which will be needed in the proofs of the last three lemmas of this section.

LEMMA 6.3. *If* $x^2 + y^2 = a$ *and* $c > 0$, *then* $|x| + c|y| \leqslant \sqrt{(c^2 + 1)a}$.

Proof. Since $2c|xy| \leqslant c^2x^2 + y^2$, we have

$$(|x| + c|y|)^2 = x^2 + 2c|xy| + c^2y^2 \leqslant (c^2 + 1)(x^2 + y^2) = (c^2 + 1)a;$$

hence, $|x| + c|y| \leqslant \sqrt{(c^2 + 1)a}$. □

LEMMA 6.4. *If* $x^2 + y^2 = a$ *and* $b > 1$, *then*

$$1 + 2|x| + x^2 + by^2 < 1 + ab + (b - 1)^{-1}.$$

Proof. This result follows from the fact that $(1 + (1 - b)|x|)^2 > 0$. □

LEMMA 6.5. *If* $M_r = 1/\theta_g^{(r-1)} = (m_1^* + m_2^*\delta + m_3^*\delta^2)/\sigma_r$, *then*

$$|m_2^* + m_3^*\delta| < \sqrt{6|e_r|}\delta, \quad |m_2^* - m_3\delta| < \sqrt{5|e_r|}\delta$$

and

$$-\sqrt{5}D < m_1^* < (1 + \sqrt{5})D; \quad |m_2^*|, |m_3^*\delta| < (1 + \sqrt{5})\delta^2.$$

Proof. By Theorem 2.1, $M_r = 1/\theta_g^{(r-1)} > 0$ is the relative minimum of the first kind adjacent to 1. Since it is well known that the minimum P of a quadratic form $Ax^2 + 2Bxy + Cy^2$ does not exceed $2\sqrt{AC - B^2}/\sqrt{3}$, we have

$$M_r'M_r'' < \frac{2}{\sqrt{3}}E_r + 1/4$$

by the remark at the beginning of this section. Thus, if (ξ_μ, η_μ) is the puncture of

M_r, then

$$\zeta_{M_r}^2 + \eta_\mu^2 < \frac{2}{\sqrt{3}} E_r + 1/4;$$

and since $M_r = \zeta_{M_r} + \xi_\mu < 1$, we get

$$|\zeta_{M_r}|,\ |\eta_\mu| < \sqrt{\frac{2}{\sqrt{3}} E_r + \frac{1}{4}},\quad |\xi_\mu| < \sqrt{\frac{2}{\sqrt{3}} E_r + \frac{1}{4}} + 1.$$

Since $E_r = 3\sqrt{3}D|e_r|/2\sigma_r^2$, we have, on using (6.1),

$$|\eta_\mu| < \frac{\sqrt{15D|e_r|}}{2\sigma_r},\qquad |\xi_\mu| < \frac{\sqrt{15D|e_r|}}{2\sigma_r} + 1;$$

hence,

$$|m_2^* - m_3^*\delta| < \sqrt{5|e_r|}\,\delta,\qquad |m_2^* + m_3^*\delta| < \sqrt{6|e_r|}\,\delta.$$

Since $0 < M_r < 1$ and $|\zeta_{M_r}| < \sqrt{(2/\sqrt{3})E_r + 1/4}$, we have

$$0 < m_1^* + m_2^*\delta + m_3^*\delta^2 < \sigma_r,\quad |2m_1^* - \delta(m_2^* + \delta m_3^*)| < 2\sigma_r\sqrt{\frac{2}{\sqrt{3}} E_r + 1/4};$$

thus, from (6.2), we get $-\sqrt{5}D < m_1^* < (1 + \sqrt{5})D$.

Since

$$m_2^* = \frac{\sigma_r}{3\delta}(\xi_\mu + \sqrt{3}\eta_\mu),\quad \delta m_3^* = \frac{\sigma_r}{3\delta}(\xi_\mu - \sqrt{3}\eta_\mu)\quad\text{and}\quad |\xi_\mu| < 1 + |\zeta_{M_r}|.$$

we have

$$|m_2^*|,\ |\delta m_3^*| < \frac{\sigma_r}{3\delta}\left(1 + 2\sqrt{\frac{2}{\sqrt{3}} E_r + 1/4}\right) < (1 + \sqrt{5})\delta^2$$

from Lemma 6.3. □

From (3.2), (6.3) and the results of the above lemma, we get

$$(\delta^{i-1} m_i')/|e_{r-1}| < (1 + \sqrt{5})\sqrt{3}D^{3/2}\qquad (i = 1, 2, 3).$$

Also, by using the above results, we see that $\xi_\mu + c|\eta_\mu| < 1 + |\zeta_{M_r}| + c|\eta_\mu|$, where

$$\zeta_{M_r}^2 + \eta_\mu^2 < \frac{2}{\sqrt{3}} E_r + 1/4 < 45D^2/4\sigma_r^2;$$

hence,

$$|\xi_\mu| + c|\eta_\mu| < 1 + 3D\sqrt{5(c^2 + 1)}/2\sigma_r\qquad (c > 0).$$

Another result of this type is given in

LEMMA 6.6. *If* $(c, d) \in \{(1, 9), (1/3, 27), (9, 1), (3, 3)\}$, *then* $c\xi_\mu^2 + d\eta_\mu^2 < 307D^2/\sigma_r^2$.

Proof. When $d/c \leqslant 1$, this result follows on using the results of Lemma 6.5. When $d/c > 1$, we use Lemma 6.4 to show that

$$\begin{aligned} c\xi_\mu^2 + d\eta_\mu^2 &= c(\xi_\mu^2 + \eta_\mu^2 d/c) < c(1 + 2|\zeta_{M_r}| + \zeta_{M_r}^2 + \eta_\mu^2 d/c) \\ &< c\left(1 + \left(\frac{3|e_r|\delta^3}{\sigma_r^2} + 1/4\right)\frac{d}{c} + \frac{c}{d-c}\right) \\ &< 307D^2/\sigma_r^2. \quad \square \end{aligned}$$

Let $[1, M_r, N_r]$ be a basis of $\mathcal{R}_r$, where

$$M_r = 1/\theta_g^{(r-1)} = (m_1^* + m_2^*\delta + m_3^*\delta^2)/\sigma_r,$$
$$N_r = \theta_h^{(r-1)}/\theta_g^{(r-1)} = (n_1^* + n_2^*\delta + n_3^*\delta^2)/\sigma_r;$$

and let $[1, \bar{M}, \bar{N}]$ be the basis formed by transforming $[1, \bar{M}_r, \bar{N}_r]$ by K, where $K = K_1(-k, 1)$ and

$$k = \begin{cases} [n_3^*/m_3^*] & \text{when } m_3^* \neq 0, \\ [n_2^*/m_2^*] & \text{when } m_3^* = 0. \end{cases}$$

Our final lemma of this section is

LEMMA 6.7. *If* $\bar{M} = (\bar{m}_1 + \bar{m}_2\delta + \bar{m}_3\delta^2)/\sigma_r$ *and* $\bar{N} = (\bar{n}_1 + \bar{n}_2\delta + \bar{n}_3\delta^2)/\sigma_r$, *then*

$$|\bar{n}_2| < (1 + \sqrt{5})\delta^2 + |e_r| \quad \textit{and} \quad |\bar{m}_2|, \delta|\bar{m}_3|, \delta|\bar{n}_3| < (1 + \sqrt{5})\delta^2.$$

Proof. From (3.3), we see that if $m_3^* \neq 0$, then

$$\bar{m}_2 = m_2^*, \quad \bar{m}_3 = m_3^*, \quad |\bar{n}_3| < |\bar{m}_3|, \quad |\bar{n}_2| < |e_r|/|m_3^*| + |m_2^*|.$$

In this case the lemma follows easily from Lemma 6.5. If $m_3^* = 0$, then $\bar{m}_2 = m_2^*$, $\bar{m}_3 = 0$, $|\bar{n}_2| < |\bar{m}_2|$. Also, since $[1, \bar{M}, \bar{N}]$ is a basis of $\mathcal{R}_r$, and $[1, \Phi, \Psi]$ is a basis of $\mathcal{R}_r$, there must exist a matrix $K = (k_{ij})_{2\times 2}$ with integer coefficients such that $|K| = \pm 1$ and

$$\begin{pmatrix} s_2 & t_2 \\ s_3 & t_3 \end{pmatrix} = \begin{pmatrix} \bar{m}_2 & \bar{n}_2 \\ \bar{m}_3 & \bar{n}_3 \end{pmatrix} K.$$

Since $\bar{m}_3 = 0$, we have $s_3 = k_{21}\bar{n}_3$ and by Lemma 6.1, $|\bar{n}_3| < 3\delta$. We also have $|\bar{n}_2| < |\bar{m}_2| < (1 + \sqrt{5})\delta^2$ by Lemma 6.5. $\square$

We conclude this section with a summary of the several inequalities derived here. We give this as Table 3.

TABLE 3

Description of Symbols	Number	Inequalities
See Table 1.	(6.1)	$\sigma_r^2/\lvert e_r\rvert < 3D$
	(6.2)	$\lvert e_r\rvert \leqslant \sigma_r < 3D$
	(6.3)	$\sigma_r/\lvert e_r\rvert < \sqrt{3D}$
	(6.4)	$\sigma_1 Q_r < 3D$
$(\bar{s}_1 + s_2\delta + s_3\delta^2)\sigma_r = \Phi$, $(\bar{t}_1 + t_2\delta + t_3\delta^2)/\sigma_r = \Psi_i$, where $[1, \Phi, \Psi]$ is a β-basis of $\mathcal{R}_r$ and Ψ_i ($i = 1$ or 2) is either of the points which belong to the puncture of Ψ	(6.5)	$0 < t_2 + t_3\delta < s_2 + \delta s_3 < 4\delta^2$ $\lvert s_2 - \delta s_3\rvert < 2\delta^2$; $\lvert t_2 - t_3\delta\rvert < 3.65\delta^2$
	(6.6)	$\lvert s_2\rvert, \delta\lvert s_3\rvert < 3\delta^2$; $\lvert t_2\rvert, \lvert\delta t_3\rvert < 3.83\delta^2$
	(6.7)	$\lvert\bar{s}_1\rvert, \lvert\bar{t}_1\rvert < 5D$
$\theta_g^{(r)} = (m_1 + m_2\delta + m_3\delta^2)/\sigma_r$	(6.8)	$\lvert m_2\rvert + \lvert m_3\rvert\delta < (2 + 2\sqrt{3})\delta^2$
	(6.9)	$-3D < m_1 < (\sqrt{3} + 5/2)D$, $\lvert m_2\rvert, \delta\lvert m_3\rvert < (1 + 2\sqrt{3})\delta^2$
$1/\theta_g^{(r-1)} =$ $(m_1^* + m_2^* + m_3^*\delta^2)/\sigma_r$	(6.10)	$\lvert m_2^* + m_3^*\delta\rvert < \sqrt{6\lvert e_r\rvert}\delta$ $\lvert m_2^* - m_3^*\delta\rvert < \sqrt{5\lvert e_r\rvert}\delta$
	(6.11)	$-\sqrt{5}D < m_1^* < (1 + \sqrt{5})D$
	(6.12)	$\lvert m_2^*\rvert, \lvert m_3^*\rvert\delta < (1 + \sqrt{5})\delta^2$
$m_1' = m_1^2 - Dm_1m_2$ $m_2' = Dm_3^2 - m_1m_2$ $m_3' = m_2^2 - m_1m_2$, where $\theta_g^{(r)} =$ $(m_1 + m_2\delta + m_3\delta^2)/\sigma_r$	(6.13)	$\delta^{i-1}m_i'/\lvert e_r\rvert < (1 + \sqrt{5})\sqrt{3}D^{3/2}$, where $i = 1, 2, 3$.

Description of Symbols	Number	Inequalities
(ξ_μ, η_μ) is the puncture of $1/\theta_g^{(r-1)}$	(6.14)	$\lvert\xi_\mu\rvert + c\lvert\eta_\mu\rvert < 1 + 3D\sqrt{5(c^2+1)}/2\sigma_r$ $(c < 0)$
	(6.15)	$c\xi_\mu^2 + d\eta_\mu^2 < 307D^2/\sigma_r$, where $(c, d) \in \{(1, 9), (1/3, 27), (9, 1), (3, 3)\}$
$[1, \bar{M}, \bar{N}]$ is the basis of $\mathcal{R}_r$ formed by transforming $[1, 1/\theta_g^{(r-1)}, \theta_h^{(r-1)}/\theta_g^{(r-1)}]$ by $K_2(-k, 1)$, where $k = \begin{cases} [n_3^*/m_3^*] & \text{when } m_3^* \neq 0 \\ [n_2^*/m_2^*] & \text{when } m_3^* = 0 \end{cases}$	(6.16)	$\lvert\bar{n}_2\rvert < (1+\sqrt{5})\delta^2 + \lvert e_r\rvert$; $\lvert\bar{m}_2\rvert, \delta\lvert\bar{m}_3\rvert, \delta\lvert\bar{n}_3\rvert < (1+\sqrt{5})\delta^2$

7. **Modifications of Steps (i)–(iv) of Algorithm A.** The object of this section is to develop an algorithm (Algorithm B) to find P, $\Lambda \in \mathcal{R}_r$ such that $[1, \Lambda, P]$ is a basis of $\mathcal{R}_r$ and such that if $(\xi_\lambda, \eta_\lambda)$ is the puncture of Λ and (ξ_ρ, η_ρ) is the puncture of P, then

$$\xi_\rho > \xi_\lambda > 0 \quad \text{and} \quad \lvert\eta_\rho\rvert < \lvert\eta_\lambda\rvert, \quad \eta_\lambda\eta_\rho < 0.$$

That is, we are searching for a basis of $\mathcal{R}_r$ which satisfies properties (1) and (2) of a β-basis. We can certainly find such a basis by using steps (i)–(iv) of Algorithm A; however, on a computer this algorithm must make use of approximations which may not be of sufficient accuracy to guarantee a correct answer. We show here how these steps can be modified such that only rational integer arithmetic is needed at any point. In order to do this we first require several lemmas.

LEMMA 7.1. *If r, $s \in Z$ and at least one of r and s is not zero, then*

$$\lvert r + s\delta\rvert \geqslant \frac{1}{r^2 + \delta\lvert rs\rvert + \delta^2 s^2} \geqslant \frac{1}{(\lvert r\rvert + \lvert s\rvert\delta)^2}.$$

Proof. Follows easily from the fact that $r^3 + s^3 D$ is a rational nonzero integer. □

Define $f(x, y) = x^2 + \delta\lvert xy\rvert + \delta^2 y^2$. We now prove

LEMMA 7.2. *If r, s, $t \in Z$, $D \geqslant 12$, and s, t are not both zero, then*

$$\lvert r + s\delta + t\delta^2\rvert > \frac{1}{3.1\delta^2 f(s, t)}.$$

Proof. Put $A = r + s\delta + t\delta^2$, $\alpha_1 = A - r$, $\alpha_2 = A' - r$, $\alpha_3 = A'' - r$. Since

$$\lvert N(A)\rvert = \lvert AA'A''\rvert = \lvert A\rvert\lvert A'\rvert^2 \geqslant 1,$$

we have

$$|A| \geq 1/|A'|^2.$$

Now if $\gamma = |\alpha_1 - \alpha_2|$, we have

$$\gamma^2 = 3\delta^2(s^2 + st\delta + t^2\delta^2) > 15.72;$$

hence,

$$\gamma + \frac{3}{3.1\gamma^2} < \gamma\sqrt{\frac{3.1}{3}}.$$

Also, $|A'| \leq |A| + \gamma$; thus, if we assume that $|A| \leq 3/3.1\gamma^2$, then $|A'| \leq \gamma + 3/3.1\gamma^2$ and $|A| \geq 1/|A'|^2 > 3/3.1\gamma^2$. Since this contradicts our assumption, we must have $|A| > 3/3.1\gamma^2$.

COROLLARY 7.2.1. *If $r, s \in Z$, $s \neq 0$, and $D > 12$, then* $|r + s\delta| > 1/3.1\delta^2 s^2$.

LEMMA 7.3. *If r, s, t, D are as defined in Lemma 7.1, then $r + s\delta + t\delta^2$ and $rI + s[\delta I] + t[\delta^2 I]$ have the same sign when $I > 3.1\delta^2(|s| + |t|)f(s, t)$.*

Proof. Let $A = Ir + s[\delta I] + t[\delta^2 I]$ and $T = I(r + s\delta + t\delta^2)$. By Lemma 7.2, $|T| > |s| + |t| > |A - T|$; hence, A and T have the same sign and the lemma follows. □

LEMMA 7.4. *If $r, s \in Z$, $s \neq 0$, $D > 12$ and $I > \min\{3.1|s|^3\delta^2, |s|f(r, s)\}$, then $r + s\delta$ and $Ir + s[\delta I]$ have the same sign.*

Proof. By Corollary 7.3.1 and Lemma 7.1,

$$|I(r + s\delta)| > |s| > |I(r + s\delta) - (Ir + s[I\delta])|.$$

Hence, by the same reasoning as that used in Lemma 7.3, we have our result. □

For the remainder of the results in this paper we assume that $D \geq 12$.

LEMMA 7.5. *If $r, s, t, u \in Z$, $t + u\delta \neq 0$, $k = [(r + s\delta)/(t + u\delta)]$, $r' = r - kt$, $s' = s - ku$, $|u|$, $|s'|$, $|s' - u| < c_1$, and $f(t, u), f(r', s'), f(r' - t, s' - u) < c_2$, then*

$$k = \left[\frac{Ir + s[\delta I]}{It + u[\delta I]}\right] \quad \textit{when } I > \min\{c_1 c_2, 3.1 c_1^3 \delta^2\}.$$

Proof. The lemma is true when $r + s\delta$ is a rational integer multiple of $t + u\delta$. Assume that this is not the case and that $t + u\delta > 0$; by Lemma 7.4, $It + u[\delta I] > 0$. Now

$$r' + s'\delta > 0 \quad \text{and} \quad r' - t + (s' - u)\delta < 0;$$

thus, by Lemma 7.4

$$Ir' + s'[I\delta] > 0 \quad \text{and} \quad (r' - t)I + (s' - u)[\delta I] < 0.$$

An easy computation gives

$$\frac{Ir + [I\delta]s}{It + [I\delta]u} - 1 < k < \frac{Ir + [I\delta]s}{It + [I\delta]u},$$

and we have the result above. If $t + u\delta < 0$, the proof is similar. □

COROLLARY 7.5.1. *If* $r, s, t, u \in Z$, $t + u\delta \neq 0$, $k = [(r + s\delta)/(t + u\delta)]$, $d = ts - ru$, $|u| < c_1$, $|t + u\delta| > c_3$, $I > 3.1\delta^2(|d|/c_3 + c_1)^3$, *then*

$$k = \left[\frac{Ir + s[\delta I]}{It + u[\delta I]}\right].$$

Proof. Put $s' = s - ku$. We first note that

$$\frac{r + s\delta}{t + u\delta} = \frac{s}{u} - \frac{d}{u(t + u\delta)}.$$

If $u > 0$, then

$$\frac{d}{t + u\delta} < s' < \frac{d}{t + u\delta} + u;$$

and if $u < 0$, then

$$\frac{d}{t + u\delta} + u < s' < \frac{d}{t + u\delta}.$$

Thus, $|u|$, $|s'|$, $|s' - u| < |d|/|t + u\delta| + |u| < |d|/d_3 + c_1$, and the corollary follows from the lemma. □

We are now ready to begin describing how to modify Algorithm A. We first note that by (6.16), we may assume the existence of a basis $[1, M, N]$ of $\mathcal{R}_r$ such that if $\mu = (\xi_\mu, \eta_\mu)$, $\nu = (\xi_\nu, \eta_\nu)$ are the punctures of M and N, then $M = 1/\theta_g^{(r-1)}$,

$$\xi_\mu = \frac{3\delta}{2\sigma_r}(m_2 + \delta m_3), \qquad \eta_\mu = \frac{\sqrt{3}\delta}{2\sigma_r}(m_2 - \delta m_3),$$

$$\xi_\nu = \frac{3\delta}{2\sigma_r}(n_2 + \delta n_3), \qquad \eta_\nu = \frac{\sqrt{3}\delta}{2\sigma_r}(n_2 - \delta n_3),$$

and

$$(7.1) \qquad |n_2| < (1 + \sqrt{5})\delta^2 + |e_r|, \qquad |m_2|, |\delta m_3|, |\delta n_3| < (1 + \sqrt{5})\delta^2.$$

We must also define the integers that will be used in Algorithm B_1 below. Let any $\Omega = (q_1 + q_2\delta + q_3\delta^2)/\sigma_r \in \mathcal{R}_r$ have puncture $\omega = (\xi_\omega, \eta_\omega)$. We define

$$x_\omega = I_1q_2 + [I_1\delta]q_3, \quad y_\omega = I_1q_2 - [I_1\delta]q_3, \quad \bar{y}_\omega = [I_2\sqrt{3}\delta]q_2 - [I_2\sqrt{3}\delta^2]q_3,$$

where I_1, I_2 are arbitrary but fixed rational integers. Since

$$\xi_\omega = \frac{3\delta}{2\sigma_r}(q_2 + q_3\delta) \quad \text{and} \quad \eta_\omega = \frac{\sqrt{3}\delta}{2\sigma_r}(q_2 - q_3\delta),$$

we see that

(7.2) $$\left|\frac{\xi_\omega}{\xi_\pi} - \frac{x_\omega}{x_\pi}\right| = \frac{|e_r|(\delta I_1 - [\delta I_1])}{|x_\pi(p_2 + p_3\delta)|},$$

(7.3) $$\left|\frac{\eta_\omega}{\eta_\pi} - \frac{y_\omega}{y_\pi}\right| = \frac{|e_r|(\delta I_1 - [\delta I_1])}{|y_\pi(p_2 - p_3\delta)|},$$

(7.4) $$\left|\frac{x_\omega}{x_\pi} - \frac{y_\omega}{y_\pi}\right| = \frac{2I_1[I_1\delta]\,|e_r|}{|I_1^2p_2^2 - p_3^2[I_1\delta]^2|},$$

where $\pi = (\xi_\pi, \eta_\pi)$ is the puncture of $\Pi = (p_1 + p_2\delta + p_3\delta^2)/\sigma_r$. We also have the following simple lemma.

LEMMA 7.6. *Let ω be the puncture of $\Omega = (q_1 + q_2\delta + q_3\delta^2)/\sigma_r \in R_r$, where $|q_2| + |q_3| < (3 + 2\sqrt{5})\delta^2$. If $I_2 > 80\delta^2$ and $|\bar{y}_\omega| \leq I_2\sigma_r$, we must have $|\eta_\omega| < 1 - \sqrt{3}/4$ and if $|\bar{y}_\omega| \geq I_2\sigma_r$, we must have $|\eta_\omega| > \sqrt{3}/4$.*

Proof. We note that

$$\left|\eta_\omega - \frac{\bar{y}_\omega}{2\sigma_r I_2}\right| < \frac{|q_2| + |q_3|}{2\sigma_r I_2} < \frac{(3 + 2\sqrt{5})\delta^2}{2\sigma_r I_2}.$$

Thus,

$$|\eta_\omega| = \left|\frac{\bar{y}_\omega}{2\sigma_r I_2}\right| + \gamma, \quad \text{where } |\gamma| < \frac{(3 + 2\sqrt{5})\delta^2}{2\sigma_r I_2} < \frac{1}{2} - \frac{\sqrt{3}}{4};$$

and the lemma follows. □

LEMMA 7.7. *With $I_1 > 3.1(2 + 2\sqrt{5})^3\delta^5 \simeq 840.44\delta^5$ and μ and ν defined as above, we can replace ξ_μ and ξ_ν by x_μ and x_ν in steps* (i) *and* (ii) *of Algorithm* A.

Proof. By Lemma 7.4 and (7.1) we see that $\operatorname{sgn}(x_\mu) = \operatorname{sgn}(\xi_\mu)$, $\operatorname{sgn}(x_\nu) = \operatorname{sgn}(\xi_\nu)$, $\operatorname{sgn}(y_\mu) = \operatorname{sgn}(\eta_\mu)$, and $\operatorname{sgn}(y_\nu) = \operatorname{sgn}(\eta_\nu)$. Also, if $r = |m_3 \pm n_3|$, then $r < 2(\sqrt{5} + 1)\delta$ by (7.1) and consequently, $\operatorname{sgn}(\xi_\nu - \xi_\mu) = \operatorname{sgn}(x_\nu - x_\mu)$, $\operatorname{sgn}(|\eta_\nu| - |\eta_\mu|) = \operatorname{sgn}(|y_\nu| - |y_\mu|)$ by Lemma 7.4. □

We have seen that we can replace ξ_μ and ξ_ν by x_μ and x_ν in steps (i) and (ii) of Algorithm A as long as $I_1 > (3.1)(2 + 2\sqrt{5})^3\delta^5$. We need now to establish how large I_1 should be in order to replace ξ_ν/ξ_μ or η_ν/η_μ by x_ν/x_μ or y_ν/y_μ in the remaining steps of the algorithm.

LEMMA 7.8. *Let (ξ_π, η_π) be the puncture of $\Pi = (p_1 + p_2\delta + p_3\delta^2)/\sigma_r \in R_r$ such that $\xi_\pi > 0$, $\xi_\pi \leq \xi_\mu$, $|\eta_\pi| \leq |\eta_\mu|$, and let $\omega = (\xi_\omega, \eta_\omega)$ be the puncture of $\Omega = (q_1 + q_2\delta + q_3\delta^2)/\sigma_r \in R_r$. If $|[\xi_\omega/\xi_\pi] - [\eta_\omega/\eta_\pi]| \leq 2$ and $I_1 > 708\delta^5$, then $[\xi_\omega/\xi_\pi] = [x_\omega/x_\pi]$ and $[\eta_\omega/\eta_\pi] = [y_\omega/y_\pi]$.*

Proof. Let $k_1 = [\xi_\omega/\xi_\pi]$, $k_2 = [\eta_\omega/\eta_\pi]$, $\xi = \xi_\omega - k_1\xi_\pi$, $\eta = \eta_\omega - k_1\eta_\pi$, and $j = k_1 - k_2$. We have $0 < \xi < \xi_\pi$ and $-j < \eta/\eta_\pi < -j + 1$. Now $\xi = 3\delta(t + u\delta)/2\sigma_r$ and $\eta = \sqrt{3}\delta(t - u\delta)/2\sigma_r$, where $t = q_2 - k_1p_2$, $u = q_3 - k_1p_3$; consequently, $3\delta t/\sigma_r = \xi + \sqrt{3}\eta$, $3\delta^2u/\sigma_r = \xi - \sqrt{3}\eta$, $3\delta(t - p_2)/\sigma_r = \xi - \xi_\pi + \sqrt{3}(\eta - \eta_\pi)$, and $3\delta^2(u - p_3)/\sigma_r = \xi - \xi_\pi - \sqrt{3}(\eta - \eta_\pi)$. Since $|j| \leq 2$, we have $|\eta|$,

$|\eta - \eta_\pi| < 3|\eta_\pi|$ and $|\xi|$, $|\xi - \xi_\pi| < |\xi_\pi|$; hence, $3\delta^2|u|/\sigma_r$ and $3\delta^2|u - p_3|/\sigma_r < |\xi_\pi| + 3\sqrt{3}|\eta_\pi| < |\xi_\mu| + 3\sqrt{3}|\eta_\mu| < 1 + 3\sqrt{35}D/2\sigma_r$, by (6.14). Thus, we have $|u|$, $|u - p_3| < (1 + \sqrt{35})\delta$. Also,

$$9\delta^2 f(t, u)/\sigma_r^2 = (\xi + \sqrt{3}\eta)^2 + |\xi + \sqrt{3}\eta||\xi - \sqrt{3}\eta| + (\xi - \sqrt{3}\eta)^2$$
$$= \begin{cases} 3\xi^2 + 3\eta^2 < 3\xi_\mu^2 + 27\eta_\mu^2 & (\text{if } \xi^2 > 3\eta^2) \\ \xi^2 + 9\eta^2 < \xi_\mu^2 + 81\eta_\mu^2 & (\text{if } \xi^2 < 3\eta^2) \end{cases}$$
$$< 3 \cdot 307D^2/\sigma_r^2;$$

and similarly,

$$9\delta^2 f(t - p_2, u - p_3)/\sigma_r^2 < 3 \cdot 307D^2/\sigma_r^2$$

by (6.15). Also, since $0 < \xi_\pi < \xi_\mu$ and $|\eta_\pi| < |\eta_\mu|$, one can show, as in Lemma 6.5, that $|p_3| < (1 + \sqrt{5})\delta$; further, from (6.10) and (6.2) we get $f(p_2, p_3) < (|p_2| + \delta|p_3|)^2 < 6|e_r|\delta < 18\delta^4$.

Since $I_1 > 708\delta^5 > (1 + \sqrt{35})\delta\ (307\delta^4)/3$, we have

$$k_1 = \left[\frac{q_2 + q_3\delta}{p_2 + p_3\delta}\right] = \left[\frac{x_\omega}{x_\pi}\right] \quad \text{by Lemma 7.5.}$$

By a somewhat similar argument, we can show that $k_2 = [y_\omega/y_\pi]$. In this case we put $\xi = \xi_\omega - k_2\xi_\pi$ and $\eta = \eta_\omega - k_2\eta_\pi$. Then $j < \xi/\xi_\pi < j + 1$ and $0 < \eta/\eta_\pi < 1$. We use (6.14) again with $c = \sqrt{3}/3$ and the remaining parts of (6.15). □

LEMMA 7.9. *Let π and ω be defined as in Lemma 7.8 and suppose π and ω form a basis of the lattice of punctures L of $\mathcal{R}_r$. If $I_1 > (3.1)(3 + \sqrt{5})^3\delta^5 \simeq 445.02\delta^5$ we must have $[x_\omega/x_\pi] = [\xi_\omega/\xi_\pi]$ when $|\eta_\pi| < 1 - \sqrt{3}/4$ and $[y_\omega/y_\pi] = [\eta_\omega/\eta_\pi]$ when $|\eta_\pi| > \sqrt{3}/4$.*

Proof. Since π and ω form a basis of L, we must have $|p_2q_3 - p_3q_2| = |e_r|$; also, as in Lemma 7.8, we have $|p_3| < (1 + \sqrt{5})\delta$. If $|\eta_\pi| > \sqrt{3}/4$, then $|p_2 - p_3\delta| > \sigma_r/2\delta$; if $|\eta_\pi| < 1 - \sqrt{3}/4 < \sqrt{3}/2$, then $|\xi_\pi| > \sqrt{\sqrt{3}/2 - 3/16} > 3/4$ (Lemma 4.2) and $|p_2 + p_3\delta| > \sigma_r/2\delta$. Since $2|e_r|\delta/\sigma_r \leqslant 2\delta$ and $I_1 > 3.1(3 + \sqrt{5})^3\delta^5$, the result follows from Corollary 7.5.1.

LEMMA 7.10. *Let π and ω be defined as in Lemma 7.8 and suppose π and ω form a basis of L. If $|[x_\omega/x_\pi] - [y_\omega/y_\pi]| \leqslant 1$, then $[\xi_\omega/\xi_\pi] = [x_\omega/x_\pi]$ and $[\eta_\omega/\eta_\pi] = [y_\omega/y_\pi]$ when $I_1 > 708\delta^5$.*

Proof. We first note that

$$|p_2 + p_3\delta||p_2 - p_3\delta| = |(|p_2| + |p_3\delta|)(|p_2| - |p_3\delta|)| \geqslant \frac{1}{|p_2| + |p_3\delta|}$$

by a direct application of Lemma 7.1. Also, since

$$|\xi_\pi| < |\xi_\mu|, \quad |\eta_\pi| < |\eta_\mu|, \quad \text{and} \quad \frac{2\sigma_r}{3\delta}|\xi_\mu|, \quad \frac{2\sigma_r}{\sqrt{3}\delta}|\eta_\mu| < \sqrt{6|e_r|\delta}$$

(by (6.10)), we see that $|p_2| + |p_3|\delta < \sqrt{6|e_r|\delta}$. Hence,

$$|p_2^2 - p_3^2\delta| > \frac{1}{\sqrt{6|e_r|\delta}}. \tag{7.5}$$

Since $3D > |e_r|$, $3\sqrt{18\delta^5} > |e_r|\sqrt{6|e_r|\delta}$, and $|p_3| < (1 + \sqrt{5})\delta$, we get

$$2(2p_3^2\delta + |e_r|)\sqrt{6|e_r|\delta} < 2(2(1 + \sqrt{5})^2 + 3)\sqrt{18\delta^5} < I_1.$$

Put $\gamma = (\delta I_1 - [\delta I_1])/I_1$. Then $0 < \gamma < I_1^{-1}$ and

$$2\gamma(2p_3^2 + |e_r|) < \frac{I_1\gamma}{\sqrt{6|e_r|\delta}} < \frac{1}{\sqrt{6|e_r|\delta}}. \tag{7.6}$$

If we put $u = (I_1^2p_2^2 - p_3^2[I_1\delta]^2)/I_1^2$, $v = p_2^2 - \delta^2p_3^2$, and $d = u - v$, then $0 < d < 2\delta\gamma p_3^2$. Also, since

$$\left|\left[\frac{x_\omega}{x_\pi}\right] - \left[\frac{y_\omega}{y_\pi}\right]\right| \leqslant 1,$$

we have

$$\left|\frac{x_\omega}{x_\pi} - \frac{y_\omega}{y_\eta}\right| \leqslant 2.$$

From (7.4), it follows that $|u| \geqslant [I_1\delta]|e_r|/I_1 = (\delta - \gamma)|e_r|$. Since $|u|/|v| \leqslant 1 + d/|v|$, we get

$$\frac{(\delta - \gamma)|e_r|}{|p_2^2 - p_3^2\delta^2|} \leqslant 1 + \frac{d}{|p_2^2 - p_3^2\delta^2|}. \tag{7.7}$$

Adding $\gamma|e_r|/|p_2^2 - p_3^2\delta^2|$ to both sides of (7.7) and multiplying through by 2, we have

$$\frac{2\delta|e_r|}{|p_2^2 - p_3^2\delta^2|} \leqslant 2 + 2\,\frac{d + \gamma|e_r|}{|p_2^2 - p_3^2\delta^2|} < 2 + \frac{d + \gamma|e_r|}{\gamma(2\delta p_3^2 + |e_r|)} < 3, \tag{7.8}$$

where the last inequalities follow from (7.5). (7.6) and the fact that $0 < d < 2p_3^2\gamma\delta$.

Since $|p_2| + |p_3|\delta < \sqrt{6|e_r|\delta}$, we see from (7.8) and (7.5) that

$$|p_2 - p_3\delta|,\ |p_2 + p_3\delta| \geqslant ||p_2| - |p_3|\delta| > 2\sqrt{\delta|e_r|}/3\sqrt{6}.$$

Now

$$|x_\pi| = |I_1(p_2 + p_3\delta) - I_1\gamma p_3| > 2I_1\sqrt{\delta|e_r|}/3\sqrt{6} - (1 + \sqrt{5})\delta;$$

hence, $|x_\pi||p_2 + p_3\delta| > |e_r|$ and from (7.2), we see that $|\xi_\omega/\xi_\pi - x_\omega/x_\pi| < 1$. Similarly, we are able to show that $|\eta_\omega/\eta_\pi - y_\omega/y_\pi| < 1$. By Lemma 7.9 either $[\xi_\omega/\xi_\pi] = [x_\omega/x_\pi]$ or $[\eta_\omega/\eta_\pi] = [y_\omega/y_\pi]$; consequently, $|[\xi_\omega/\xi_\pi] - [\eta_\omega/\eta_\pi]| \leqslant 2$ and our result follows from Lemma 7.8. □

LEMMA 7.11. *Let π and ω be defined as in Lemma 7.8 and suppose that π and ω form a basis of L. If $j = [x_\omega/x_\pi] - [y_\omega/y_\pi]$ ($I_1 > 708\delta^5$), then j and $[\xi_\omega/\xi_\pi] - [\eta_\omega/\eta_\pi]$ have the same sign.*

Proof. By Lemma 7.10 the result is certainly true when $j \leqslant 1$ and by Lemma 7.8 the result is true when $|[\xi_\omega/\xi_\pi] - [\eta_\omega/\eta_\pi]| \leqslant 2$. Assume that $j > 1$ and $|[\xi_\omega/\xi_\pi] - [\eta_\omega/\eta_\pi]| > 2$. The sign of $[\xi_\omega/\xi_\pi] - [\eta_\omega/\eta_\pi]$ is the same as that of $\xi_\omega/\xi_\pi - \eta_\omega/\eta_\pi = 3\sqrt{3}\delta^3 e_r/2\xi_\pi\eta_\pi$ and the sign of $[x_\omega/x_\pi] - [y_\omega/y_\pi]$ is the same as that of $I_1[I_1\delta]e_r/x_\pi y_\pi$. Since $x_\pi\xi_\pi$ and $\eta_\pi y_\pi > 0$, the result follows. □

We are finally able to present the main result of this section. We give here

Algorithm B_1. Let I_1, I_2 be any integers such that $I_1 > 841\delta^5, I_2 > 80\delta^2$. Also, let $[1, M, N]$ be the basis $[1, 1/\theta_g^{(r-1)}, \theta_h^{(r-1)}/\theta_g^{(r-1)}]$ of R_r; and let $M = (m_1 + m_2\delta + m_3\delta^2)/\sigma_r$ and $N = (n_1 + n_2\delta + n_3\delta^2)/\sigma_r$. Perform the following steps in the indicated order:

(i) Transform the basis $[1, M, N]$ of R_r by $K_2(-k, 1)$, where $k = [n_3/m_3]$ when $m_3 \neq 0$ and $k = [n_2/m_2]$ otherwise.

(ii) Transform the new basis by $\binom{k_1\ 0}{0\ k_2}$, where $k_1 = \operatorname{sgn}(x_\mu)$, $k_2 = \operatorname{sgn}(x_\nu)$.

(iii) If $x_\nu > x_\mu$ go to (iv); otherwise, transform the basis by $K_2(1, 1)$ and go to (iv) 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 terminate B_1.

(iv) If $y_\mu y_\nu < 0$, go to step (v); 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 (v).

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

(4) If $[x_\nu/x_\mu] < [y_\nu/y_\mu] - 1$, transform the basis by $K_1([x_\nu/x_\mu] + 1, -1)$ when $|\bar{y}_\mu| < I_2\sigma_r$; otherwise, transform the basis by $K_2([y_\nu/y_\mu], -1)$. Terminate B_1.

(5) If $[x_\nu/x_\mu] > [y_\nu/y_\mu] + 1$, transform the basis by $K_1(-[x_\nu/x_\mu], 1)$ when $|\bar{y}_\mu| < I_2\sigma_r$; otherwise, transform the basis by $K_2(-[y_\nu/y_\mu] - 1, 1)$. Terminate B_1.

(v) If $|y_\mu| > |y_\nu|$ terminate B_1. If $|y_\mu| \leqslant |y_\nu|$ transform the basis by $K_1(-[x_\nu/x_\mu], 1)$ when $|\bar{y}_\mu| < I_2\sigma_r$; otherwise, transform by $K_2([-y_\nu/y_\mu], 1)$.

THEOREM 7.12. *If $[1, \Lambda, P]$ is the basis of R_r which results on executing Algorithm* B_1, *then $\xi_\rho > \xi_\lambda > 0$ and $|\eta_\rho| < |\eta_\lambda|$, $\eta_\lambda\eta_\rho < 0$.*

Proof. If, starting with the basis $[1, \bar{M}, \bar{N}]$ which results after performing step (i) of Algorithm B_1, we execute steps (i)–(iv) of Algorithm A, we will certainly produce a basis of R with the same properties as $[1, \Lambda, P]$ above. We have already seen in Lemma 7.7 that, in this case, steps (i) and (ii) of A can be replaced by steps (ii) and (iii) of B_1.

If $\bar{\mu} = (\bar{\xi}_\mu, \bar{\eta}_\mu)$, $\bar{\nu} = (\bar{\xi}_\nu, \bar{\eta}_\nu)$ are the punctures of $\bar{M}$ and $\bar{N}$ and $\mu = (\xi_\mu, \eta_\mu)$, $\nu = (\xi_\nu, \eta_\nu)$ are the punctures of the basis produced by Algorithm A at the beginning of step (iii), then $|\xi_\mu| = |\bar{\xi}_\mu| = 3\delta(\bar{m}_2 + \delta\bar{m}_3)/2\sigma_r$, $|\eta_\mu| = |\bar{\eta}_\mu|$ and $|n_3| \leqslant 2|\bar{m}_3| < 2(1+\sqrt{5})\delta$. Indeed, if $\eta_\nu\eta_\mu < 0$, then $|\eta_\nu| = |\bar{\eta}_\nu|$. Thus, by Lemma 7.4, $\operatorname{sgn}(\eta_\mu\eta_\nu) = \operatorname{sgn}(y_\mu y_\nu)$. Now at any point in the execution of substep (a) of A(iii), our new punctures μ and ν satisfy the inequalities $|\xi_\mu| \leqslant |\bar{\xi}_\mu|$ and $|\eta_\mu| \leqslant |\bar{\eta}_\mu|$; thus, if $|[x_\nu/x_\mu] - [y_\nu/y_\mu]| \leqslant 1$, then $[x_\nu/x_\mu] = [\xi_\nu/\xi_\mu]$, $[y_\nu/y_\mu] = [\eta_\nu/\eta_\mu]$ by Lemma 7.10. Also, if $[x_\nu/x_\mu] > [y_\nu/y_\mu] + 1$, then $[\xi_\nu/\xi_\mu] > [\eta_\nu/\eta_\mu] + 1$; and if $[y_\nu/y_\mu] > [x_\nu/x_\mu] + 1$, then $[\eta_\nu/\eta_\mu] > [\xi_\nu/\xi_\mu] + 1$ by Lemmas 7.10 and 7.11. Now, if $|\bar{y}_\mu| < I_2\sigma_r$, then $|\eta_\mu| < 1 - \sqrt{3}/4$ and if $|\bar{y}_\mu| \geqslant I_2\sigma_r$, then $|\eta_\mu| > \sqrt{3}/4$ by Lemma 7.6; hence, by Lemma 7.9, if $|\bar{y}_\mu| < I_2\sigma_r$, then $[x_\nu/x_\mu] = [\xi_\nu/\xi_\mu]$ and if $|\bar{y}_\mu| \geqslant I_2\sigma_r$, then $[y_\nu/y_\mu] = [\eta_\nu/\eta_\mu]$. It follows that we can replace step (iii) of A by step (iv) of B_1 and still obtain a result that some form of Algorithm A would produce.

If we use Algorithm A on $[1, \bar{M}, \bar{N}]$ and arrive at the beginning of step (iv) with a new basis with punctures $\mu = (\xi_\mu, \eta_\mu)$, $\nu = (\xi_\nu, \eta_\nu)$, then either $0 < \xi_\mu = |\bar{\xi}_\mu|$, $|\eta_\mu| = |\bar{\eta}_\mu|$, $|\eta_\nu| = |\bar{\eta}_\nu|$ or $0 < \xi_\mu < \xi_\nu \leqslant |\bar{\xi}_\mu|$, $|\eta_\mu| \leqslant |\bar{\eta}_\mu|$, $|\eta_\nu| \leqslant |\bar{\eta}_\mu|$, the latter case occurring when either (iii)-b or (iii)-c is executed. It follows that in each of these cases we have $|n_3|, |m_3| < (1+\sqrt{5})\delta$. By Lemmas 7.4, 7.6, and 7.9 we see that step (v) of B_1 can be used to replace step (iv) of A and the basis $[1, \Lambda, P]$ which results on performing this step will have the required properties. □

In the next section we show how we can modify step (v) of Algorithm A in order that only integers are used.

8. Modification of Step (v) of Algorithm A. Let $\mu = (\xi_\mu, \eta_\mu)$, $\nu = (\xi_\nu, \eta_\nu)$ be the punctures of $M = (m_1 + m_2\delta + m_3\delta^2)/\sigma_r$, $N = (n_1 + n_2\delta + n_3\delta^2)/\sigma_r$, respectively. For the result that follows we assume that μ, ν forms the basis of L which results on applying Algorithm B_1. For this basis we have

(8.1) $$\xi_\nu > \xi_\mu > 0, \quad |\eta_\mu| > |\eta_\nu|, \quad \eta_\mu\eta_\nu < 0.$$

We must now prove some preliminary lemmas.

LEMMA 8.1. *For the μ and ν described above, we have*

$$\xi_\mu/3,\ \xi_\nu/3,\ |\eta_\mu|/\sqrt{3},\ |\eta_\nu|/\sqrt{3} < (3+2\sqrt{5})D/2\sigma_r.$$

Proof. We first note that since η_ν and η_μ have different signs and $\xi_\nu, \xi_\mu > 0$, we have $\xi_\mu|\eta_\nu|$, $\xi_\nu|\eta_\mu| < E_r$. Thus, if $|\eta_\nu| < 1 - \sqrt{3}/4 < \sqrt{3}/2$, then $\xi_\nu > \sqrt{\sqrt{3}/2 - 3/16} > 3/4$ (Lemma 4.2) and $|\eta_\mu|/\sqrt{3} < 4E_r/3\sqrt{3} = 2D|e_r|/\sigma_r^2 < 2D/\sigma_r$ by (6.2). Also, if $\eta_\mu > \sqrt{3}/4$, then $\xi_\nu/3 < 2D/\sigma_r$.

If we arrive at the end of B_1 by skipping over all the substeps of (iv) and step (v), then, since $|\xi_\mu|$, $|\eta_\mu|$ do not change after (i) has been executed, we get

$$\xi_\mu/3 < \delta\sqrt{6|e_r|\delta}/2\sigma_r < 3\sqrt{2}D/2\sigma_r,$$

$$|\eta_\nu|/\sqrt{3} < |\eta_\mu|/\sqrt{3} < \delta\sqrt{5|e_r|\delta}/2\sigma_r < \sqrt{15}D/2\sigma_r$$

by (6.10). We also have either $\xi_\nu/3 < 2\xi_\mu/3 < 6D/2\sigma_r$ or $|n_3| < (1+\sqrt{5})\delta$. In the latter case, if $|\eta_\nu| < 1/2\sqrt{3}$, then $|n_2 - n_3\delta| < \sigma_r/3\delta < \delta^2$ and $2\sigma_r\xi_\nu/3\delta < \delta^2 + 2(1+\sqrt{5})\delta^2 = (3+2\sqrt{5})\delta^2$. If $|\eta_\nu| > 1/2\sqrt{3}$, then $|\eta_\mu| > 1/2\sqrt{3}$ and $\xi_\nu/3 < 2\sqrt{3}E_r/3 < 6D/2\sigma_r$.

If we arrive at the end of B_1 by executing step (iv) or step (v), then we must execute one of substep (4) of (iv) or substep (5) of (iv) or step (v). If $\bar{\mu} = (\xi_\mu, \bar{\eta}_\mu)$ is the puncture of M just before either of (iv)-4, (iv)-5 or (v) is executed, we get

$$|\xi_\mu|, |\bar{\eta}_\mu| < \frac{3\delta}{2\sigma_r}\sqrt{6|e_r|\delta} < \frac{9\sqrt{2}D}{2\sigma_r},$$

by using the reasoning in Theorem 7.12, (6.10) and (6.2). If, in any of these steps, we start with $|\bar{y}_{\bar{\mu}}| < I_2\sigma_r$, then, since a transformation of the form $K_1(a, b)$ is used to obtain μ and ν, we get $\nu = \bar{\mu}$. Hence, by Lemma 7.6, we see that $|\eta_\nu| < 1 - \sqrt{3}/4$ and, therefore,

$$|\eta_\nu|/\sqrt{3} < (1 - \sqrt{3}/4)/\sqrt{3} < 3D/\sigma_r, \quad |\eta_\mu|/\sqrt{3} < 2D/\sigma_r, \quad \xi_\mu/3 < \xi_\nu/3 < 3\sqrt{2}D/2\sigma_r.$$

If we start with $|\bar{y}_{\bar{\mu}}| \geqslant I_2\sigma_r$, then a transformation of the form $K_2(a, b)$ is used and $\mu = \bar{\mu}$. It follows in this case that $|\eta_\mu| > \sqrt{3}/4$ and

$$\xi_\mu/3 < \xi_\nu/3 < 2D/\sigma_r, \quad |\eta_\nu|/\sqrt{3} < |\eta_\mu|/\sqrt{3} < 3\sqrt{6}D/2\sigma_r.$$

The lemma is now proved. □

LEMMA 8.2. *Let* μ, ν *be any basis of* L *such that* (8.1) *is true. If* $|\eta_\mu| > \sqrt{3}/4$, $|\bar{y}_\nu| > I_2\sigma_r$ $(I_2 > 80\delta^2)$, $|\eta_\nu|/\sqrt{3} < (3 + 2\sqrt{5})D/2\sigma_r$, *then* $|\eta_\nu| > \sqrt{3}/4$, $|n_2| + |n_3|\delta < (3 + 2\sqrt{5})\delta^2$, *and* $|n_2|$, $|\delta n_3| < (2 + \sqrt{5})\delta^2$; *if* $|\eta_\nu| < 1 - \sqrt{3}/4$, $|\bar{y}_\mu| \leqslant I_2\sigma_r$, $\xi_\mu/3 < (3 + 2\sqrt{5})D/2\sigma_r$, *then* $|\eta_\mu| < 1 - \sqrt{3}/4$, $|m_2| + |m_3|\delta < (3 + 2\sqrt{5})\delta^2$, *and* $|m_2|$, $|\delta m_3| < (2 + \sqrt{5})\delta^2$.

Proof. We prove the second part of this lemma here. The proof of the first part is similar and somewhat easier.

Since $|\eta_\nu| < 1 - \sqrt{3}/4 < \sqrt{3}/2$ and $|\eta_\mu|\xi_\nu < E_r$, we have $\xi_\nu > \sqrt{1 - \eta_\nu^2} > 3/4$ (Lemma 4.2) and $|\eta_\mu| < 4E_r/3$. It follows that $|m_2 - m_3\delta| < 4|e_r|\delta^2/\sigma_r \leqslant 4\delta^2$. Since $|m_2 + m_3\delta| < (3 + 2\sqrt{5})\delta^2$, $|m_2| + |m_3\delta| < \max\{(3 + 2\sqrt{5})\delta^2, 4\delta^2\} = (3 + 2\sqrt{5})\delta^2$ and from Lemma 7.6 we see that $|\eta_\mu| < 1 - \sqrt{3}/4$. We also note that since $|\eta_\mu|\xi_\mu < \xi_\nu|\eta_\mu| < E_r$, we have

$$|m_2^2 - m_3^2\delta^2| < 2|e_r|\delta < 6\delta^4. \tag{8.2}$$

If $|m_2 - m_3\delta| < \delta^2$, then $|m_2|$, $|\delta m_3| < (\delta^2 + (3 + 2\sqrt{5})\delta^2)/2 < (2 + \sqrt{5})\delta^2$. If $\delta^2 < |m_2 - m_3\delta| < 2\delta^2$, then, from (8.2), we have $|m_2 + \delta m_3| < 6\delta^2$ and $|m_2|$, $|\delta m_3| < (2\delta^2 + 6\delta^2)/2 = 4\delta^2$. Finally if $|m_2 - m_3\delta^2| > 2\delta^2$, then $|m_2 + \delta m_3| < 3\delta^2$ and $|m_2|$, $|\delta m_3| < 3.5\delta^2$. □

We now consider the following algorithm (Algorithm B_2). We assume that we begin with a basis $[1, M, N]$ whose punctures $\mu = (\xi_\mu, \eta_\mu)$, $\nu = (\xi_\nu, \eta_\nu)$ have the properties (8.1).

Algorithm B_2. If $|\bar{y}_\mu| \geqslant I_2\sigma_r$ and $|\bar{y}_\nu| \leqslant I_2\sigma_r$, we terminate the algorithm immediately. When these conditions are not satisfied and $|\bar{y}_\mu| < I_2\sigma_r$, execute step (1); otherwise, execute step (2).

(1) Transform the basis $[1, M, N]$ by $K_1(-k, 1)$, where $k = [x_\nu/x_\mu]$. Continue doing this until $|\bar{y}_\mu| \geq I_2\sigma_r$. At this point terminate the algorithm.
(2) Transform the basis $[1, M, N]$ by $K_3(1, k)$, where $k = [-y_\mu/y_\nu]$. Continue doing this until $|\bar{y}_\nu| \leq I_2\sigma_r$. At this point terminate the algorithm.

Put $[1, M_r^*, N_r^*] = [1, 1/\theta_g^{(r-1)}, \theta_h^{(r-1)}/\theta_g^{(r-1)}]$, where $\theta_g^{(r-1)}$ and $\theta_h^{(r-1)}$ are defined in Section 2. We now prove

THEOREM 8.3. *Let* $I_1 > 3.1(2+\sqrt{5})^3\delta^5$ *and* $I_2 > 80\delta^2$. *If the basis* $[1, M, N]$ *is the basis of* R_r *which results on applying the steps of the Algorithm* B_1 *to* $[1, M_r^*, N_r^*]$, *then Algorithm* B_2 *terminates.*

Proof. Suppose we deal with step (2) of B_2. By Lemma 8.1 we have $|n_2| + \delta|n_3| < (3 + 2\sqrt{5})\delta^2$; and since $|\bar{y}_\nu| > I_2\sigma_r$, we have $|\eta_\nu| > \sqrt{3}/4$ by Lemma 7.6. From (8.1) it follows that $|\eta_\mu| > \sqrt{3}/4$ and from Lemma 8.2, we get $|n_3| < (2 + \sqrt{5})\delta$. Thus, since

$$|e_r|/|n_2 - \delta n_3| + |n_3| < 2\delta|e_r|/\sigma_r + (2+\sqrt{5})\delta < (2 + 2\sqrt{5})\delta,$$

we deduce from Corollary 7.5.1 that $k = [|\eta_\mu/\eta_\nu|] = [|y_\mu/y_\nu|]$. If we put $\eta_\nu^{(1)} = \eta_\mu$, $\eta_\nu^{(2)} = \eta_\nu$, $k_i = [|y_\nu^{(i)}/y_\nu^{(i+1)}|]$, we see by Lemma 8.2 that step (2) of B_2 will generate a sequence

$$\eta_\nu^{(1)}, \eta_\nu^{(2)}, \eta_\nu^{(3)}, \ldots, \eta_\nu^{(h)}, \ldots, \tag{8.3}$$

where $|\bar{y}_\nu^{(j+1)}| > I_2\sigma_r$, $\eta_\nu^{(j+2)} = k_j\eta_\nu^{(j+1)} + \eta_\nu^{(j)}$, $\eta_\nu^{(j+2)}\eta_\nu^{(j+1)} < 0$ and

$$|\eta_\nu^{(1)}| > |\eta_\nu^{(2)}| > |\eta_\nu^{(3)}| > \cdots > |\eta_\nu^{(h)}| > \cdots.$$

By Lemma 8.2, we know that, if $2\sigma_r\eta_\nu^{(j)}/\sqrt{3}\delta = n_2^{(j)} + n_3^{(j)}\delta$, then the values of $|n_2^{(j)}|$ and $|\delta n_3^{(j)}|$ are bounded by $(2+\sqrt{5})\delta^2$, thus there can be at most $4(2+\sqrt{5})^2D$ different pairs $(n_2^{(j)}, n_3^{(j)})$. If $|\bar{y}_\nu^{(j)}| > I_2\sigma_r$ for $j = 2, 3, 4, \ldots, h > 4(2+\sqrt{5})^2D$, we must have $r < s < h$ such that $(n_2^{(r)}, n_3^{(r)}) = (n_2^{(s)}, n_3^{(s)})$. Since $|\eta_\nu^{(r)}| > |\eta_\nu^{(s)}|$, this is impossible. It follows that we must eventually find some $h \leq 4(2+\sqrt{5})D^2$ such that $|\bar{y}_\nu^{(h)}| \leq I_2\sigma_r$. The proof that step (1) of B_2 terminates when $|\bar{y}_\mu| < I_2\sigma_r$ is similar to the above. □

When, after being applied to the basis $[1, M, N]$ above, Algorithm B_2 terminates we have a new basis $[1, \Psi, \Phi]$ of R_r, where

$$\Phi = (s_1 + s_2\delta + s_3\delta^2)/\sigma_r, \qquad \Psi = (t_1 + t_2\delta + t_3\delta^2)/\sigma_r. \tag{8.4}$$

If $\phi = (\xi_\phi, \eta_\phi)$ is the puncture of Φ and $\psi = (\xi_\psi, \eta_\psi)$ is the puncture of Ψ, then

$$|\eta_\phi| < |\eta_\psi|, \quad \eta_\phi\eta_\psi < 0, \quad \xi_\phi > \xi_\psi > 0, \quad |\bar{y}_\phi| \leq \sigma_r I_2 \quad \text{and} \quad |\bar{y}_\psi| \geq \sigma_r I_2.$$

LEMMA 8.4. *If* $I_2 > 128\sqrt{3}\delta^5/3 \simeq 73.90\delta^5$, *then* $[1, \Phi, \Psi]$ *is a* β*-basis.*

Proof. If we find Φ and Ψ by executing the steps of part (2) of B_2, we have $2\sigma_r|\eta_\psi|/\sqrt{3}\delta$, $2\sigma_r|\eta_\phi|/\sqrt{3}\delta < (3 + 2\sqrt{5})\delta^2$. Also, since η_ψ precedes η_ϕ in (8.3) we have $|\eta_\psi| > \sqrt{3}/4$ by Lemma 7.6. It follows that $|s_2 + \delta s_3| < 4\delta^2$ and $|s_2 - \delta s_3| < (3 + 2\sqrt{5})\delta^2$ and by Lemma 7.6, $|\eta_\phi| < 1 - \sqrt{3}/4$. By similar reasoning we can show that if we execute the steps of part (1) of B_2, we have $|\eta_\phi| < 1 - \sqrt{3}/4$, $|\eta_\psi| > \sqrt{3}/4$. If Φ and Ψ are found without having to execute either step (1) or (2) of B_2, then $|\eta_\phi| < 1 - \sqrt{3}/4$ and $|\eta_\psi| > \sqrt{3}/4$ by Lemmas 7.6 and 8.1.

Now $|\eta_\psi| = |\bar{y}_\psi|/2\sigma_r I_2 + \gamma \geqslant 1/2 - |\gamma|$, where $|\gamma| < (|t_2| + |t_3|\delta)/2\sigma_r I_2 < 2\delta^2/\sigma_r I_2$, from the proof of Lemma 6.1. Also,

$$|\eta_\phi|/2 = \sqrt{3}\delta|s_2 - s_3\delta|/4\sigma_r > \sqrt{3}\delta/(4\sigma_r(|s_2| + |s_3|\delta)^2) \quad \text{(Lemma 7.1)};$$

hence, from Lemma 6.1,

$$|\eta_\phi|/2 > \frac{\sqrt{3}}{64\sigma_r D} > \frac{2\delta^2}{\sigma_r I_2} > |\gamma|,$$

and $|\eta_\psi| > (1 - |\eta_\phi|)/2$. □

Let *Algorithm* B be that algorithm which we obtain on using Algorithm B_1 to substitute for the first four steps ((i), (ii), (iii), (iv)) of Algorithm A and Algorithm B_2 for the fifth step (v) of A with $I_1 > 3.1(2 + 2\sqrt{5})^3\delta^5$ and $I_2 > 128\sqrt{3}\delta^5/3$. We have now proved the following

THEOREM 8.5. *If θ is the puncture of $\theta_g^{(r)}$, the relative minimum of the second kind adjacent to* 1 *in R_r, then*

$$\theta = a\phi + b\psi,$$

where $(a, b) \in \{(1, 0), (0, 1), (1, -1), (1, 1), (2, 1)\}$ and ϕ and ψ are the punctures of Φ and Ψ found by using Algorithm B *on the basis* $[1, M_r^*, N_r^*]$ *of R_r.*

In the next section we show how to find $\theta_g^{(r)}$ once Φ and Ψ are known. As in Algorithm B, we wish to use as much integer arithmetic as possible.

9. Determination of $\theta_g^{(r)}$. Let $[1, \Phi, \Psi]$ in (8.4) be a β-basis. In order to determine the set S in Section 5 we need to be able to discover when $\xi_\psi > 1/3$, $\xi_\psi < 1/2$, and $|\eta_\psi| < \sqrt{3}/2$ by using only integers. To this end we define the symbols

$$X_\omega = [I_3\delta]q_2 + [I_3\delta^2]q_3, \quad Y_\omega = [I_3\delta]q_2 - [I_3\delta^2]q_3,$$

where I_3 is an arbitrary but fixed integer. Here $\omega = (\xi_\omega, \eta_\omega)$ is the puncture of any $\Omega = (q_1 + q_2\delta + q_3\delta^2)/\sigma_r \in R_r$.

Now $\xi_\psi = 3X_\psi/2I_3\sigma_r + \gamma$, where $|\gamma| < 3(|t_2| + |t_3|)/2I_3\sigma_r$. If $I_3 > 150\delta^2$, we see from (6.5) that $|\gamma| < 1/25$; thus, when $4X_\psi > \sigma_r I_3$, we have $3X_\psi/2I_3\sigma_r > 3/8$ and $\xi_\psi > .256$. Also, when $4X_\psi < \sigma_r I_3$, we have $\xi_\psi < ½$ $(I_3 > 150\delta^2)$.

To determine whether or not $|\eta_\psi| < \sqrt{3}/2$ is somewhat more difficult, we first note that $|\eta_\psi| < \sqrt{3}/2$ if and only if $\epsilon = \operatorname{sgn}(\sigma_r - |\delta t_1 - \delta^2 t_2|) > 0$. From (6.5) we have $|t_2| + \delta|t_3| < 4\delta^2$ and $3.1\delta^2(|t_2| + |t_3|)f(t_2, t_3) < 3.1\delta^2(4\delta^2)^3 < 200\delta^8$. It follows from Lemma 7.3 that $\operatorname{sgn}(I_3\sigma_r - |Y_\psi|) = \epsilon$ when $I_3 > 200\delta^8$. It should also be noted here that if $\Omega = \theta_g^{(r)}$, then from (6.8) we get $|q_2| + |q_3|\delta < (2 + 2\sqrt{3})\delta^2$ and

$$506\delta^8 > 3.1(2 + 2\sqrt{3})^3\delta^8 > 3.1\delta^2(|q_2| + |q_3|)f(q_2, q_3). \tag{9.1}$$

Hence, we can determine whether or not $|\eta_\omega| < \sqrt{3}/2$ by checking whether or not $|Y_\omega| < \sigma_r I_3$.

We now have

LEMMA 9.1. *Let S be defined as in Section 5. Then, if $I_3 > 200\delta^8$, S is given by Table 4 below.*

TABLE 4

restrictions on X_ψ and Y_ψ	S
$\lvert Y_\psi \rvert < \sigma_r I_3$	$\{(1, 0), (0, 1), (1, -1)\}$
$4\lvert X_\psi \rvert > \sigma_r I_3$	$\{(1, 0), (0, 1), (1, -1), (1, 1)\}$
$\lvert Y_\psi \rvert > \sigma_r I_3$, $4\lvert X_\psi \rvert < \sigma_r I_3$	$\{(1, 0), (1, -1), (1, 1), (2, 1)\}$

Proof. Follows from the above remarks and Table 2 of Section 5. □

We must now show how to find that element of S to which the puncture of $\theta_g^{(r)}$ corresponds. If $\Omega = a\Phi + b\Psi + c = (q_1 + q_2\delta + q_3\delta^2)/\sigma_r$, then $q_1 = \sigma_r c + q$, $q = as_1 + bt_1$, $q_2 = as_2 + bt_2$, and $q_3 = as_3 + bt_3$. Also

$$(9.2)\quad \begin{cases} [-a\zeta_\Phi - b\zeta_\Psi] = [(-2q + q_2\delta + q_3\delta^2)/2\sigma_r] \\ \qquad = [(-2q + [q_2\delta + q_3\delta^2])/2\sigma_r], \\ [1/2 - a\zeta_\Phi - b\zeta_\Psi] = [(\sigma_r - 2q + q_2\delta + q_3\delta^2)/2\sigma_r] \\ \qquad = [(\sigma_r - 2q + [q_2\delta + q_3\delta^2])/2\sigma_r]. \end{cases}$$

We now prove

LEMMA 9.2. *If $r, s, t \in Z$ and s and t are not both zero, then*

$$[r + s\delta + t\delta^2] = [(rI + s[\delta I] + t[\delta^2 I])/I],$$

when $I > 3.1\delta^2(|s| + |t|)f(s, t)$.

Proof. In the inequality $|r + s\delta + t\delta^2| > 1/3.1\delta^2 f(s, t)$ of Lemma 7.2, we note that the right-hand side is independent of r. If we put $T = s\delta + t\delta^2$ and select r such that $r + T = \{T\}$, then $\{T\} > 1/3.1\delta^2 f(s, t)$. If we select r such that $r + T = 1 - \{T\}$, then $1 - \{T\} > 1/3.1\delta^2 f(s, t)$.

If we put $A = (s[\delta I] + t[\delta^2 I])/I$, then

$$|A - T| < (|s| + |t|)/I < 1/3.1\delta^2 f(s, t).$$

Hence, $|A - T| < \min(\{T\}, 1 - \{T\})$ and we have $[T] < A < [T] + 1$. The lemma now follows easily. □

Now if $\Omega = \theta_g^{(r)}$, then $\Omega^* = \Omega$; thus by the remarks in Section 4, formulas (9.1) and (9.2) and Lemma 9.2, we have $c = l$ or possibly $l + 1$, where

$$(9.3)\qquad l = \begin{cases} [(([X_\omega/I_3] - 2q)/2\sigma_r] & (|Y_\omega| < \sigma_r I_3), \\ [(\sigma_r - 2q + [X_\omega/I_3])/2\sigma_r] & (|Y_\omega| > \sigma_r I_3), \end{cases}$$

and $I_3 > 506\delta^8$. Further c can be $l + 1$ only when $|Y_\omega| < \sigma_r I_3$ and

$$(9.4)\qquad (2\sigma_r l + 2q - q_2\delta - q_3\delta^2)/2\sigma_r < -1/2.$$

By (9.1) and Lemma 7.3, we see that (9.4) is true if and only if

$$(9.5)\qquad X_\omega - 2I_3 q > I_3\sigma_r + 2I_3\sigma_r l.$$

If, for each element of the set $\{a\Phi + b\Psi | (a, b) \in S\}$, we calculate possible values for c and $\Omega = c + a\Phi + b\Psi$ by using the formulas (9.3) and (9.5) above with $I_3 > 506\delta^8$, we get a set $P = \{\Omega_1, \Omega_2, \Omega_3, \ldots, \Omega_k\}$, where $k \leqslant 8$ and $\Omega_i = (q_{1i} + q_{2i}\delta + q_{3i}\delta^2)/\sigma_r$. One of these Ω_i is $\theta_g^{(r)}$. Further, if $\Omega = (q_1 + q_2\delta + q_3\delta^2)/\sigma_r$ is any element of this set, then by (6.5),

$$(9.6)\qquad |q_2| + |q_3|\delta \leqslant a(|s_2| + |s_3|\delta) + b(|t_2| + |t_3|\delta) < 12\delta^2$$

and

$$|X_\omega/I_3 - q_2\delta - q_3\delta^2| < (|q_2| + |q_3|)/I_3 < 1.$$

Since $-2 < [r] - s < 1$ when $|r - s| < 1$, we see, on putting $r = ([X_\omega/I_3] - 2q)/2\sigma_r$, $s = (-2q + q_2\delta + q_3\delta^2)/2\sigma_2$, that $|\zeta_\Omega| < 2$. Since $q_1/\sigma_r = \zeta_\Omega + \xi_\omega/3$, we have $|q_1| < 2\sigma_r + 12\delta^3/2$ from (9.6) and, therefore,

$$(9.7)\qquad |q_1| < 12D, \quad |q_2| < 12\delta^2, \quad |q_3| < 12\delta.$$

For each $\Omega_i = (q_{1i} + q_{2i}\delta + q_{3i}\delta^2)/\sigma_r \in P$ define $W_i = q_{1i}I_3 + q_{2i}[I_3\delta] + q_{3i}[I_3\delta^2]$, and let $W = \{W_i | \Omega_i \in P\}$. We now prove

LEMMA 9.3. *If W_j is the least element of W such that $\Omega_j \in C$, then $\theta_g^{(r)} = \Omega_j$.*

Proof. If $\Omega \in C \cap P$, then $\zeta_\Omega > -1$ and $\xi_\omega > 0$; hence $\Omega > -1$, and, since 1 is a relative minimum of R_r, we must have $\Omega > 1$. It follows that $\theta_g^{(r)}$ is the least element of $C \cap P$.

Suppose $\Omega_i = \theta_g^{(r)} \neq \Omega_j$; then $X = (x_1 + x_2\delta + x_3\delta^2)/\sigma_r = \Omega_j - \Omega_i > 0$. Further, $|x_2| + \delta|x_3| < |m_2| + |m_3|\delta + |q_{2j}| + |q_{3j}|\delta < (2 + 2\sqrt{3})\delta^2 + 12\delta^2 < 18\delta^2$ by (6.8) and (9.6). If χ is the puncture of X, we see that, since $\Omega_i, \Omega_j \in C$, we have $|\zeta_\chi|, |\eta_\chi| < 2$. Now $X \in R_r$ and $\sigma_1\sigma_r|e_r| \,|\, N(\sigma_r X)$ by Theorem 3.2; hence,

$$N(X) = |X|(\eta_\chi^2 + \zeta_\chi^2) > \sigma_1|e_r|/\sigma_r^2 = 1/Q_r > 1/3D$$

by (3.1) and (6.4). Since $\eta_\chi^2 + \zeta_\chi^2 < 8$, we find that $|X| > 1/24D$ and

$$I_3\sigma_r|X| > 506\delta^8\sigma_r/24D > 18\delta^2 > |x_2| + |x_3|\delta > |I_3\sigma_r X - W_j + W_i|;$$

thus, $\operatorname{sgn}(X) = \operatorname{sgn}(W_j - W_i)$. Since $X > 0$ and $W_j - W_i \leqslant 0$ (by definition of Ω_j), we have a contradiction. □

It remains to devise a technique, which uses integers only, to determine when $\Omega \in \mathcal{C}$. We do this in

THEOREM 9.4. *If* $q_1 + q_2[I_3\delta] + q_3[I_3\delta^2]$ *is the least element of* $\mathcal{W}$ *such that*

$$\sigma_1^2 Q_r^2 > 3\tau_r(\sigma_r q_1'/|e_r| - q_1\Sigma) + \Sigma^2,$$

where $\tau_r = \sigma_r/|e_r|$, $q_1' = q_1^2 - Dq_2q_3$, $q_2' = Dq_3^2 - q_1q_2$, $q_3' = q_2^2 - q_1q_3$, *and* $\Sigma = q_1'q_1 + D(q_2q_3' + q_3q_2')/|e_r|\sigma_r$, *then* $\theta_g^{(r)} = (q_1 + q_2\delta + q_3\delta^2)/\sigma_r$.

Proof. If $\Omega \in \mathcal{R}_r$, then $\Omega \in \mathcal{C}$ if and only if $\Omega'\Omega'' < 1$. But $\Omega'\Omega'' < 1$ if and only if $\Omega N(\Omega) < \Omega^2$ or $N(\Omega)N(\Omega - N(\Omega)) = N(\Omega^2 - \Omega N(\Omega)) > 0$ (since A and $N(A)$ have the same sign). It now suffices to note that

$$\begin{aligned} N(\Omega - N(\Omega)) &= N(\Omega)(1 - \mathrm{Tr}(\Omega\Omega') + N(\Omega)\mathrm{Tr}(\Omega) - N(\Omega)^2) \\ &= \frac{N(\Omega)}{\sigma_r^4}(\sigma_r^4 - 3q_1'\sigma_r^2 + 3\sigma_r q_1 N(\Omega)\sigma_r^2 - N(\Omega)^2\sigma_r^4) \\ &= \frac{N(\Omega)e_r^2}{\sigma_r^4}(\sigma_1^2Q_r^2 - 3\tau_r(\sigma_r q_1'/|e_r| - q_1\Sigma) - \Sigma^2), \end{aligned}$$

from (3.1). □

Note that from Theorem 3.2 both Σ and $q_1'/|e_r|$ are integers. Also, if $\Omega = \theta_g^{(r)}$, then

$$\Sigma = \sigma_r^2 N(\theta_g^{(r)})/|e_r| = \sigma_{r+1}^2/|e_{r+1}| = \sigma_1 Q_{r+1} < 3D \tag{9.8}$$

by Theorem 3.3, (3.1) and (6.4).

10. The Final Algorithm. We are now able to present the algorithm for determining R for $Q(\sqrt[3]{D})$ in its entirety. We first assume that $\delta = \sqrt[3]{D}$ has been calculated with sufficient accuracy that we can determine

$$d_1 = [I_1\delta], \quad d_2 = [\sqrt{3}I_2\delta], \quad d_3 = [\sqrt{3}I_2\delta^2], \quad d_4 = [I_3\delta],$$

$d_5 = [I_3\delta^2]$, where $I_1 = [841\delta^2 D] + 1, I_2 = [80\delta^2 D] + 1, I_3 = [506D^2\delta^2] + 1$.

In practice this is easily done by using Newton's method to determine δ. We also determine g_2 such that $D = g_1g_2^2$, $(g_1, g_2) = 1$ and g_1, g_2 are square-free.

When $D \equiv \pm 1 \pmod 9$, we put $m_1 = 0, m_2 = 3g_2, m_3 = 0, n_1 = g_2^2, n_2 = \pm g_2^2, n_3 = 1, \sigma = \sigma_1 = 3g_2, e = e_1 = 3g_2$; otherwise, put $m_1 = 0, m_2 = g_2, m_3 = 0, n_1 = 0, n_2 = 0, n_3 = 1, \sigma_1 = \sigma = e = e_1 = g_2$. We also initialize the value of r to be 1 and that of R to be 0.

Algorithm.

(I) Calculate, by using Algorithm B, the coefficients $s_1, s_2, s_3, t_1, t_2, t_3$ of the elements Φ and Ψ of the β-basis $[1, \Phi, \Psi]$ of $\mathcal{R}_r$.

(II) Determine $\theta_g^{(r)}, \theta_h^{(r)}$ and increase R by $\log \theta_g^{(r)}$. Calculate the coefficients $m_1, m_2, m_3, n_1, n_2, n_3$ and σ_{r+1} of the basis $[1, 1/\theta_g^{(r)}, \theta_h^{(r)}/\theta_g^{(r)}]$ of $\mathcal{R}_{r+1}$.

(III) Find $e_{r+1} = m_2 n_3 - n_2 m_3$. If $\sigma_{r+1} = \sigma$ and $|e_{r+1}| = e$, terminate the algorithm; otherwise increase r by 1 and return to (I).

We now describe the algorithms of I and II in more detail. We define as above

$$x_\mu = I_1 m_2 + d_1 m_3, \quad y_\mu = I_1 m_2 - d_1 m_3, \quad x_\nu = I_1 n_2 + d_1 n_3,$$
$$y_\nu = I_1 n_2 - d_1 n_3, \quad \bar{y}_\mu = d_2 m_2 - d_3 m_3, \quad \bar{y}_\nu = d_2 n_2 - d_3 n_3.$$

Algorithm I.

(i) Transform the basis of R_r by $K_2(-k, 1)$, where $k = [n_3/m_3]$ when $m_3 \neq 0$ or $k = [n_2/m_2]$ when $m_3 = 0$.

(ii) Transform the basis by $\begin{pmatrix} k_1 & 0 \\ 0 & k_2 \end{pmatrix}$, where $k_1 = \operatorname{sgn}(x_\mu)$, $k_2 = \operatorname{sgn}(x_\nu)$.

(iii) If $x_\nu < x_\mu$, transform the basis by $K_2(1, 1)$ and go to (iv) *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 go to (vi).

(iv) If $y_\mu y_\nu < 0$ go directly to step (v); 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 we find a basis such that $[y_\nu/y_\mu] \neq [x_\nu/x_\mu]$ we 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 (v).

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

(4) If $[x_\nu/x_\mu] < [y_\nu/y_\mu] - 1$, then transform the basis by $K_1([x_\nu/x_\mu] + 1, -1)$ when $|\bar{y}_\mu| < I_2\sigma_r$; otherwise, transform by $K_2([y_\nu/y_\mu], -1)$. Go to (vi).

(5) If $[x_\nu/x_\mu] > [y_\nu/y_\mu] + 1$, transform the basis by $K_1(-[x_\nu/x_\mu], 1)$ when $|\bar{y}_\mu| < I_2\sigma_r$; otherwise, transform by $K_2(-[y_\nu/y_\mu] - 1, 1)$. Go to (vi).

(v) If $|y_\mu| > |y_\nu|$, go to (vi). If $|y_\mu| \leqslant |y_\nu|$, transform the basis by $K_1(-[x_\nu/x_\mu], 1)$ when $|\bar{y}_\mu| < I_2\sigma_r$; otherwise transform by $K_2([-y_\nu/y_\mu], 1)$.

(vi) If $|\bar{y}_\mu| \geqslant I_2\sigma_r$ and $|\bar{y}_\nu| \leqslant I_2\sigma_r$, terminate Algorithm I. If $|\bar{y}_\mu| < I_2\sigma_r$ execute step (1) below; otherwise execute step (2).

(1) Transform the basis by $K_1(-k, 1)$, where $k = [x_\nu/x_\mu]$. Repeat this process until $|\bar{y}_\mu| \geqslant I_2\sigma_r$; at this point terminate Algorithm I.

(2) Transform the basis by $K_3(1, k)$, where $k = [-y_\mu/y_\nu]$. Repeat this process until $|\bar{y}_\nu| \leqslant I_2\sigma_r$; at this point terminate Algorithm I.

Note that in the process of making all the calculations needed to execute Algorithm I we never need an integer larger than $\max(n_2, m_2, n_3, m_3)I_1$. However, this is always less than $(|e_r| + (1 + \sqrt{5})\delta^2)I_1 < (3D + (1 + \sqrt{5})\delta^2)I_1$. Also, if we did not wish to carry the values of m_1 and n_1 during these calculations we could still determine s_1 and t_1 by using the formulas

$$e_r t_1 = k_{11} m_1 + k_{12} n_1, \quad e_r s_1 = k_{21} m_1 + k_{22} n_1,$$

where

$$k_{11} = \begin{vmatrix} t_2 & n_2^* \\ t_3 & n_3^* \end{vmatrix}, \quad k_{12} = \begin{vmatrix} m_2^* & t_2 \\ m_3^* & t_3 \end{vmatrix}, \quad k_{21} = \begin{vmatrix} s_2 & n_2^* \\ s_3 & n_3^* \end{vmatrix}, \quad k_{22} = \begin{vmatrix} m_2^* & s_2 \\ m_3^* & s_3 \end{vmatrix};$$

and n_2^*, n_3^*, m_2^*, m_3^* are, respectively, the values of n_2, n_3, m_2, m_3 before Algorithm I is executed. In order to ensure that s_1 and t_1 are not too large, we can reduce them modulo σ_r.

Algorithm II.

(i) Initialization. Put $\tau_r = \sigma_r/|e_r|$, $Q = \sigma_r \tau_r$. Calculate $s_2 d_4$, $s_3 d_5$, $t_2 d_4$, $t_3 d_5$, Q^2, $\sigma_r I_3$, $X_\phi = s_2 d_4 + s_3 d_5$, $Y_\phi = s_2 d_4 - s_3 d_5$, $X_\psi = t_2 d_4 + t_3 d_5$, $Y_\psi = t_2 d_4 - t_3 d_5$.

(ii) If $|Y_\psi| < \sigma_r I_3$, put $k = 3$ and $(a_1, b_1) = (1, 0)$, $(a_2, b_2) = (0, 1)$, $(a_3, b_3) = (1, -1)$. When $|Y_\psi| > \sigma_r I_3$, put $k = 4$. If $4|X_\psi| < \sigma_r I_3$, put $(a_1, b_1) = (1, 0)$, $(a_2, b_2) = (0, 1)$, $(a_3, b_3) = (1, -1)$, $(a_4, b_4) = (1, 1)$; otherwise put $(a_1, b_1) = (1, 0)$, $(a_2, b_2) = (1, -1)$, $(a_3, b_3) = (1, 1)$ and $(a_4, b_4) = (2, 1)$.

(iii) For each pair (a_i, b_i) calculate $q_i = a_i s_1 + b_i t_1$, $X_i = a_i X_\phi + b_i X_\psi$, $Y_i = a_i Y_\phi + b_i Y_\psi$.
If $|Y_i| < \sigma_r I_3$, put

$$l_{1i} = \left[\frac{[X_i/I_3] - 2q_i}{2\sigma_r} \right], \qquad q_{1i} = q_i + \sigma_r l_{1i}.$$

If $X_i - 2I_3 q_i > 2\sigma_r I_3 l_{1i} + \sigma_r I_3$, put

$$l_{2i} = l_{1i} + 1, \qquad q_{2i} = q_{1i} + \sigma_r.$$

If $|Y_i| > \sigma_r I_3$, put

$$l_{1i} = \left[\frac{\sigma_r - 2q_i + [X_i/I_3]}{2\sigma_r} \right], \qquad q_{1i} = q_i + \sigma_r l_{1i}.$$

Let $\mathcal{W} = \{I_3 q_{ji} + X_i | i \leqslant k, j \leqslant 2\}$. Since t_1 and s_1 have been reduced modulo σ_r, $q_i < 3\max(t_1, s_1) < 9D$ and $|2\sigma_r I_3 l_{1i}| < |X_i| + |2q_i I_3| + 2\sigma_r I_3$, we see by (9.6) that the largest integer needed in the calculations of Algorithm II to this point is less than $(24D + 13\delta^2)I_3$.

(iv) Find the minimum $I_3 q_{j\kappa} + X_\kappa$ of the set $\mathcal{W}$. Put $m_1 = q_{j\kappa}$, $m_2 = a_\kappa s_2 + b_\kappa t_2$, $m_3 = a_\kappa s_3 + b_\kappa t_3$ and calculate the integers (Theorem 3.2)

$$\bar{m}_1 = (m_1^2 - Dm_2 m_3)/|e_r|, \quad \bar{m}_2 = (Dm_3^2 - m_1 m_2)/|e_r|, \quad \bar{m}_3 = (m_2^2 - m_1 m_3)/|e_r|,$$

$$\Sigma = (m_1 \bar{m}_1 + D(m_2 \bar{m}_3 + m_3 \bar{m}_2))/\sigma_r.$$

If either

$$|\bar{m}_1| > [(1+\sqrt{5})\sqrt{3DD}], \quad |\bar{m}_2| > [(1+\sqrt{5})\sqrt{3D}\delta^2],$$

$$|\bar{m}_3| > [(1+\sqrt{5})\sqrt{3D}\delta], \quad \text{or } \Sigma > 3D,$$

then by (6.13) or (9.8), $(m_1 + m_2\delta + m_3\delta^2)/\sigma_r \neq \theta_g^{(r)}$ and we eliminate $I_3 q_{j\kappa} + X_\kappa$ from $\mathcal{W}$ and return to the beginning of step (iv). (This step is optional. It simply ensures that the numbers $\bar{m}_1, \bar{m}_2, \bar{m}_3$ and Σ do not get too large.)

If $\Sigma^2 + 3\tau_r(\bar{m}_1\sigma_r - m_1\Sigma) > Q^2$, eliminate $I_3 q_{j\kappa} + X_\kappa$ from $\mathcal{W}$ and return to step (iv); otherwise, put $n_1 = t_1$, $n_2 = t_2$, $n_3 = t_3$ when $\kappa = 1$ or $n_1 = s_1$, $n_2 = s_2$, $n_3 = s_3$ when $\kappa \neq 1$.

(v) Find $d = \text{g.c.d.}(\bar{m}_1, \bar{m}_2, \bar{m}_3)$ and replace the values of $\bar{m}_i$ by those of $\bar{m}_i/d$ $(i = 1, 2, 3)$. Calculate $\bar{n}_1 = n_1\bar{m}_1 + D(n_3\bar{m}_2 + n_2\bar{m}_3)$, $\bar{n}_2 = n_2\bar{m}_1 + n_1\bar{m}_2 + Dn_3\bar{m}_3$, $\bar{n}_3 = n_3\bar{m}_1 + n_2\bar{m}_2 + n_1\bar{m}_3$, $\bar{d} = \text{g.c.d.}(\bar{n}_1, \bar{n}_2, \bar{n}_3, \sigma_r)$, $\bar{\sigma}_r = \sigma_r/\bar{d}$.

Put $m_i = \bar{\sigma}_r\bar{m}_i$, $n_i = \bar{n}_i/\bar{d}$, $(i = 1, 2, 3)$, $\sigma_{r+1} = \Sigma/d\bar{d}$.

From (6.6), (6.11), (6.12) and the fact that $n_1 < \sigma_r < 3D$, we see that the numbers in (v) never exceed $36D^2$. Also, in step (iv), by (9.7), $|m_1| < 12D$, $|m_2| < 12\delta^2$, $|m_3| < 12\delta$; thus, we have $|\bar{m}_1|, |\bar{m}_2|, |\bar{m}_3| < 288D^2$.

11. Implementation of the Algorithms. Programs implementing the algorithms described above were written in Assembler Language for an IBM 370-168 computer. Use was made of double-precision arithmetic in all steps of the algorithms except in steps (i), (ii), (iii) and part of step (iv) of Algorithm II, where some extended-precision arithmetic was necessary. In the process of running these programs it was found that the speed of the algorithm could be improved by making the following alterations.

(1) When $D \geqslant 579$ check in step (iv) of Algorithm II whether or not

$$|Y_\kappa| > \left[\frac{2\sqrt{3}}{3}\sigma_r I_3\right] + [5\delta^2]$$

before calculating $\bar{m}_1, \bar{m}_2, \bar{m}_3$. If $\theta_g^{(r)} = \Omega_\kappa = (m_1 + m_2\delta + m_3\delta^2)/\sigma_r$, then from (6.9) $|m_2| + |m_3| < (2\sqrt{3}+1)\delta^2 + (2\sqrt{3}+1)\delta < 5\delta^2$. Thus, if

$$|Y_\kappa| > \left[\frac{2\sqrt{3}}{3}\sigma_r I_3\right] + [5\delta^2],$$

then

$$|Y_\kappa| > \frac{2\sqrt{3}}{3}\sigma_r I_3 + |m_2| + |m_3|.$$

Since $|2\sigma_r\eta/\sqrt{3} - Y/I_3| < (|m_2| + |m_3|)/I_3$, where (ξ, η) is the puncture of Ω_κ, we see that $|\eta| > 1$. It follows that $\theta_g^{(r)} \neq \Omega_\kappa$, and we can eliminate $I_3 q_{j\kappa} + X_\kappa$ from $\mathcal{W}$.

(2) Calculate R by adding $\log(\theta_g^{(k)}\theta_g^{(k+1)}\theta_g^{(k+2)} \cdots \theta_g^{(k+15)})$ instead of $\Sigma_{i=0}^{15} \log \theta_g^{(k+i)}$. This decreases the use of the expensive routine to calculate $\log x$.

With these improvements the computer was able to calculate $[1, M_{r+1}, N_{r+1}]$ from $[1, M_r, N_r]$ in less than 500 μ seconds. This improved the speed of our previous algorithm [2] by a factor of 10. Much, but not all, of this increase is due to the change in computer language from FORTRAN H to Assembler Language.

These programs were run for all 8984 $Q(\delta)$ such that $D < 10^5$ and the class number of $Q(\delta)$ is not divisible by three. These fields are those for which (Honda [4]) D has the following values:

(i) $D = 3$,

(ii) $D = p$, $p \equiv -1 \pmod 3$,

(iii) $D = 3p$ or $9p$ where $p \equiv 2, 5 \pmod 9$,

(iv) $D = pq$, where $p \equiv 2$, $q \equiv 5 \pmod 9$,

(v) $D = p^2q$, where $p \equiv q \equiv 2, 5 \pmod 9$ $(p < q)$.

Here p, q are primes. After the regulators were calculated, the class numbers $h(D)$ were evaluated by using the method of [8]. In the tables below we give some of the results of these calculations.

In Table 5 we give each class number h found, together with the frequency $f(h)$ with which h occurred, the percentage $100f(h)/8984$, and least D value such that $Q(\delta)$ has class number h.

TABLE 5

h	f(h)	100f(h)/8984	D
1	4537	50.50	2
2	2132	23.73	11
4	882	9.82	113
5	258	2.87	263
7	160	1.78	235
8	297	3.31	141
10	102	1.14	303
11	38	0.42	2348
13	29	0.32	1049
14	49	0.55	514
16	96	1.07	681
17	14	0.16	8511
19	16	0.18	667
20	54	0.60	761
22	22	0.24	281
23	7	0.08	21241
25	8	0.09	10181
26	11	0.12	3403
28	34	0.38	509
29	6	0.07	12079
31	2	0.02	16553
32	19	0.21	2399
34	10	0.11	1719
35	3	0.03	37207
37	6	0.07	5545
38	5	0.06	12813
40	17	0.19	2733
41	3	0.03	6659
43	5	0.06	32847
44	9	0.10	4817
46	2	0.02	59975
49	5	0.06	8171
50	6	0.07	14372
52	6	0.07	4793
53	1	0.01	38373
56	11	0.12	857
58	2	0.02	6814

h	f(h)	100f(h)/8984	D
59	1	0.01	95905
61	1	0.01	36161
62	2	0.02	42407
64	7	0.08	9749
65	1	0.01	88169
67	2	0.02	14073
68	4	0.04	9521
70	3	0.03	3467
71	3	0.03	3539
74	1	0.01	3581
76	2	0.02	23469
79	1	0.01	61741
80	6	0.07	4799
83	1	0.01	17362
85	2	0.02	10783
86	1	0.01	43403
89	1	0.01	64882
92	1	0.01	15131
95	3	0.03	15797
100	4	0.04	31547
101	1	0.01	48767
104	3	0.03	11549
110	2	0.02	17333
112	2	0.02	11665
115	1	0.01	99973
118	1	0.01	47093
121	1	0.01	57543
124	2	0.02	35349
127	1	0.01	2741
128	1	0.01	5987
136	4	0.04	3209
140	1	0.01	36263
148	3	0.03	60149
149	2	0.02	52737
154	2	0.02	9041
155	1	0.01	36107
158	1	0.01	66813
161	1	0.01	95001
170	1	0.01	45321
175	1	0.01	5711
181	1	0.01	12251
191	1	0.01	47639
193	1	0.01	46783
196	1	0.01	10522
200	2	0.02	12197
214	2	0.02	16823
230	1	0.01	4451
232	1	0.01	84093
254	1	0.01	8002
262	1	0.01	28979
280	1	0.01	35969
284	1	0.01	25913
296	1	0.01	26601
305	1	0.01	39821
316	2	0.02	39106
334	1	0.01	87257
340	1	0.01	18257
352	1	0.01	51549
358	1	0.01	27329
370	1	0.01	73779
389	1	0.01	24023
392	1	0.01	67157

h	f(h)	100f(h)/8984	D
400	1	0.01	53434
421	1	0.01	47303
433	1	0.01	69539
583	1	0.01	63766
628	1	0.01	61547
698	1	0.01	30867
706	1	0.01	26991
748	1	0.01	17573
827	1	0.01	97066
920	1	0.01	17579
980	1	0.01	38463
1190	1	0.01	74079
1442	1	0.01	32771
1484	1	0.01	79601
1640	1	0.01	54874
2380	1	0.01	54869

In Table 6, we give the values of D, the regulator $R(D)$ of $Q(\delta)$ and J, the length of Voronoi's algorithm period for δ such that $R(D) > R(d)$ for all d such that $8429 < d < D$ and $3 \nmid h(d)$. For the earlier part of this table see Table 5 of Barrucand, Williams and Baniuk [1].

TABLE 6

D	R(D)	J
10037	17941.60487	15972
10067	18150.81288	16318
11621	25661.99636	22908
14897	28630.01878	25280
15261	28634.12148	25190
15527	31541.56340	27991
17669	32388.80366	28517
19391	42811.86808	38337
21839	47361.35191	42122
22469	47942.75017	42716
26417	56816.82041	50385
28517	57091.82492	50671
29063	63398.84106	56707
32213	71481.68242	63674
34607	75693.99813	66931
36821	76097.18294	67252
38039	79677.96103	70707
39129	87213.59555	77128
39521	92172.43813	81615
43863	101072.02023	89956
54293	108016.52068	95477
55901	115433.63108	102213
56993	117983.12761	104106
60887	130509.10552	116010
62889	135188.22005	119536
66431	150019.35639	133096
72227	154817.70011	136734
72617	168197.50896	149072
76259	172072.28147	152790
84629	180297.38717	159867
88661	191840.92392	169795
90033	198214.96650	175891
92009	218706.73901	193034
96797	222426.50649	197114

Finally, in Table 7, we give the continuation of Table 3 of [8]. Here $n(x)$ is the number of primes q ($q \equiv -1 \pmod 3$) which are less than or equal to x and $g(x)$ is the number of those primes such that $h(q) = 1$.

TABLE 7

x	100g(x)/n(x)	x	100g(x)/n(x)	x	100g(x)/n(x)
36000	47.327	58000	48.474	80000	47.984
37000	46.910	59000	48.381	81000	48.030
38000	46.951	60000	48.225	82000	47.978
39000	46.945	61000	48.250	83000	47.975
40000	47.326	62000	48.210	84000	47.959
41000	47.190	63000	48.315	85000	47.837
42000	47.528	64000	48.260	86000	47.824
43000	47.184	65000	48.313	87000	47.798
44000	47.302	66000	48.336	88000	47.810
45000	47.595	67000	48.359	89000	47.747
46000	47.766	68000	48.203	90000	47.818
47000	47.826	69000	48.089	91000	47.920
48000	47.868	70000	47.998	92000	47.883
49000	47.866	71000	48.024	93000	47.826
50000	47.904	72000	47.979	94000	47.781
51000	47.922	73000	48.001	95000	47.680
52000	47.886	74000	48.081	96000	47.671
53000	47.994	75000	48.063	97000	47.617
54000	48.046	76000	47.941	98000	47.479
55000	48.111	77000	47.978	99000	47.418
56000	48.336	78000	47.884	100000	47.420
57000	48.432	79000	47.933	101000	47.379

The program described above was also used in [9] to find the class numbers of all pure cubic fields of the form $Q(\sqrt[3]{r})$, where $r \equiv 17 \pmod{18}$, r is a prime and $r < 2 \times 10^5$.

12. Acknowledgements. The authors wish to thank the referee for his careful reading of the original manuscript and his many useful suggestions for improvements. They also wish to thank D. H. and Emma Lehmer for making available to them an English translation of [6].

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

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

2. B. D. BEACH, H. C. WILLIAMS & C. R. ZARNKE, "Some computer results on units in quadratic and cubic fields," *Proc. Twenty-Fifth Summer Meeting of the Canadian Math. Congress*, Lakehead Univ., Thunder Bay, Ont., 1971, pp. 609–648.

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

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

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

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

7. HIDEO WADA, "A table of fundamental units of purely cubic fields," *Proc. Japan Acad.*, v. 46, 1970, pp. 1135–1140.

8. H. C. WILLIAMS, "Certain pure cubic fields with class number one," *Math. Comp.*, v. 31, 1977, pp. 578–580.

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