ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 15, Number 2, Spring 1985

# CONTINUED FRACTIONS AND NUMBER-THEORETIC COMPUTATIONS

HUGH C. WILLIAMS

Dedicated to the memory of E.G. Straus

ABSTRACT. The purpose of this mainly expository paper is to describe how continued fractions over $\mathcal{K} = \mathbf{Q}(\sqrt{D})$ can be used in the development of algorithms for solving computational problems in number theory. These problems include: the factoring problem, i. e., the determination of whether an ideal in $\mathcal{K}$ is principal; and the class group structure of $\mathcal{K}$. Some attention is also given to the extension of these methods to complex cubic fields.

**1. Introduction.** The purpose of this mainly (but not entirely) expository paper is to describe how continued fraction algorithms can be used to solve computational problems which arise in the study of real quadratic and complex cubic fields. Many of the recent results presented here are due to Shanks [**12**], [**13**], [**14**], [**15**], Lenstra [**5**], Schoof [**11**], and Williams, Dueck, Schmid [**22**]. They show that by using the fairly simple idea of 'distance', the usual algorithms for solving the type of problem discussed here (determination of the regulator, class number, class group structure, etc.) can be considerably improved. As this material is scattered about in several diverse places and is described in rather different ways, it was thought that a simple, unified approach to these results would be useful. Our presentation will stress the computational rather than the theoretic aspects of these ideas. For a more sophisticated description of the quadratic case see the work of Lenstra [**5**] and Schoof [**11**].

The material described here is pretty-well self-contained. We require only some well-known properties of ideals and lattices and these are reviewed in §2 and §3. In §4, §5, and §6 we show how continued fractions can be used to solve certain problems in real quadratic extensions and in §7 we describe some means by which the ideas developed here can be applied to the problem of factoring. Finally, in §8, §9, and §10

Received by the editors April 11, 1984.
Research supported by NSERC of Canada grant A7649 and by the I. W. Killam Foundation.

we discussed the extension of our previous developments to the case of complex cubic fields. Incidentally, the analogy between the type of continued fraction of the earlier sections and Voronoi's continued fraction is also pointed out.

It seems as if it should be possible to develop some further extension of the algorithms described here. Indeed, in an earlier version of [11] Schoof wrote that "it even seems probable that similar algorithms can be developed for every class of number field with fixed degree and signature, but perhaps it is even more probable that a project like that will involve a tremendous amount of work". It certainly seems that if the former part of this remark is true, then so is the latter. The results of §1 and §2 give some indication of how such extensions might be developed, but at the moment no general method is known for extending the results presented here.

**2. Ideals and reduced ideals.** In this section we summarize many well-known properties of ideals in algebraic number fields. Most of these can be found in any standard text such as Hua [3]. We begin with some notation. Let $p(x) \in \mathbf{Z}[x]$ be any polynomial of degree $d(\geqq 2)$, which is irreducible over the rationals $\mathbf{Q}$. If $\gamma$ is any zero of $p(x)$, denote by $\mathscr{K} = \mathbf{Q}(\gamma)$ the algebraic number field of degree $d$ formed by adjoining $\gamma$ to $\mathbf{Q}$. Let $p(x)$ have $s$ real zeros $\gamma_1, \gamma_2, \gamma_3, \ldots, \gamma_s$ and $2t$ complex zeros $\gamma_{s+1}, \bar{\gamma}_{s+1}, \gamma_{s+2}, \bar{\gamma}_{s+2}, \ldots, \gamma_{s+t}, \bar{\gamma}_{s+t}$, where this ordering of the $d = s + 2t$ zeros is fixed. If we define the $d$ mappings $\sigma_i$ $(i = 1, 2, 3, \ldots, d)$ of $\mathscr{K}$ into the set of complex numbers by $\sigma_i(\gamma) = \gamma_i$, $\sigma_i(\alpha + \beta) = \sigma_i(\alpha) + \sigma_i(\beta)$, and $\sigma_i(\alpha\beta) = \sigma_i(\alpha)\sigma_i(\beta)$, for any $\alpha, \beta \in \mathscr{K}$, then $\sigma_j(\gamma) = \gamma$, for some $j$, and the $d - 1$ conjugates of $\alpha \in \mathscr{K}$ are given by $\sigma_i(\alpha)$, where $1 \leqq i \leqq d$, but $i \neq j$. In the case of $d = 2$ or 3 we often use $\alpha'$ or $\alpha'$, $\alpha''$ to denote the conjugates of $\alpha$. We define the norm of $\alpha \in \mathscr{K}$ to be $N(\alpha) = \prod_{i=1}^{d} \sigma_i(\alpha)$. If $\alpha_i \in \mathscr{K} (i = 1, 2, 3, \ldots, k)$ are rationally independent, denote by $[\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_k]$ the set $\{\sum_{i=1}^{k} x_i\alpha_i \mid x_i \in \mathbf{Z}\}$. If $\mathrm{GL}_k(\mathbf{Z})$ is the group of all $k \times k$ matrices with entries from $\mathbf{Z}$ and determinant $\pm 1$, then $[\beta_1, \beta_2, \beta_3, \ldots, \beta_k] = [\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_k]$ if and only if

$$A = MB, \tag{2.1}$$

where $A$ is the vector $(\alpha_1\alpha_2\alpha_3\cdots\alpha_k)$, $B = (\beta_1\beta_2\beta_3\cdots\beta_k)$ and $M \in \mathrm{GL}_k(\mathbf{Z})$. We will require the following theorem.

THEOREM 2.1. *Let $a$ be the* $\gcd(a_{11}, a_{12}, a_{13}, \ldots, a_{1k})$, *where* $a_{ij} \in \mathbf{Z}$ $(j = 1, 2, 3, \ldots, k)$. *There is a matrix* $M \in \mathrm{GL}_k(\mathbf{Z})$ *whose first row is made up of the entries* $a_{11}/a, a_{12}/a, a_{13}/a, \ldots, a_{1k}/a$.

For a proof of this result, where we insist that $|M| = 1$, see, for example, [3, p. 376].

Let $\mathcal{O}_{\mathcal{K}}$ be the ring of algebraic integers in $\mathcal{K}$. There exist $\omega_1, \omega_2, \omega_3, \ldots, \omega_d \in \mathcal{O}_{\mathcal{K}}$ such that $\mathcal{O}_{\mathcal{K}} = [\omega_1, \omega_2, \omega_3, \ldots, \omega_d]$ and the set $\{\omega_1, \omega_2, \omega_3, \ldots, \omega_4\}$ is called a basis of $\mathcal{O}_{\mathcal{K}}$. By virtue of Theorem 2.1 and (2.1) we may assume that there exists a basis of $\mathcal{O}_{\mathcal{K}}$, where $\omega_1 = 1$. If we put $\beta_{ij} = \sigma_i(\alpha_j)$ and define $\Delta[\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_d] = |\beta_{ij}|^2_{d\times d}$, then the discriminant $\Delta$ of $\mathcal{K}$ is defined to $\Delta[\omega_1, \omega_2, \omega_3, \ldots, \omega_d]$.

The subset $\mathfrak{a}$ of $\mathcal{O}_{\mathcal{K}}$ is an ideal of $\mathcal{O}_{\mathcal{K}}$ if for any $\alpha, \beta \in \mathfrak{a}$ we must have $\alpha + \beta \in \mathfrak{a}$ and $\alpha\xi \in \mathfrak{a}$ for any $\xi \in \mathcal{O}_{\mathcal{K}}$. If $\beta_1, \beta_2, \beta_3, \ldots, \beta_m \in \mathcal{O}_{\mathcal{K}}$ and we denote by $(\beta_1, \beta_2, \beta_3, \ldots, \beta_m)$ the set $\{\sum_{i=1}^{m} \xi_i\beta_i \mid \xi_i \in \mathcal{O}_{\mathcal{K}}\}$, then we see that this set is an ideal of $\mathcal{O}_{\mathcal{K}}$ and we say that $\beta_1, \beta_2, \beta_3, \ldots, \beta_m$ are generators of this ideal. Further, if $\mathfrak{a}$ is any ideal of $\mathcal{O}_{\mathcal{K}}$, then $\mathfrak{a} = (\beta_1, \beta_2, \beta_3, \ldots, \beta_m)$ for some $\beta_i \in \mathcal{O}_{\mathcal{K}}$ $(i = 1, 2, 3, \ldots m)$ and $m$ is finite. Indeed, we have the following result.

THEOREM 2.2. *If $\mathfrak{a}$ is any ideal of $\mathcal{O}_{\mathcal{K}}$, then there exist $\alpha_i \in \mathcal{O}_{\mathcal{K}}$ $(i = 1, 2, 3, \ldots d)$ such that*

$$\begin{aligned}
\alpha_1 &= a_{11}\omega_1 \\
\alpha_2 &= a_{21}\omega_1 + a_{22}\omega_2 \\
&\cdots\cdots\cdots\cdots \\
\alpha_d &= a_{d1}\omega_1 + a_{d2}\omega_2 + a_{d3}\omega_3 + \cdots + a_{dd}\omega_d,
\end{aligned}$$

*where $a_{ij} \in \mathbf{Z}$, $a_{ii} > 0$ $(i = 1, 2, 3, \ldots, d)$ and*

$$\mathfrak{a} = [\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_d].$$

If, for some $\beta_1, \beta_2, \beta_3, \ldots, \beta_d \in \mathcal{O}_{\mathcal{K}}$, we have $\mathfrak{a} = [\beta_1, \beta_2, \beta_3, \ldots, \beta_d]$, we say that the set $\{\beta_1, \beta_2, \beta_3, \ldots, \beta_d\}$ is a basis of $\mathfrak{a}$.

We say that an ideal $\mathfrak{a} = (\alpha)$, which is generated by a single generator, is a principal ideal. If $\mathfrak{a} = (\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_k)$, $\mathfrak{b} = (\beta_1, \beta_2, \beta_3, \ldots \beta_m)$, we define the product $\mathfrak{a}\mathfrak{b}$ as that ideal generated by the $km$ generators $\alpha_i\beta_j (i = 1, 2, 3, \ldots k; j = 1, 2, 3, \ldots, m)$. If $\mathfrak{a}$ and $\mathfrak{b}$ are two ideals of $\mathcal{O}_{\mathcal{K}}$ and there exist $\alpha, \beta \in \mathcal{O}_{\mathcal{K}}$ such that $(\alpha)\ \mathfrak{a} = (\beta)\ \mathfrak{b}$, then $\mathfrak{a}$ and $\mathfrak{b}$ are equivalent and write this as $\mathfrak{a} \sim \mathfrak{b}$. This is a true equivalence relation which partitions the set of ideals of $\mathcal{O}_{\mathcal{K}}$ into a finite number $h$ (the class number) of distinct equivalence classes. This set of equivalence classes forms a group $G$ called the class group of $\mathcal{K}$. From the definition of an ideal we see that if $\mathfrak{a} = [\alpha_1, \alpha_2, \ldots, \alpha_d]$ is an ideal of $\mathcal{O}_{\mathcal{K}}$ and $\lambda A = \mu MB$, where $\lambda, \mu \in \mathcal{O}_{\mathcal{K}}$, $A = (\alpha_1\alpha_2\alpha_3 \cdots \alpha_d)$, $B = (\beta_1\beta_2\beta_3 \cdots \beta_d)$, then $\mathfrak{b} = [\beta_1, \beta_2, \beta_3, \ldots, \beta_d]$ is an ideal and $\mathfrak{a} \sim \mathfrak{b}$.

As usual we say that the ideal $\mathfrak{a}$ divides the ideal $\mathfrak{b}$ $(\mathfrak{a}|\mathfrak{b})$ if there exists an ideal $\mathfrak{c}$ such that $\mathfrak{b} = \mathfrak{a}\mathfrak{c}$. Also $\mathfrak{a}|\mathfrak{b}$ if and only if $\mathfrak{b} \subseteq \mathfrak{a}$. If $\mathfrak{a}|(\alpha)$, we say that $\mathfrak{a}$ divides $\alpha$ $(\mathfrak{a}|\alpha)$. If $\mathfrak{a}|\alpha - \beta$, when $\alpha, \beta \in \mathcal{O}_{\mathcal{K}}$, then we say that $\alpha$ and

$\beta$ are congruent modulo $\mathfrak{a}$ ($\alpha \equiv \beta \pmod{\mathfrak{a}}$). If we denote by $N(\mathfrak{a})$ (the norm of $\mathfrak{a}$) the number of distinct residue classes modulo $\mathfrak{a}$, then

$$\Delta[\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_d] = N(\mathfrak{a})^2\Delta, \tag{2.2}$$

where $\mathfrak{a} = [\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_d]$. Also, if $\mathfrak{a} = (\alpha)$, then $N(\mathfrak{a}) = |N(\alpha)|$. We also mention the result that $N(\mathfrak{a}\mathfrak{b}) = N(\mathfrak{a})N(\mathfrak{b})$. Throughout this work we shall assume that the ideals we are considering are not the zero ideal (0).

If $\omega_1 = 1$, we see from Theorem 2.2 that $\mathfrak{a} = [a_{11}, \alpha_2, \alpha_3, \ldots, \alpha_d]$, where $a_{11} \in \mathbf{Z}$. This value of $a_{11}$ is unique for $\mathfrak{a}$ and is the least positive rational integer in $\mathfrak{a}$. We denote it by $L(\mathfrak{a})$. Since $L(\mathfrak{a}) \in \mathfrak{a}$, we know that there must exist an ideal $\mathfrak{a}'$ such that

$$\mathfrak{a}\mathfrak{a}' = (L(\mathfrak{a})). \tag{2.3}$$

We use (2.3) to define $\mathfrak{a}'$.

We say that $\mathfrak{a}$ is a primitive ideal if it has no rational integer divisors except 1; that is, if $(k)|\mathfrak{a}$, where $k \in \mathbf{Z}$, then $k = 1$. A reduced ideal is a primitive ideal $\mathfrak{a}$ such that there does not exist any non-zero $\alpha \in \mathfrak{a}$ that satisfies $|\sigma_i(\alpha)| < L(\mathfrak{a})$ for $i = 1, 2, 3, \ldots, d$. In what follows, this concept of a reduced ideal will prove to be very important.

**3. Lattices in $\mathscr{K}$.** If $\{A_1, A_2, A_3, \ldots A_k\}$ is a set of $k$ $n$-vectors which are independent over $\mathbf{Z}$, we say that $\mathscr{L} = \{\sum_{i=1}^{k} x_i A_i \mid x_i \in \mathbf{Z}\}$ is a lattice with basis $\{A_1, A_2, A_3, \ldots, A_k\}$. In this section we discuss some properties of special lattices in $\mathscr{K}$. For more information on this topic we refer the reader to Delone and Faddeev [2].

For $\alpha \in \mathscr{K}$, define the corresponding $d$-vector $A$ by

$$A = (\sigma_1(\alpha), \sigma_2(\alpha), \ldots, \sigma_s(\alpha), \operatorname{Re}(\sigma_{s+1}(\alpha)), \operatorname{Im}(\sigma_{s+1}(\alpha)),$$
$$\operatorname{Re}(\sigma_{s+2}(\alpha)), \operatorname{Im}(\sigma_{s+2}(\alpha)), \ldots, \operatorname{Re}(\sigma_{s+t}(\alpha)), \operatorname{Im}(\sigma_{s+t}(\alpha))),$$

where $\operatorname{Re}(z)$ and $\operatorname{Im}(z)$ are the real and imaginary parts of the complex number $z$. (Note that, in this instance, the notation represents a $d$-vector and should not be confused with the notation for an ideal given in section 2.) If $\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_d \in \mathscr{K}$ are rationally independent, consider the lattice $\mathscr{L} = \{\sum_{i=1}^{d} x_i A_i \mid x_i \in \mathbf{Z}\}$ in $\mathscr{K}$. Since the ordering of the zeros of $p(x)$ is fixed, we see that $A$ is completely determined once $\alpha$ is. We therefore often use the more convenient expression $\alpha \in \mathscr{L}$ to denote that it is actually the correspnding vector $A$ that is in $\mathscr{L}$. We also say that $\mathscr{L}$ above has $\{\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_d\}$ as a basis. Further if $\theta \in \mathscr{K}$, we define $\mathscr{L}^* = \theta\mathscr{L}$ to be the lattice with basis $\{\theta\alpha_1, \theta\alpha_2, \theta\alpha_3, \ldots, \theta\alpha_d\}$.

LEMMA 3.1. *Let $\mathscr{L}$ be a lattice with basis $\{\mu_1, \mu_2, \mu_3, \ldots, \mu_d\}$, with* $\mu_1 =$

1. *If* $\lambda = \sum_{i=1}^{d} x_i\mu_i (x_i \in \mathbf{Z})$, *and* gcd $(x_1, x_2, x_3, \ldots, x_d) = 1$, *then* $\mathscr{L}$ *has a basis* $[\nu_1, \nu_2, \nu_3, \ldots, \nu_d]$, *with* $\nu_1 = 1$ *and* $\nu_2 = \lambda$.

PROOF. Let $X \in \mathrm{GL}_{d-1}(\mathbf{Z})$ such that the first row of $X$ is made up of the entries $x_2, x_3, x_4, \ldots, x_d$. Put

$$Y = \left(\begin{array}{c|c} 1 & 0 \\ \hline x_1 & \\ 0 & X \end{array}\right)_{d\times d}, \quad M = \begin{pmatrix} \mu_1 \\ \mu_2 \\ \vdots \\ \mu_d \end{pmatrix}, \quad N = \begin{pmatrix} \nu_1 \\ \nu_2 \\ \vdots \\ \nu_d \end{pmatrix}.$$

Clearly, $Y \in \mathrm{GL}_d(\mathbf{Z})$, and if $N = YM$, we have our result.

If $\mathfrak{a} = [L(\mathfrak{a}), \alpha_2, \alpha_3, \ldots, \alpha_d]$ is an ideal of $\mathscr{O}_{\mathscr{K}}$ we say that the lattice $\mathscr{L}$ with basis $\{1, \alpha_2/L(\mathfrak{a}), \alpha_3/L(\mathfrak{a}), \ldots, \alpha_d/L(\mathfrak{a})\}$ is the lattice that corresponds to $\mathfrak{a}$.

LEMMA 3.2. *Let* $\mathscr{L}$ *be the lattice that corresponds to an ideal* $\mathfrak{a}$ *and let* $\mathscr{L}^*$ *be a lattice with basis* $\{1, \nu_2, \nu_3, \ldots, \nu_d\}$. *If* $\theta\,\mathscr{L}^* = \mathscr{L}$, *then there exists a primitive ideal* $\mathfrak{b}$ *such that* $\mathscr{L}^*$ *corresponds to* $\mathfrak{b}$ *and*

$$(L(\mathfrak{a})\theta)\mathfrak{b} = (L(\mathfrak{b}))\mathfrak{a}. \tag{3.1}$$

PROOF. Let $m$ be the least positive rational integer such that $\lambda_i = m\nu_i \in \mathscr{O}_{\mathscr{K}} (i = 1, 2, 3, \ldots, d)$. If $\mathfrak{a} = [L(\mathfrak{a}), \alpha_2, \alpha_3, \ldots, \alpha_d]$, then

$$L(\mathfrak{a})\theta \begin{pmatrix} m \\ \lambda_2 \\ \vdots \\ \lambda_d \end{pmatrix} = mM \begin{pmatrix} L(\mathfrak{a}) \\ \alpha_2 \\ \vdots \\ \alpha_d \end{pmatrix},$$

where $M \in \mathrm{GL}_d(\mathbf{Z})$. Thus $\mathfrak{b} = [m, \lambda_2, \lambda_3, \ldots \lambda_d]$ is an ideal, $m = L(\mathfrak{b})$ and $\mathfrak{b}$ is primitive.

The normed body $\mathscr{N}(\alpha)$ for $\alpha \in \mathscr{L}$ is defined to be the set of $d$-vectors

$$\mathscr{N}(\alpha) = \{(x_1, x_2, x_3, \ldots, x_d) | x_i \text{ real}, |x_i| < \sigma_i(\alpha)\ (i = 1, 2, 3, \ldots, s),$$
$$x_i^2 + x_{i+1}^2 < \sigma_i(\alpha)^2\ (i = s + 1, s + 3, \ldots, s + 2t - 1)\}.$$

For example, when $d = 2$ and $t = 0$, $\mathscr{N}(\alpha)$ can be considered geometrically as an open rectangle which is symmetric about the origin. We say that $\phi$ (or the corresponding vector $\Phi$) is a minimum of $\mathscr{L}$ if $\phi \in \mathscr{L}$ and $\mathscr{N}(\phi) \cap \mathscr{L} = \{0\}$, where 0 is the $d$-vector $(0, 0, 0, \ldots, 0)$. If $\mathscr{L}$ is a lattice with basis $\{1, \mu_2, \mu_3, \ldots, \mu_d\}$ and 1 is also a minimum of $\mathscr{L}$, we say that $\mathscr{L}$ is a reduced lattice. Notice that an ideal $\mathfrak{a}$ is reduced if and only if its corresponding lattice is reduced.

THEOREM 3.3. *Let* $\mathscr{L}$ *be a lattice with basis* $\{1, \mu_2, \mu_3, \ldots, \mu_d\}$. *There exists some* $\theta \in \mathscr{L}$ *such that* $\mathscr{L}^* = (1/\theta)\,\mathscr{L}$ *and* $\mathscr{L}^*$ *is a reduced lattice.*

PROOF. If $\mathscr{L}$ is already reduced, then $\theta = 1$ and $\mathscr{L}^* = \mathscr{L}$. If $\mathscr{L}$ is not reduced there must exist some $\rho \in \mathscr{L}$ such that $\rho \neq 0$ and

$$|\sigma_i(\rho)| < 1 \quad (i = 1, 2, 3, \ldots, s + t). \tag{3.2}$$

If $S$ is the matrix $(\sigma_i(\mu_j))_{d\times d}$ ($\mu_1 = 1$), then since the $\mu_i$ are rationally independent, we have $|S| \neq 0$. Let $S^{-1} = (\tau_{ij})_{d\times d}$. If

$$\rho = \sum_{j=1}^{d} x_j\mu_j \qquad (x_j \in \mathbf{Z},\ j = 1, 2, 3, \ldots, d),$$

then

$$x_j = \sum_{i=1}^{d} \tau_{ji}\sigma_i(\rho)$$

and

$$|x_j| \leqq \sum_{i=1}^{n} |\tau_{ji}|.$$

Thus, there can only be a finite number of elements of $\mathscr{L}$ that satisfy (3.2). Let $P_1 = \{\rho_1^{(1)}, \rho_2^{(1)}, \rho_3^{(1)}, \ldots, \rho_k^{(1)}\}$ be the set of these $\rho$ values in $\mathscr{L} = \mathscr{L}_1$. Since $|\sigma_i(-\rho)| = |\sigma_i(\rho)|$, we see that $k$ must be even. If $\rho \in P_1$ and $\rho = \sum_{i=1}^{d} x_i\mu_i$, put $f = \gcd(x_2, x_3, \ldots, x_d)$ and $y \equiv x_1 \pmod f$, with $|y| \leqq f/2$. We have $0 \neq \beta = (\rho - y)/f \in \mathscr{L}$ and $|\sigma_i(\beta)| \leqq |\sigma_i(\rho)|/f + |y/f| < 1/f + 1/2$. Thus, if $f \geqq 2$, we see that $\beta \in P_1$. We may therefore assume with no loss of generality that we have a $\rho = \rho_g^{(1)} = \sum_{i=1}^{d} x_i\mu_i \in P_1$ with $\gcd(x_2, x_3, \ldots, x_d) = 1$. By Lemma 3.1, $\mathscr{L}_1$ has a basis of the form $\{1, \rho_g^{(1)}, \nu_3, \nu_4, \ldots, \nu_d\}$. If $\mathscr{L}_2 = 1/\rho_g^{(1)}\,\mathscr{L}_1$, then $\mathscr{L}_2$ has a basis containing 1. If $\mathscr{L}_2$ is reduced, we are finished. If $\mathscr{L}_2$ is not reduced, there must exist a set $P_2 = \{\rho_1^{(2)}, \rho_2^{(2)}, \ldots, \rho_h^{(2)}\}$ of all the non-zero elements of $\mathscr{L}_2$ which satisfy (3.2). If $\rho \in P_2$, then $\lambda = \pm\rho_g^{(1)}\rho \in \mathscr{L}_1$ and

$$|\sigma_i(\lambda)| = |\sigma_i(\rho_g^{(i)})|\ |\sigma_i(\rho)| < 1 \quad (i = 1, 2, 3, \ldots, s + t);$$

thus $\lambda \in P_1$. Since $\lambda \neq \pm\rho_g^{(1)}$, we get $|P_1| \geqq |P_2| + 2$. We can next find a value for $\rho_g^{(2)}$ in $\mathscr{L}_2$ and define $\mathscr{L}_3 = (1/\rho_g^{(2)})\mathscr{L}_2$. Since the number of elements satisfying (3.2) in $\mathscr{L}_3$ is strictly less than $|P_2|$, we see that by continuing this process, we must ultimately find some $\mathscr{L}_n$ such that $\mathscr{L}_n$ is reduced.

If we define

$$\rho_n = \prod_{i=1}^{n-1} \rho_g^{(i)}, \tag{3.3}$$

we have

$$\mathscr{L}^* = \mathscr{L}_n = (1/\rho_n)\mathscr{L}. \tag{3.4}$$

Putting $\mathscr{L}^* = \mathscr{L}_n$ and $\theta = \rho_n$, we have our result.

COROLLARY. *If* $\mathfrak{a}$ *is any ideal, then there exists a reduced ideal* $\mathfrak{b}$ *and a* $\lambda \in \mathfrak{a}$ *such that* $(\lambda)\mathfrak{b} = (\mathscr{L}(\mathfrak{b}))\mathfrak{a}$.

PROOF. Let $\mathfrak{b}$ be the primitive ideal which corresponds to $\mathscr{L}_n$ in (3.4). Since $\lambda = \rho_n \mathscr{L}(\mathfrak{a}) \in \mathfrak{a}$, the corollary follows by the theorem and Lemma 3.2.

Thus, there is always at least one reduced ideal in every ideal class of $\mathscr{K}$. The proof of Theorem 3.3 provides us with an algorithm for finding a reduced ideal equivalent to another; however, it is not a very practical algorithm. We will describe better algorithms in the case of $d = 2$, $s = 2$ and $d = 3$, $s = 1$ below. Another important aspect of minima in $\mathscr{L}$ for our work is given in the following result.

THEOREM 3.4. *Let* $\mathscr{L}$ *and* $\mathscr{L}^*$ *be reduced lattices. If* $\theta\mathscr{L}^* = \mathscr{L}$, *then* $\theta$ *is a minimum of* $\mathscr{L}$.

PROOF. Clearly, $\theta \in \mathscr{L}$. If $\theta$ is not a minimum of $\mathscr{L}$, then there must exist $\phi \in \mathscr{L}$ such that $\phi \neq 0$ and $|\sigma_i(\phi)| < |\sigma_i(\theta)|$ $(i = 1, 2, 3, \ldots, s + t)$. Now consider $\beta = \phi/\theta$. We must have $\beta \in \mathscr{L}^*$, but $|\sigma_i(\beta)| = |\sigma_i(\theta)/\sigma_i(\phi)| < 1$ $(i = 1, 2, 3, \ldots, s + t)$ and $\beta \neq 0$. This contradicts the assumption that $\mathscr{L}^*$ is a reduced lattice.

Thus, the problem of finding all of the reduced ideals in any ideal class containing a given ideal $\mathfrak{a}$ reduces to the problem of finding all the minima in the lattice $\mathscr{L}$ corresponding to $\mathfrak{a}$. We also notice that if $\eta$ is any unit of $\mathscr{K}$, then $(\eta)\mathfrak{a} = \mathfrak{a}$ and, as a consequence of this, $\eta\theta$ is a minimum of $\mathscr{L}$ if $\theta$ is a minimum of $\mathscr{L}$ and $\mathscr{L}$ corresponds to $\mathfrak{a}$. In general, the problem of finding all the minima in $\mathscr{L}$ is rather complicated. In order to simplify it, we make at this point an assumption concerning our lattice $\mathscr{L}$ in $\mathscr{K}$. We will assume that $\mathscr{K}$ has the property that if $\alpha, \beta \in \mathscr{K}$ and $|\sigma_i(\alpha)| = |\sigma_i(\beta)|$ for any $i \leqq s + t$, then $\alpha = \pm \beta$. This is certainly true when $\mathscr{K}$ is totally real $(s = d)$, and it is also true for $d = 3$ and $s = 1$. It is not, however, true for $d = 4$ and $s = 0$. For example, let $\gamma = \sqrt{(-1 + \sqrt{-3})/2}$ and $\mathscr{K} = \mathbf{Q}(\gamma)$. We have $|\alpha| = |\beta|$, when $\alpha = \gamma\beta$.

Under our simplifying assumption, we can define what is meant when two minima of $\mathscr{L}$ are said to be adjacent. Let $\theta$ and $\phi$ be minima of $\mathscr{L}$ such that, for some $k \leqq s + t$, we have $|\sigma_k(\theta)| > |\sigma_k(\phi)|$ and $|\sigma_i(\theta)| < |\sigma_i(\phi)|$, for all other $i \neq k$. The minima $\theta$ and $\phi$ are adjacent if there does not exist $a\ \psi \in \mathscr{L}$ such that $|\sigma_k(\phi)| < |\sigma_k(\psi)| < |\sigma_k(\theta)|$ and $|\sigma_i(\psi)| < |\sigma_i(\phi)|$ for all $i \neq k$. If $k$ is a fixed integer such that $1 \leqq k \leqq s + t$ and

$$\theta_1, \theta_2, \theta_3, \ldots, \theta_m, \ldots \tag{3.5}$$

is a sequence of minima in $\mathscr{L}$ such that $|\sigma_k(\theta_{i+1})| > |\sigma_k(\theta_i)|$ and $\theta_{i+1}$, $\theta_i$

are adjacent, we call (3.5) a $k$-chain of minima of $\mathscr{L}$. By Minkowski's Theorem (see [2]) we know that such chains always exist in $\mathscr{L}$ and that they may be extended to any length.

In order to show how the elements in (3.5) can be constructed, we require several simple lemmas.

LEMMA 3.5. *Let $\mathscr{L}$ be a reduced lattice. If $\theta$ is a minimum of $\mathscr{L}$ adjacent to* 1, *then there exist $\nu_3, \nu_4, \nu_5, \ldots, \nu_d \in \mathscr{K}$ such that $\mathscr{L}$ has $\{1, \theta, \nu_3, \nu_4, \ldots, \nu_d\}$ as a basis.*

PROOF. Certainly, there exist $x_1, x_2, x_3, \ldots, x_d \in \mathbf{Z}$ such that $\theta = \sum_{i=1}^{d} x_i \mu_i$, where $\mu_1 = 1$ and $\{\mu_1, \mu_2, \mu_3, \ldots, \mu_d\}$ is a basis of $\mathscr{L}$. Let $f = \gcd(x_2, x_3, \ldots, x_d)$ and put $y \equiv x_i \pmod{d}$, where $|y| \leqq d/2$. If $\beta = (\theta - y)/f$, then $\beta \neq 0$ and $\beta \in \mathscr{L}$. Further,

$$|\sigma_i(\beta)| \leqq |\sigma_i(\theta)|/f + |y/f| \leqq |\sigma_i(\theta)|/f + 1/2.$$

Now, for some $k$, we have $|\sigma_k(\theta)| > 1$ and $|\sigma_i(\theta)| < 1$, for all $i \neq k$. Thus, if $f \geqq 2$, we get $|\sigma_k(\beta)| < |\sigma_k(\theta)|$ and $|\sigma_i(\beta)| < 1$ for $i \neq k$. By definition of $\theta$, this is impossible; thus, our lemma follows from Lemma 3.1.

LEMMA 3.6. *If $\mathscr{L}$ and $\theta$ are as defined in Lemma* 3.5 *and $\mathscr{L}^* = (1/\theta)\mathscr{L}$, then $\mathscr{L}^*$ is a reduced lattice.*

PROOF. We note from the previous lemma that there exists a basis of $\mathscr{L}^*$ which contains 1. If $\mathscr{L}^*$ were not reduced, there would exist $\beta \in \mathscr{L}^*$ ($\beta \neq 0$) such that $|\sigma_i(\beta)| < 1$ ($i = 1, 2, 3, \ldots, s + t$). In this case, we have $\lambda = \beta\theta \in \mathscr{L}$ and

$$|\sigma_i(\lambda)| = |\sigma_i(\beta)\sigma_i(\theta)| < |\sigma_i(\theta)| \quad (i = 1, 2, 3, \ldots, s + t).$$

By definition of $\theta$, this is impossible.

LEMMA 3.7. *Let $\mathscr{L}$, $\mathscr{L}^*$ and $\theta$ be as defined in Lemma* 3.6 *and let $\omega$ be the minimum adjacent to $\theta$ in $\mathscr{L}$. If $\theta^*$ is the minimum adjacent to* 1 *in $\mathscr{L}^*$, then $\omega = \theta\theta^*$.*

PROOF. Let $\phi = \theta\theta^*$. For some $k \leqq s + t$, we have $|\sigma_k(\phi)| = |\sigma_k(\theta)\sigma_k(\theta^*)| > |\sigma_k(\theta)|$ and $|\sigma_i(\phi)| < |\sigma_i(\theta)|$, for $1 \leqq i \leqq s + t$ and $i \neq k$. Thus, if $\phi \neq \omega$, then $|\sigma_k(\omega)| < |\sigma_k(\phi)|$ and $|\sigma_i(\omega)| < |\sigma_i(\theta)|$ ($i \neq k$). Since $\omega/\theta \neq 0$, $\omega/\theta \in \mathscr{L}^*$, and

$$|\sigma_k(\omega/\theta)| < |\sigma_k(\theta^*)|, |\sigma_i(\omega/\theta)| < 1 \quad (i \neq k),$$

we have a contradiction to the definition of $\theta^*$.

Let $\mathscr{L} = \mathscr{L}_1$ be any reduced lattice. As an example of such we mention that if $\{\omega_1, \omega_2, \omega_3, \ldots, \omega_d\}$ is a basis of $\mathcal{O}_{\mathscr{K}}$, then it is also the basis of a reduced lattice. For a fixed $k$, let $\theta_g^{(i)}$ be a minimum adjacent to 1 in $\mathscr{L}_i$,

with $|\sigma_k(\theta_g^{(i)})| > 1$. Define $\mathscr{L}_{i+1} = (1/\theta_g^{(i)})\mathscr{L}_i$. By our previous results, we see that each $\mathscr{L}_i$ is reduced, and if $\theta_1 = 1$ in (3.5), then we have

$$\theta_n = \prod_{i=1}^{n-1} \theta_g^{(i)} \tag{3.6}$$

and

$$\theta_n \mathscr{L}_n = \mathscr{L}_1. \tag{3.7}$$

Thus, we can find the elements in a chain (3.5) with $\theta_1 = 1$, once we are able to solve the problem of finding the minimum adjacent to 1 in any reduced lattice. This is a problem that we shall examine for the case of $s + t = 2$ only. The reason we choose this case is explained by the following lemma.

LEMMA 3.8. *If $s + t = 2$ and $\theta$ is any minimum in a reduced lattice $\mathscr{L}$ such that $|\sigma_k(\theta)| > 1$, then there must exist some $\theta_m$ in the $k$-chain* (3.6) *such that $\theta = \pm\theta_m$.*

PROOF. Since $s + t = 2$, if $i \neq k$, then $i = 3 - k$. If $\pm\theta$ is not an element of the $k$-chain (3.5), there must exist a $\theta_m$ and $\theta_{m+1}$ such that

$$|\sigma_k(\theta_m)| < |\sigma_k(\theta)| < |\sigma_k(\theta_{m+1})|.$$

Since $\theta$ is a minimum, we must also have $|\sigma_i(\theta_m)| > |\sigma_i(\theta)|$ for $i \neq k$. This contradicts the definition of $\theta_{m+1}$.

We are left with lattices in fields for which $s = 2$, $t = 0$, $\mathscr{K} = \mathbf{Q}(\sqrt{D})$, $D \in \mathbf{Z}$, $D > 0$, $\sqrt{D} \notin \mathbf{Q}$ and $s = t = 1$, $\mathscr{K} = \mathbf{Q}(\delta)$, where $\delta$ is the real zero of an irreducible cubic $p(x)$ with negative discriminant. We will denote lattices in these fields by the symbols $\mathscr{S}$ and $\mathscr{R}$ respectively. We also define $\sigma_1(\alpha) = \alpha$, $\sigma_2(\alpha) = \alpha'$ and, in the case of $d = 3$, $\sigma_3(\alpha) = \alpha''$.

**4. Continued fractions.** Let $\mathscr{K} = \mathbf{Q}(\sqrt{D})$, where $D > 0$, $D \in \mathbf{Z}$ and $\sqrt{D} \notin \mathbf{Q}$. Let $\mathscr{S}$ be any lattice in $\mathscr{K}$ as described in the previous section. If $\mathscr{S}$ is not a reduced lattice we have the problem of finding a reduced lattice $\mathscr{S}^*$ and $\rho \in \mathscr{S}$ such that $\rho\mathscr{S}^* = \mathscr{S}$. If $\mathscr{S}$ is a reduced lattice, we have the problem of finding a chain (3.5) when $\theta_1 = 1$. We will show how a particular continued fraction can be used to solve both problems in an expeditious manner. In order to do this we need the following result of Voronoi [19].

THEOREM 4.1. *Let $\mathscr{S}$ have $\{\phi, \psi\}$ as a basis and suppose that $\psi > \phi > 0$. Then $\phi$ and $\psi$ are adjacent minima of $\mathscr{S}$ if and only if $|\phi'| > |\psi'|$ and $\psi'\phi' < 0$.*

PROOF. If $\psi$ and $\phi$ are adjacent minima of $\mathscr{S}$, then we have $|\phi'| > |\psi'|$.

Since $0 < \psi - \phi < \psi$, we must have $|\psi' - \phi'| > |\psi'|$; otherwise, $\psi$ could not be a minimum. Hence $\phi'\psi' < 0$.

Suppose $|\phi'| > |\psi'|$ and $\phi'\psi' < 0$. If $\phi$ is not a minimum of $\mathscr{S}$, there must exist $\beta \in \mathscr{S}$ such that $|\beta| < \phi$ and $|\beta'| < |\phi'|$. Since $\beta = a\phi + b\psi$ ($a, b \in \mathbf{Z}$), this means that $|a\phi + b\psi| < \phi$, $|a\phi' + b\psi'| < |\phi'|$. Clearly, neither $a$ nor $b$ is zero; but, if $ab > 0$, then $|a\phi + b\psi| > \phi$ and if $ab < 0$, then $|a\phi' + b\psi'| > |\phi'|$. Thus, $\phi$ must be a minimum of $\mathscr{S}$ and, by similar reasoning, so is $\psi$. Further, there can not exist $a, b \in \mathbf{Z}$ such that both $|a\phi + b\psi| < \psi$ and $|a\phi' + b\psi'| < |\phi'|$ hold; thus, $\phi$ and $\psi$ are adjacent minima of $\mathscr{S}$.

We are now ready to develop our continued fraction algorithm. Let $\mathscr{S} = \mathscr{S}_1$ have $\{1, \mu_1\}$ as a basis and define

$$\begin{aligned}
\nu_n &= \mu_n + [-\mu_n'], \\
\psi_n &= \begin{cases} \nu_n + 1 & \text{when } \nu_n < -1/2 \\ \nu_n & \text{otherwise,} \end{cases} \\
\mu_{n+1} &= -\operatorname{sgn}(N(\psi_n))/\psi_n, \\
\mathscr{S}_{n+1} &= (1/\psi_n)\mathscr{S}_n.
\end{aligned}$$

(We use $[\alpha]$ here to denote that integer such that $\alpha - 1 < [\alpha] \leqq \alpha$.)

We note that $-1 < \nu_n' < 0$; thus, if $\nu_n > 1$, then $\mathscr{S}_n$ must be reduced by Theorem 4.1. If $\nu_n < -2$, then $-1 < -1 - \nu_n' < 0$ and $-1 - \nu_n > 1$. Again, $\mathscr{S}_n$ is reduced. Notice that, in either case, $|\psi_n|$ is the minimum adjacent to 1 in $\mathscr{S}_n$. Now, if $-2 < \nu_n < -1$, or if $0 < \nu_n < 1$, then $N(\psi_n) < 0$ and $\nu_{n+1} = 1/\psi_n + [-1/\psi_n']$. We have $\nu_{n+1} < -2$ when $-2 < \nu_n < -1$, and $\nu_{n+1} > 1$ when $0 < \nu_n < 1$. Thus, $\mathscr{S}_{n+1}$ is a reduced lattice. Also, $|\psi_n| < 1$. If $-1 < \nu_n < 0$, then $\mathscr{S}_n$ can not be a reduced lattice and $0 < \psi_n < 1/2$. Since there can only be a finite number of elements of $\mathscr{S}$ inside the normed body of 1, there must exist a positive $c$ ($< 1$) such that each of these elements in absolute value exceeds $c$. If we put $\rho_g^{(i)} = \psi_i$, we must have $\rho_n$ in (3.3) satisfying $\rho_n \geqq c$. Then $n < -\log c/\log 2$ and our algorithm will find a reduced lattice $\mathscr{S}_m$ in $O(|\log c|)$ operations.

If we define $\phi_n$ by $\phi_0 = -\mu_1'$, $\phi_n|\psi_n'| = 1$ ($n \geqq 1$), we see that $\phi_n > 1$ ($n \geqq 1$) and, if $r_1 = 1$, then

$$\phi_{n+1} = r_{n+1}/(\phi_n - q_n),$$

where $|r_{n+1}| = 1$ and $r_{n+1}, q_n \in \mathbf{Z}$. Indeed, $r_{n+1} = -\operatorname{sgn} \psi_n \operatorname{sgn} \psi_{n+1}'$ ($n \geqq 1$), and it can be shown that if $n \geqq 1$, then $r_{n+1} = -1$, when $-\phi_n' + [\phi_n] < -1/2$ and $r_{n+1} = 1$ otherwise. Thus

$$\phi = \phi_0 = q_0 + \cfrac{r_1}{q_2 + \cfrac{r_2}{q_3 + \ddots + \cfrac{r_n}{\phi_n}}} \tag{4.1}$$

is a semi-regular continued fraction expansion of $\phi$ (see Perron [8, p. 152]).

If we define

$$C_m = q_0 + \cfrac{r_1}{q_2 + \cfrac{r_2}{q_3 + \ddots + \cfrac{r_m}{q_m}}},$$

then $C_m = A_m/B_m$, where $r_0 = 1$, $A_{-2} = 0$, $A_{-1} = 1$, $B_{-2} = 1$, $B_{-1} = 0$ and $A_{k+1} = q_{k+1}A_k + r_{k+1}A_{k-1}$, $B_{k+1} = q_{k+1}B_k + r_{k+1}B_{k-1}$ $(k = -1, 0, 1, \ldots)$.

Further

$$A_mB_{m-1} - B_mA_{m-1} = (-1)^{m-1}\, r_1r_2r_3 \ldots r_m.$$

If $\phi_0 = (P_0 + \sqrt{D})/Q_0$, with $P_0, Q_0 \in \mathbf{Z}$, and $Q_0 | D - P_0^2$, define $P_n$, $Q_n$ by $\phi_n = (P_n + \sqrt{D})/Q_n$ $(P_n, Q_n \in \mathbf{Z})$. It is easy to verify that

$$P_{k+1} = q_kQ_k - P_k,\ Q_{k+1} = r_{k+1}\,(D - P_{k+1}^2)/Q_k \quad (k = 0, 1, 2, \ldots).$$

Also,

$$q_{k+1} = \left[\frac{p_{k+1} + \sqrt{D}}{Q_{k+1}}\right] + \frac{1 - r_{k+2}}{2} \quad (k = -1, 0, 1, \ldots).$$

Put $\theta_1 = 1$ and, for $n > 1$, define

$$\theta_n = (Q_{n-1} \prod_{i=1}^{n-1} \phi_i)\, Q_0 \tag{4.2}$$

Since $N(\phi_i) = -r_iQ_{i-1}/Q_i$, we see that

$$N(\theta_n) = (-1)^{n-1}\,(Q_{n-1}/Q^0) \prod_{i=1}^{n-1} r_i, \tag{4.3}$$

$$|\psi_n| = |Q_n\phi_n/Q_{n-1}|,$$

and

$$|\theta_n| = \prod_{i=1}^{n-1} |\phi_i|. \tag{4.4}$$

Since

$$\phi_0 = \phi = \frac{\phi_n A_{n-1} + r_n A_{n-2}}{\phi_n B_{n-1} + r_n B_{n-2}},$$

we have

$$r_n \phi_n = \frac{A_{n-2} - \phi B_{n-2}}{\phi B_{n-1} - A_{n-1}}.$$

From this result it is a simple matter to show by induction that

$$\theta_n = A_{n-2} - \phi' B_{n-2} \ (n = 1, 2, 3, \ldots). \tag{4.5}$$

It is also a simple matter to show that $\mathscr{S}_n$ is reduced if and only if $-1 < \phi_n' < 0$. When this occurs we see that $r_{n+1} = 1$ and $-1 - [\phi_n] < \phi_n' - [\phi_n] < -[\phi_n]$; thus, $-1 < \phi_{n+1}' = (\phi_n' - [\phi_n])^{-1} > 0$ and we have, for all $k \geqq n$, $r_{k+1} = 1$,

$$(P_k + \sqrt{D})/Q_n > 1, \quad -1 < (P_k - \sqrt{D})/Q_k < 0;$$

consequently,

$$0 < Q_k < 2\sqrt{D}; \quad 0 < P_k < \sqrt{D}. \tag{4.6}$$

Furthermore,

$$\theta_g^{(k)} = |\psi_k| = \frac{P_k + \sqrt{D}}{r_k Q_{k-1}} > 1 \text{ and } -1 < \theta_g^{(k)\prime} < 0, \tag{4.7}$$

for all $k \geqq n$.

In the case of $\mathscr{S}_1$ being reduced, we see that the $\theta_n$ in (4.2) is the same as the $\theta_n$ in (3.6). That is, our continued fraction algorithm produces all the minima $\theta$ of $\mathscr{S}_1$ such that $\theta > 1$. Since

$$\theta_g^{(k+1)} = 1/\theta_g^{(k)} + [-1/\theta_g^{(k)\prime}],$$

we get

$$\theta_g^{(k+1)} \theta_g^{(k)} > 1 + [-1/\theta_g^{(k)\prime}] > 2;$$

hence

$$\theta_n > 2^{[(n-1)/2]}. \tag{4.8}$$

We end this section by remarking that if we have a regular continued fraction expansion of $\phi$; that is, if all $r_i = 1$ $(i \geqq 1)$, (we certainly do when $\mathscr{S}_1$ is reduced), then Lévy has shown that for almost all irrational $\phi$, we have

$$\lim_{n\to\infty} (\phi_1 \phi_2 \phi_3 \cdots \phi_n)^{1/n} = e^{\prime}, \tag{4.9}$$

where $\prime = \pi^2/(12 \log 2) \approx 1.18656911$.

**5. Ideals in $\mathbf{Q}(\sqrt{D})$.** Let $D$ be a positive square-free rational integer, $\mathscr{K} = \mathbf{Q}(\sqrt{D})$, and

$$r = \begin{cases} 2 & D \equiv 1 \pmod 4 \\ 1 & \text{otherwise.} \end{cases}$$

We have $\Delta = 4D/r^2$, and if $\omega = (r - 1 + \sqrt{D})/r$, then $\mathcal{O}_{\mathscr{K}} = [1, \omega]$. By the remarks of §2, we see that if $\mathfrak{a}$ is any ideal of $\mathcal{O}_{\mathscr{K}}$, then $\mathfrak{a} = [L(\mathfrak{a}), b + c\omega]$ $(b, c \in \mathbf{Z}, c > 0)$. Since $L(\mathfrak{a}) \in \mathfrak{a}$ and $b + c\omega \in \mathfrak{a}$, we must have $N(\mathfrak{a}) | N(b + c\omega)$ and $N(\mathfrak{a}) | N(L(\mathfrak{a}))$. Since $N(\mathfrak{a}) = |cL(\mathfrak{a})|$, $N(L(\mathfrak{a})) = L(\mathfrak{a})^2$, and $N(b + c\omega) = b^2 + bc(\omega + \omega') + c^2\omega\omega'$, it follows that if $\mathfrak{a}$ is primitive, then $|c| = 1$ and $N(\mathfrak{a}) = L(\mathfrak{a})$. Also, two primitive ideals $\mathfrak{a}_1 = [L(\mathfrak{a}_1), b_1 + \omega]$ and $\mathfrak{a}_2 = [L(\mathfrak{a}_2), b_2 + \omega]$ are equal if and only if $L(\mathfrak{a}_1) = L(\mathfrak{a}_2)$ and $b_1 \equiv b_2 \pmod{L(\mathfrak{a}_1)}$. We can also easily prove the following theorem.

THEOREM 5.1. *If* $\mathfrak{a} = [L(\mathfrak{a}), b + \omega]$, *then* $\mathfrak{a}$ *is a primitive ideal of* $\mathscr{K}$ *if and only if* $L(\mathfrak{a}) | N(b + \omega)$.

We illustrate a means of finding a basis of $\mathfrak{a}$, given the generators of $\mathfrak{a}$, by using the specific case of $\mathfrak{a} = (\alpha, \beta)$. By definition of $\mathfrak{a}$, we must get $\mathfrak{a} = [\alpha, \beta, \alpha\omega, \beta\omega]$. If $\alpha = a_1 + a_2\omega$, $\beta = b_1 + b_2\omega$, then

$$\mathfrak{a} = [a_1 + a_2\omega, b_1 + b_2\omega, -\omega\omega' a_2 + \omega(a_1 + a_2(\omega + \omega')), \\ - b_2\omega\omega' + \omega(b_1 + b_2(\omega + \omega'))].$$

We may assume that $g = \gcd(a_1, b_1, a_2, b_2) = 1$; for, otherwise we can write $\mathfrak{a} = (g)(\alpha/g, \beta/g)$ and consider $(\alpha/g, \beta/g)$. Thus, we can find $x_1$, $x_2$, $x_3$, $x_4 \in \mathbf{Z}$ such that

$$x_1a_2 + x_2b_2 + x_3(a_1 + a_2(\omega + \omega')) + x_4(b_1 + b_2(\omega + \omega')) = 1$$

and put

$$m = x_1a_1 + x_2b_1 - \omega\omega' a_2x_3 - \omega\omega' b_2x_4.$$

Then $\mathfrak{a} = [\alpha, \beta, \alpha\omega, \beta\omega, m + \omega]$ and, by subtracting suitable multiples of $m + \omega$ from each of $\alpha$, $\beta$, $\alpha\omega$, $\alpha\beta$, we get $\mathfrak{a} = [c_1, c_2, c_3, c_4, m + \omega]$, where $c_1, c_2, c_3, c_4 \in \mathbf{Z}$. Hence, if $n = \gcd(c_1, c_2, c_3, c_4)$, then $\mathfrak{a} = [n, m + \omega]$.

If $\mathfrak{a} = [a_1, b_1 + \omega]$, $\mathfrak{b} = [a_2, b_2 + \omega]$, then $\mathfrak{ab} = (s)[a_3, b_3 + \omega]$. The problem of determining $s, a_3, b_3$ given $a_1, b_1, a_2, b_2$ can be handled (see [5]) by noting that

$$\mathfrak{ab} = [a_1a_2, a_1b_2 + a_1\omega, a_2b_1 + a_2\omega, b_1b_2 - \omega\omega' + (\omega + \omega' + b_1 + b_2)\omega] \\ = (s)[a_3, b_3 + \omega].$$

From this, it follows that $s = \gcd(a_1, a_2, \omega + \omega' + b_1 + b_2)$. Also, since $N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b}) = s^2a_3$, we have $a_3 = a_1a_2/s^2$ and

$$L(\mathfrak{ab}) = L(\mathfrak{a})L(\mathfrak{b})/s^2. \tag{5.1}$$

Now there exist $x_1, x_2, x_3 \in \mathbf{Z}$ such that

$$s = x_1a_1 + x_2a_2 + x_3(\omega + \omega' + b_1 + b_2);$$

hence,

$$b_3 \equiv (x_1a_1b_2 + x_2a_2b_1 + x_3(b_1b_2 - \omega\omega'))/s \pmod{a_3}.$$

In order to develop a connection between the continued fraction (4.1) and our ideals here, we simply point out that $\mathscr{S}_n$ has as a basis $\{1, \mu_n\}$, $|\mu_n| = |1/\psi_{n-1}|$, $|1/\psi_{n-1}| = |\phi_n'|$ for $n \geqq 2$, and $|\phi_0'| = |\mu_1|$. Thus $\mathscr{S}_n$ has $\{1, \phi_n'\}$ as a basis for $n \geqq 1$. By Theorem 5.1. we may assume that $\mathfrak{a}_1 = [Q_0/r, (-P_0 + \sqrt{D})/r]$, where $L(\mathfrak{a}_1) = Q_0/r$, $P_0 \in \mathbf{Z}$, and $rQ_0|D - P_0^2$. Since $\mathscr{S}_n$ is the lattice that corresponds to $\mathfrak{a}_n$, when

$$\begin{aligned} \mathfrak{a}_n &= [|Q_{n-1}|/r, \quad (-P_{n-1} + \sqrt{D})/r] \\ &= [|Q_{n-1}|/r, \quad (P_n + \sqrt{D})/r], \end{aligned} \tag{5.2}$$

we have, from (3.1), that

$$(L(\mathfrak{a}_1)\theta_n)\mathfrak{a}_n = (L(\mathfrak{a}_n))\mathfrak{a}_1, \tag{5.3}$$

for $\theta_n$ defined in (4.2). For any primitive $\mathfrak{a}_1$ we know that there must exist some $n$ for which $\mathfrak{a}_n$ will be reduced. We will now obtain an upper bound on this value of $n$. We require first some results on reduced ideals in $\mathbf{Q}(\sqrt{D})$.

THEOREM 5.2. *If $\mathfrak{a}$ is a reduced ideal in $\mathbf{Q}(\sqrt{D})$, then $L(\mathfrak{a}) < \sqrt{\Delta}$.*

PROOF. If $\mathfrak{a}$ is reduced, by Theorem 4.1 and Lemma 3.5, there must exist $\lambda \in \mathfrak{a}$ such that $\lambda > L(\mathfrak{a})$, $-L(\mathfrak{a}) < \lambda' < 0$, and $\mathfrak{a} = [L(\mathfrak{a}), \lambda]$; thus, $L(\mathfrak{a}) < \lambda - \lambda'$ and $\lambda - \lambda' = \omega - \omega' = \sqrt{\Delta}$.

THEOREM 5.3. *Let $\mathfrak{a}$ be any primitive ideal in $\mathbf{Q}(\sqrt{D})$. If $L(\mathfrak{a}) < \sqrt{\Delta}/2$, then $\mathfrak{a}$ is reduced.*

PROOF. Let $\mathfrak{a} = [L(\mathfrak{a}), \beta]$, where $\beta = b + \omega$ and put $\lambda = \beta + [-\beta'/L(\mathfrak{a})]L(\mathfrak{a})$. Then $\mathfrak{a} = [L(\mathfrak{a}), \lambda]$ and $-L(\mathfrak{a}) < \lambda' < 0$. Since $\lambda > \omega - \omega' - L(\mathfrak{a})$ and $\omega - \omega' = \sqrt{\Delta} > 2L(\mathfrak{a})$, we have $\lambda > L(\mathfrak{a})$. By Theorem 4.1, $\mathfrak{a}$ is reduced.

Let $\mathfrak{a}_n$ in (5.3) be reduced and suppose that $\mathfrak{a}_{n-1}$ is not reduced. By virtue of the results derived in the earlier part of this section, we may assume that $|\psi_i| < 1/2$ for $1 \leqq i \leqq n - 2$; thus,

$$|N(\psi_i)| = L(\mathfrak{a}_{i+1})/L(\mathfrak{a}_i) < 1/2 \quad (i \leqq n - 2)$$

and $L(\mathfrak{a}_{n-1})/L(\mathfrak{a}_1) < 1/2^{n-2}$, for $n \geqq 2$. Since $\mathfrak{a}_{n-1}$ is not reduced, we have $L(\mathfrak{a}_{n-1}) > \sqrt{\Delta}/2$ by the previous theorem; hence, $1/2^{n-2} > \sqrt{\Delta}/2L(\mathfrak{a}_1)$. It follows that

$$n < 3 + \log(L(\mathfrak{a}_1)/\sqrt{\Delta}) \log 2. \tag{5.4}$$

Also, if $\lambda = L(\mathfrak{a}_1)|\theta_n|$, then, from (4.4), we have $|\lambda| \leqq L(\mathfrak{a}_1)$, $|\lambda'| \leqq L(\mathfrak{a}_1)$. Since $\lambda \in \mathfrak{a}_1$ we have $(\lambda)|\mathfrak{a}_1$ and $N(\lambda)|N(\mathfrak{a}_1)$. Thus $|\lambda\lambda'| \geqq L(\mathfrak{a}_1)$ and

$$1 < \lambda \leqq L(\mathfrak{a}_1) \tag{5.5}$$

with equality only when $\mathfrak{a}_1$ is reduced.

Let $\varepsilon_0 (> 1)$ be the fundamental unit of $\mathbf{Q}(\sqrt{D})$. If $\mathfrak{a}_1$ and $\mathfrak{b}$ are any two reduced ideals in the same ideal class of $\mathbf{Q}(\sqrt{D})$, then there must exist some $\theta$ in the lattice $\mathscr{S}_1$ which corresponds to $\mathfrak{a}_1$ such that $(\theta L(\mathfrak{a}_1))\mathfrak{b} = (L(\mathfrak{b}))\mathfrak{a}_1$. Let $\phi = \pm \varepsilon_0^m \theta$ such that $\phi > 1$. Then $(\phi L(\mathfrak{a}_1))\mathfrak{b} = (L(\mathfrak{b}))\mathfrak{a}_1$, and, by Theorem 3.4, $\phi$ must also be a minimum of $\mathscr{S}_1$. By Lemma 3.8, we have $\phi = \theta_k$ for some $k$; hence, since $\mathfrak{b}$ and $\mathfrak{a}_k$ are both primitive, we must have $\mathfrak{b} = \mathfrak{a}_k$. Thus the continued fraction (4.1) finds, for any given primitive ideal, all the reduced ideals that are in the same ideal class. We also note that $\varepsilon_0 \in \mathscr{S}_1$ and, indeed, is a minimum of $\mathscr{S}_1$; hence, there must exist some $p$ such that $\theta_{p+1} = \varepsilon_0$. Also, since $\mathfrak{a}_{p+1} = \mathfrak{a}_1$, we get

$$\mathfrak{a}_{p+t} = \mathfrak{a}_t \quad (t \geqq 1) \tag{5.6}$$

and

$$\theta_{p+t} = \varepsilon_0 \theta_t \quad (t \geqq 1). \tag{5.7}$$

This of course, is simply the well-known result that the continued fraction development of a quadratic irrational is periodic. Here, the period length is the quantity $p$.

**6. The distance between reduced ideals and applications.** Let $\mathscr{K} = \mathbf{Q}(\sqrt{D})$ and let $\mathfrak{a}_1$ be any reduced ideal of $\mathscr{O}_{\mathscr{K}}$. From (5.3), we get

$$(L(\mathfrak{a}_m)\theta_n)\mathfrak{a}_n = (L(\mathfrak{a}_n)\theta_m)\mathfrak{a}_m.$$

Let $n \geqq m$. In [13] Shanks introduced the idea of distance between $\mathfrak{a}_n$ and $\mathfrak{a}_m$ and defined this as $d(\mathfrak{a}_n, \mathfrak{a}_m) = \log(\theta_n/\theta_m)$. In [5] Lenstra defines a different distance, using $(1/2)\log(L(\mathfrak{a}_m)/L(\mathfrak{a}_n)) + \log(\theta_n/\theta_m)$ instead of just $\log(\theta_n/\theta_m)$. Lenstra's definition is more convenient in certain applications but we will use Shanks' definition here, as it is more easily extended to the cubic case. From (4.2), (4.4), and (4.7), we find that

$$\theta_n/\theta_m \geqq Q_{n-1}/Q_{m-1} = L(\mathfrak{a}_n)/L(\mathfrak{a}_m) \tag{6.1}$$

and

$$\theta_n/\theta_m = \prod_{i=m}^{n-1} \theta_g^{(i)} \geqq 1.$$

Thus $d(\mathfrak{a}_n, \mathfrak{a}_m) \geqq 0$ and

$$\theta_n/\theta_m \geqq \sqrt{L(\mathfrak{a}_n)/L(\mathfrak{a}_m)}, \tag{6.2}$$

with equality only when $n = m$. From (4.9) we also see that when $n - m$ is large, we would expect that

$$d(\mathfrak{a}_n, \mathfrak{a}_m) \approx \prec(n - m). \tag{6.3}$$

Note that distance is only defined for two reduced ideals in the same class.

If $p$ is defined as in (5.7), we also have $d(\mathfrak{a}_{p+1}, \mathfrak{a}_1) = \log(\theta_{p+1}) = \log \varepsilon_0 = R$, the regulator of $\mathscr{K}$. If $k = n + tp$, then, from (5.7), we derive the result

$$d(\mathfrak{a}_k, \mathfrak{a}_m) = d(\mathfrak{a}_n, \mathfrak{a}_m) + tR$$

and $\mathfrak{a}_k = \mathfrak{a}_n$, from (5.6). Thus, we need only consider those distances which are reduced modulo $R$. Under this convention we may assume that

$$d(\mathfrak{a}_n, \mathfrak{a}_m) < R. \tag{6.4}$$

Further, since $R < \sqrt{\Delta} \log \Delta$ (see, for example, [3, p. 329]), we have an upper bound of $\sqrt{\Delta} \log \Delta$ on $d(\mathfrak{a}_n, \mathfrak{a}_m)$.

Suppose that $\mathfrak{c} = \mathfrak{c}_1$ is any primitive ideal and suppose further that $\mathfrak{c}_k$ is a reduced ideal and that $\mathfrak{c}_{k-1}$ is not reduced. We have

$$(L(\mathfrak{c}_1)\rho_k)\mathfrak{c}_k = (L(\mathfrak{c}_k))\mathfrak{c}_1, \tag{6.5}$$

where, by (5.5), we have $1 < L(\mathfrak{c}_1)\rho_k \leqq L(\mathfrak{c}_1)$. If $\mathfrak{a}_1 = (1)$ and $\mathfrak{b}_1$ is any reduced ideal, let $\mathfrak{c}_1$ be the primitive ideal found by multiplication of $\mathfrak{a}_n$ and $\mathfrak{b}_m$. Then

$$(s)\mathfrak{c}_1 = \mathfrak{a}_n\mathfrak{b}_m \quad (s \in \mathbf{Z}). \tag{6.6}$$

We have minima $\theta_n$ and $\phi_m$ in the lattices corresponding to $\mathfrak{a}_1$ and $\mathfrak{b}_1$, respectively, such that

$$(L(\mathfrak{a}_1)\theta_n)\mathfrak{a}_n = (L(\mathfrak{a}_n))\mathfrak{a}_1 \tag{6.7}$$

and

$$(L(\mathfrak{b}_1)\phi_m)\mathfrak{b}_m = (L(\mathfrak{b}_m))\mathfrak{b}_1. \tag{6.8}$$

By combining (6.5), (6.6), (6.7), and (6.8) we get

$$(\psi L(\mathfrak{b}_1))\,\mathfrak{c}_k = (L(\mathfrak{c}_k))\mathfrak{b}_1,$$

where

$$\psi = (sL(\mathfrak{c}_1)\rho_k\theta_n\phi_m)/L(\mathfrak{a}_n)L(\mathfrak{a}_m) = \rho_k\mathfrak{a}_n\mathfrak{a}_m/s > 0,$$

by (5.5). Since $\mathfrak{b}_1$ is reduced and $|\psi'| < 1$, we must have $\psi > 1$. Since

$\mathfrak{c}_k \sim \mathfrak{b}_1$ and $\mathfrak{c}_k$ is reduced, we must also have $\mathfrak{c}_k = \mathfrak{b}_t$, for some $t \geqq 1$, $\phi_t = \phi$, and

$$(\phi_t L(b_1))\mathfrak{b}_t = (L(\mathfrak{b}_t))\mathfrak{b}_1.$$

Thus,

$$d(\mathfrak{b}_t, \mathfrak{b}_1) = d(\mathfrak{b}_m, \mathfrak{b}_1) + d(\mathfrak{a}_n, \mathfrak{a}_1) + \eta, \tag{6.9}$$

where $\eta = \log(\rho_k/s)$. Also, since $s \leqq \min(L(\mathfrak{a}_n), L(\mathfrak{b}_m)) < \sqrt{\Delta}$, by Theorem 5.2, we have

$$-\log \Delta < \eta < 0. \tag{6.10}$$

By (4.8) we see that $\eta$ will be small when compared to $d_1 = d(\mathfrak{a}_m, \mathfrak{b}_1)$ and $d_2 = d(\mathfrak{a}_n, \mathfrak{a}_1)$, when $n$ and $m$ are large. The process of multiplying the two ideals $\mathfrak{a}_n$ and $\mathfrak{b}_m$ and then reducing the resulting ideal gives us an ideal $\mathfrak{b}_t$, with $d(\mathfrak{b}_t, \mathfrak{b}_1) \approx d_1 + d_2$.

Now, if $\mathfrak{a} = [L(\mathfrak{a}), b + \omega]$, we easily find that $\mathfrak{a}' = [L(\mathfrak{a}), b + \omega']$. Further, we may assume the existence of $\lambda \in \mathfrak{a}$ such that $\lambda > L(\mathfrak{a})$, $-L(\mathfrak{a}) < \lambda' < 0$ and $\mathfrak{a} = [L(\mathfrak{a}), \lambda]$. Putting $\chi = -\lambda + [\lambda/L(\mathfrak{a})]L(\mathfrak{a})$, we have $\mathfrak{a} = [L(\mathfrak{a}), \chi]$ and $\mathfrak{a}' = [L(\mathfrak{a}), \chi']$. But since $\chi' > L(\mathfrak{a})$ and $-L(\mathfrak{a}) < \chi < 0$, it follows that $\mathfrak{a}'$ is also reduced.

If $\mathfrak{a}_1$ is an ideal such that $\mathfrak{a}_1 = \mathfrak{a}_1'$ (for example, $\mathfrak{a}_1 = (1)$), we say that $\mathfrak{a}_1$ is ambiguous. (This definition applies only in the case $\mathscr{K} = \mathbf{Q}(\sqrt{D})$.) Suppose that $\mathfrak{a}_1$ is a reduced ambiguous ideal. Let $1 < n \leqq p$ and $(\theta_n L(\mathfrak{a}_1))\mathfrak{a}_n = (L(\mathfrak{a}_n))\mathfrak{a}_1$. Since $\mathfrak{a}_n'$ is also a reduced ideal, we must have $\mathfrak{a}_n' = \mathfrak{a}_m$ for some $m \leqq p$. Thus, $(\theta_m L(\mathfrak{a}_1))\mathfrak{a}_m = (L(\mathfrak{a}_m))\mathfrak{a}_1$. Since $L(\mathfrak{a}_m) = L(\mathfrak{a}_n') = L(\mathfrak{a}_n)$ and $\mathfrak{a}_1 = \mathfrak{a}_1'$, we get

$$(\theta_n \theta_m L(\mathfrak{a}_1)) = (L(\mathfrak{a}_n)). \tag{6.11}$$

From (6.2), we have $1 < \theta_n \sqrt{L(\mathfrak{a}_1)/L(\mathfrak{a}_n)} < \varepsilon_0$ and $1 \leqq \theta_m \sqrt{L(\mathfrak{a}_1)/L(\mathfrak{a}_m)} < \varepsilon_0$. Thus, $1 < \theta_n \theta_m L(\mathfrak{a}_1)/L(\mathfrak{a}_n) < \varepsilon_0^2$ and, from (6.11), we get $\varepsilon_0 = \theta_n \theta_m L(\mathfrak{a}_1)/L(\mathfrak{a}_n)$. It follows that

$$d(\mathfrak{a}_n', \mathfrak{a}_1) = R - d(\mathfrak{a}_n, \mathfrak{a}_1) + \log(L(\mathfrak{a}_n)/L(\mathfrak{a}_1)). \tag{6.12}$$

If we combine (6.9) and (6.12), we see that if $(s)\mathfrak{c}_1 = \mathfrak{a}_n' \mathfrak{b}_m$, and $(L(\mathfrak{c}_1)\rho_k)\mathfrak{b}_t = (L(\mathfrak{b}_t))\mathfrak{c}_1$, then

$$d(\mathfrak{b}_t, \mathfrak{b}_1) = R + d(\mathfrak{b}_m, \mathfrak{b}_1) - d(\mathfrak{a}_n, \mathfrak{a}_1) + \eta,$$

where

$$(-3/2)\log \Delta < \eta = \log(\rho_k L(\mathfrak{a}_n)/s) \leqq (1/2)\log \Delta. \tag{6.13}$$

Thus, if $d(\mathfrak{b}_m, \mathfrak{b}_1) > d(\mathfrak{a}_n, \mathfrak{a}_1) + (3/2)\log \Delta$, we get

$$d(\mathfrak{b}_t, \mathfrak{b}_1) = d(\mathfrak{b}_m, \mathfrak{b}_1) - d(\mathfrak{a}_n, \mathfrak{a}_1) + \eta. \tag{6.14}$$

We also point out that, in order to find $\mathfrak{b}_t$, we require only $O(\log L(\mathfrak{c}_1)) = O(\log \Delta)$ steps.

The ideas and formulas introduced above can be used to solve a number of problems which arise in performing arithmetic in $\mathscr{K}$. Consider the problem of determining whether or not a given ideal $\mathfrak{b}$ is principal. One method of doing this would be to simply find a reduced ideal $\mathfrak{b}_m \sim \mathfrak{b}$ and then compare $\mathfrak{b}_m$ to $\mathfrak{a}_1 = (1), \mathfrak{a}_2, \mathfrak{a}_3, \ldots, \mathfrak{a}_p$. If $\mathfrak{b}_m$ is equal to one of these, then $\mathfrak{b}$ is a principal ideal; if not, then $\mathfrak{b}$ is non-principal. The difficulty with this approach is that for large values of $D$, $p$ can be quite large and this process will be rather time consuming. For example, if $D = 300272328240091$, then $p = 65344634$. It certainly appears (see Willams [21]) that we often have $p > \Delta^{1/2}$. Thus, $O(\Delta^{(1/2)+\varepsilon})$ steps could be required to execute this algorithm.

Here is another algorithm for doing this.

1) Calculate and store the bases of $\mathfrak{a}_1 = (1), \mathfrak{a}_2, \mathfrak{a}_3, \ldots \mathfrak{a}_s, \mathfrak{a}_{s+1}, \ldots, \mathfrak{a}_t$. Here $s$ and $t$ are determined by $d(\mathfrak{a}_s, \mathfrak{a}_1) \approx R^{1/2}$ and

$$d(\mathfrak{a}_t, \mathfrak{a}_1) > (3/2)\log \Delta + d(\mathfrak{a}_s, \mathfrak{a}_1). \tag{6.15}$$

Put $i = 1$, $\mathfrak{c}_1 = \mathfrak{b}_m$, where $\mathfrak{b}_m$ is a reduced ideal equivalent to $\mathfrak{b}$. Sort the ideals above on the values of $L(\mathfrak{a}_j)$.

2) If $\mathfrak{c}_i = \mathfrak{a}_j (1 \leqq j \leqq t)$, then we are done and $\mathfrak{b}$ is principal. (This part of the algorithm is most expeditiously achieved by first searching in the sorted list of $L(\mathfrak{a}_j)$'s above for those which have $L(\mathfrak{c}_i) = L(\mathfrak{a}_j)$.) Otherwise, put $\mathfrak{c}_{i+1}$ equal to the reduced ideal (as found by our continued fraction algorithm) equivalent to $\mathfrak{c}_i\mathfrak{a}_s'$.

3) Replace the value of $i$ by that of $i + 1$ and check that

$$i < R/(d(\mathfrak{a}_s, \mathfrak{a}_1) - (1/2)\log \Delta). \tag{6.16}$$

If this is so, go back to step 2; otherwise, $\mathfrak{b}$ is not principal.

To show why this algorithm works we first mention that $\mathfrak{b} \sim \mathfrak{c}_i$ ($i = 1, 2, 3, \ldots$). Suppose $\mathfrak{b}$ is principal. If $\mathfrak{c}_i \neq \mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3, \ldots, \mathfrak{a}_t$, then

$$d(\mathfrak{c}_k, \mathfrak{a}_1) > d(\mathfrak{a}_s, \mathfrak{a}_1) + (3/2)\log\Delta \quad (k = 1, 2, 3, \ldots, i).$$

Hence, from (6.13) and (6.14),

$$d(\mathfrak{c}_{k+1}, \mathfrak{a}_1) = d(\mathfrak{c}_k, \mathfrak{a}_1) - d(\mathfrak{a}_s, \mathfrak{a}_1) + \eta_k,$$

where $k \leqq i$ and $(-3/2)\log \Delta < \eta_k < (1/2)\log \Delta$. It follows that

$$d(\mathfrak{c}_{i+1}, \mathfrak{a}_1) = d(\mathfrak{b}_m, \mathfrak{a}_1) - i\, d(\mathfrak{a}_s, \mathfrak{a}_1) + \sum_{k=1}^{i} \eta_k. \tag{6.17}$$

Now, since $d(\mathfrak{b}_m, \mathfrak{b}_1) < R$, we must have

$$0 \leqq d(\mathfrak{c}_{i+1}, \mathfrak{a}_1) < R - i\, d(\mathfrak{a}_s, \mathfrak{a}_1) + (i \log \Delta)/2$$

or

$$i \leqq R/(d(\mathfrak{a}_s, \mathfrak{a}_1) - (1/2)\log \Delta) \approx R^{1/2} < \Delta^{(1/4)+\varepsilon}.$$

Thus, we see that our algorithm solves the problem in $O(\Delta^{(1/4)+\varepsilon})$ steps, an improvement over the previous algorithm. If $R$ were not known in advance, we could use the bound $\Delta^{1/2} \log \Delta$ instead. We shall see below, however, that a variant of this algorithm can also be used to compute $R$.

If, further, we wished to find the value of $d(\mathfrak{b}_m, \mathfrak{a}_1)$ above, we see that, for some $i$, we would have $\mathfrak{c}_i = \mathfrak{a}_k$, for some $k \leqq t$. If the values of $d(\mathfrak{a}_j, \mathfrak{a}_i)$ $(j = 1, 2, 3, \ldots, t)$ were computed and stored along with the bases of the $\mathfrak{a}_j$'s, then we would have

$$d(\mathfrak{b}_m, \mathfrak{a}_1) = d(\mathfrak{a}_k, \mathfrak{a}_1) + (i - 1)d(\mathfrak{a}_s, \mathfrak{a}_1) + \sum_{j=1}^{i-1} \eta_j \tag{6.18}$$

from (6.17). Thus, if the values of the $\eta_j$'s were all computed by using (6.13) as we go along, we could easily calculate $d(\mathfrak{b}_m, \mathfrak{a}_1)$. Notice that if we began with $\mathfrak{b}_m = \mathfrak{a}_2'$ and found $d(\mathfrak{a}_2', \mathfrak{a}_1)$ by this procedure, then, from (6.12), we would get

$$R = d(\mathfrak{a}_2', \mathfrak{a}_1) + d(\mathfrak{a}_2, \mathfrak{a}_1) + \log L(\mathfrak{a}_2).$$

Hence, this algorithm provides an $O(\Delta^{(1/4)+\varepsilon})$ method of computing $R$. Actually, if certain generalized Riemann Hypotheses hold, it is possible to develop an $O(\Delta^{(1/5)+\varepsilon})$ algorithm for finding $R$ and the class number $h$ of $\mathscr{K}$. The means by which this can be done is explained in **[12]**, **[5]** and **[11]**.

From (6.18), we also see that it would be possible to find $\phi_m = \exp\{d(\mathfrak{b}_m, \mathfrak{a}_1)\}$ such that $(\phi_m)\mathfrak{b}_m = (L)\mathfrak{b}_m)$, when $\mathfrak{b}_m$ is principal. Since $\mathfrak{b}_m = (\phi_m')$, this algorithm would provide a method of finding a single generator of any principal ideal. If $h = 1$ and $\alpha, \beta \in \mathscr{O}_{\mathscr{K}}$, then we can find the $\gcd(\alpha, \beta)$ by simply determining a basis of $\mathfrak{a} = (\alpha, \beta)$ and then finding a generator of the principal ideal $\mathfrak{a}$.

Since two ideals $\mathfrak{a}$ and $\mathfrak{b}$ of $\mathscr{O}_{\mathscr{K}}$ are in the same ideal class if and only if $\mathfrak{a}\mathfrak{b}' \sim (1)$, we can use our algorithm as a means of determining whether or not two ideals belong in the same ideal class. Given the value of $h$, we can now develop a $O(\Delta^{(1/4)+\varepsilon})$ algorithm for finding the structure of the class group of $\mathscr{K}$. A method for doing this was first described by Shanks **[12]** and has been more fully discussed by Solderitsh **[17]**, Lenstra **[5]**, and Schoof **[11]**. Again, in order to show that these methods are of order $\Delta^{(1/4)+\varepsilon}$, we must assume some generalized Riemann Hypotheses.

**7. Factoring.** We have already seen a number of applications of the results developed in the previous sections. In this section we show how these ideas can also aid in solving the problem of factoring a composite rational

integer $D$. We first require several results concerning ambiguous ideals in $\mathcal{K} = \mathbf{Q}(\sqrt{D})$. Many of these results go back to Gauss but they are included here for the sake of completeness.

LEMMA 7.1. *If $\mathfrak{a}$ is a primitive ambiguous ideal, then $\mathfrak{a} | (\sqrt{\Delta})$.*

PROOF. Let $\mathfrak{a} = [L(\mathfrak{a}), b + \omega]$. Since $\mathfrak{a}' = [L(\mathfrak{a}), b + \omega']$ and $\mathfrak{a} = \mathfrak{a}'$, we must have $\omega - \omega' \in \mathfrak{a}$; thus, $\omega - \omega' \equiv 0 \pmod{\mathfrak{a}}$ and $\mathfrak{a} | (\sqrt{\Delta})$.

LEMMA 7.2. *Let $\mathfrak{a}$ be a primitive ambiguous ideal. If $L(\mathfrak{a}) < \sqrt{\Delta}$, then $\mathfrak{a}$ is either reduced or $4 | \Delta$ and $\sqrt{\Delta}/2 \in \mathfrak{a}$.*

PROOF. Suppose $\mathfrak{a} = [L(\mathfrak{a}), b + \omega]$ is not reduced. There must exist $\alpha \in \mathfrak{a}$ such that $\alpha \neq 0$, $|\alpha| < L(\mathfrak{a})$, $|\alpha'| < L(\mathfrak{a})$. If $\alpha = xL(\mathfrak{a}) + y(b + \omega)$ $(x, y \in \mathbf{Z})$, we find that

$$|2xL(\mathfrak{a}) + y(2b + \omega + \omega')| < 2L(\mathfrak{a}). \tag{7.1}$$

Now, by Lemmas 7.1 and 6.1, $L(\mathfrak{a}) | \Delta$ and $L(\mathfrak{a}) | N(b + \omega)$. Also,

$$4N(b + \omega) = (2b + \omega + \omega')^2 - \Delta; \tag{7.2}$$

thus, $L(\mathfrak{a}) | 2b + \omega + \omega'$ and, from (7.1), we get

$$2xL(\mathfrak{a}) + y(2b + \omega + \omega') = \eta\, L(\mathfrak{a}), \tag{7.3}$$

where $\eta = 0, 1$, or $-1$. Hence, $2\alpha = \eta\, L(\mathfrak{a}) + y(\omega - \omega')$. Since $|\alpha|$, $|\alpha'| < L(\mathfrak{a})$, we get $L(\mathfrak{a}) + |y|(\omega - \omega') < 2L(\mathfrak{a})$ when $\eta \neq 0$. In this case, then, $L(\mathfrak{a}) > |y|(\omega - \omega') \geqq \sqrt{\Delta}$, a contradiction. If $\eta = 0$, then $\alpha = y(\omega - \omega')/2$. If $\omega + \omega' = 1$, we have $2 | y$ from (7.2) and $|\alpha| \geqq \sqrt{\Delta} > L(\mathfrak{a})$, which is also a contradiction. If $\omega + \omega' = 0$, and $|y| = 1$, then $4 | \Delta$ and $\sqrt{\Delta}/2 = (\omega - \omega')/2 \in \mathfrak{a}$.

THEOREM 7.3. *If $\mathfrak{a}$ is a primitive ambiguous ideal, there exists a reduced ambiguous ideal $\mathfrak{b}$ such that $\mathfrak{b} \sim \mathfrak{a}$.*

PROOF. If $4 | \Delta$ and $\sqrt{\Delta}/2 \in \mathfrak{a}$, put $\beta = \sqrt{\Delta}/2$; otherwise, put $\beta = \sqrt{\Delta}$. If $L(\mathfrak{a}) < \beta$ we see from Theorem 5.3 and Lemma 7.2 that $\mathfrak{a}$ is already reduced. Suppose $L(\mathfrak{a}) > \beta$. Since $\beta \in \mathfrak{a}$, there must exist an ideal $\mathfrak{b}$ such that $\mathfrak{a}\mathfrak{b} = (\beta)$, Since $\beta' = -\beta$, we see that $|N(\beta)| = \beta^2$ and $L(\mathfrak{b}) < \beta$. Further, since $\mathfrak{a} = \mathfrak{a}'$, we have $\mathfrak{b} = \mathfrak{b}'$; hence, $\mathfrak{b}$ is reduced, $(L(\mathfrak{a}))\mathfrak{b} = (\beta)$ $\mathfrak{a}$ and $\mathfrak{b} \sim \mathfrak{a}$.

If $4 | \Delta$, let $\mathfrak{r} = [2, k + \omega]$, where $k \equiv D \pmod 2$, be the prime ideal such that $\mathfrak{r}^2 = (2)$.

THEOREM 7.4. *If $\mathfrak{a}$ is a reduced ambiguous ideal and $\mathfrak{a} \neq (1), \mathfrak{r}$, then $L(\mathfrak{a})$ or $L(\mathfrak{a})/2$ is a nontrivial factor of $D$.*

PROOF. From the previous results we have $L(\mathfrak{a}) | \Delta$ and $L(\mathfrak{a}) < \sqrt{\Delta}$.

Thus, if $L(\mathfrak{a}) \neq 1$ (i.e., $\mathfrak{a} \neq (1)$), then $L(\mathfrak{a})$ is a nontrivial factor of $\Delta$. If $L(\mathfrak{a})$ is odd, then $L(\mathfrak{a})$ is a nontrivial factor of $D$. Since $\mathfrak{a}^2 = (L(\mathfrak{a}))$, we see that if $2|L(\mathfrak{a})$, then $4|\Delta$. Now, if $4|L(\mathfrak{a})$, we get (2) $|\mathfrak{a}$ which is not possible; thus, if $L(\mathfrak{a})/2 \neq 1$ ($\mathfrak{a} \neq \mathfrak{r}$), then $L(\mathfrak{a})/2$ is a nontrivial factor of $D$.

Thus, if we can find a reduced ambiguous ideal of $\mathcal{O}_{\mathscr{K}}$, we can very likely find a factor of $D$. In the next set of results we develop one method of attempting to find such an ideal.

THEOREM 7.5. *If* $\mathfrak{b}$ *is an ideal such that* $\mathfrak{b}^2 = \mathfrak{a} = (\alpha)$, *where* $N(\alpha) > 0$, *then there exists an ambiguous ideal* $\mathfrak{c}$ *such that* $\mathfrak{c} \sim \mathfrak{b}$.

PROOF. Since $N(\alpha) > 0$, we get $L(\mathfrak{b})^2 = N(\alpha)$. If we put $\beta = L(\mathfrak{b}) + \alpha'$, then

$$\beta'\alpha' = L(b)\alpha' + N(\alpha) = L(\mathfrak{b})\beta. \tag{7.4}$$

Now, since $\mathfrak{b}^2 = (\alpha)$, we have $(L(\mathfrak{b}))\mathfrak{b}' = (\alpha')\mathfrak{b}$ and $(\beta L(\mathfrak{b}))\mathfrak{b}' = (\alpha'\beta)\mathfrak{b}$. From (7.4), we find that if $\mathfrak{c} = (\beta)\mathfrak{b}$, then $\mathfrak{c} = \mathfrak{c}'$.

LEMMA 7.6. *Let* $\mathfrak{a}$ *be a primitive principal ideal of* $\mathcal{O}_{\mathscr{K}}$ *such that* gcd $(L(\mathfrak{a}), D) = 1$. *If* $L(\mathfrak{a}) = t^2 (t \in \mathbf{Z})$, *then there exists an ideal* $\mathfrak{b}$ *such that* $\mathfrak{a} = \mathfrak{b}^2$.

PROOF. If $\mathfrak{a} = [L(\mathfrak{a}), b + \omega]$, put $\mathfrak{b} = [|t|, b + \omega]$. Since $L(\mathfrak{a})|N(b + \omega)$ and $t|L(\mathfrak{a})$, we see that $\mathfrak{b}$ is an ideal of $\mathcal{O}_{\mathscr{K}}$. If $2|t$ and $\omega + \omega' = 0$, we have $\Delta = 4D$ and $(2)|\mathfrak{a}$, a contradiction; thus, it follows from (7.2), that $(t, 2b + \omega + \omega') = 1$. Let $x, y \in \mathbf{Z}$ such that $x|t| + y(2b + \omega + \omega') = 1$. Putting $c = x|t|b + y(b^2 - \omega\omega')$, we have $c \equiv b \pmod{L(\mathfrak{a})}$. Thus, $b + \omega \in \mathfrak{b}^2$ and $\mathfrak{a} = \mathfrak{b}^2$.

From our developments here we can see that one method of attempting to factor $D$ would be to search for an ideal $\mathfrak{a} = (\alpha)$ such that $L(\mathfrak{a})$ is a perfect square and $N(\alpha) > 0$. We could then find a reduced ambiguous ideal such that $\mathfrak{b} \sim \mathfrak{a}$. If $L(\mathfrak{b}) \neq 1, 2$ we would have a nontrivial factor of $D$.

Shanks [16] has developed a method of factoring, called SQUFOF, which utilizes this idea. His algorithm can be very simply stated as follows:

1) In the regular continued fraction expansion of $\phi_0 = \omega$, search for an odd value of $m$ and a $Q_{m-1}$ such that $Q_{m-1}/r = t^2$ $(t \in \mathbf{Z})$.

2) Compute the regular continued fraction of $\tilde{\phi}_0 = (P_m + \sqrt{D})/r|t| = (\tilde{P}_0 + \sqrt{D})/\tilde{Q}_0$ until we find $\tilde{P}_k = \tilde{P}_{k-1}$. Then $\tilde{Q}_{k-1}/r$ or $\tilde{Q}_{k-1}/2r$ is a factor of $D$.

We now explain why this algorithm works. We first remark that $\mathfrak{a}_n = [Q_{n-1}/r, (P_{n-1} - \sqrt{D}/r]$ is reduced, as $\mathfrak{a}_1 = [1, \omega]$ is. We have

$$(\theta_m)\mathfrak{a}_m = (L(\mathfrak{a}_m)) \quad (L(\mathfrak{a}_1) = 1) \tag{7.5}$$

and $N(\theta_m) > 0$, by (4.3). Thus, $\mathfrak{a}'_m = (\theta_m)$ and $L(\mathfrak{a}'_m) = t^2$. If $\mathfrak{c} = [|t|,$

$(P_{m-1} - \sqrt{D})/r]$, then $\mathfrak{c}' = [|t|, (P_m - \sqrt{D})/r]$, and $\mathfrak{c}^2 = \mathfrak{a}_m$. Now $L(\mathfrak{c}) = \sqrt{L(\mathfrak{a}_m)}$ and $\mathfrak{a}_m$ is reduced; thus, $L(\mathfrak{c}) < \sqrt[4]{\Delta} < \sqrt{\Delta}/2$ and $\mathfrak{c}$ is reduced. If $\mathfrak{b}_1 = \mathfrak{c}'$, then $\mathfrak{g}_1$ is reduced and

$$\mathfrak{b}_1^2 = \mathfrak{a}_m'. \tag{7.6}$$

By Theorems 7.5 and 7.3, there must exist a reduced ambiguous ideal $\mathfrak{b}$ such that $\mathfrak{b} \sim \mathfrak{b}_1$. Now $\mathfrak{b}_s = [\tilde{Q}_{s-1}/r, (\tilde{P}_{s-1} - \sqrt{D})/r] = [\tilde{Q}_{s-1}/r, (\tilde{P}_s + \sqrt{D})/r]$. If $\tilde{P}_s = \tilde{P}_{s-1}$, we have $\mathfrak{b}_s = \mathfrak{b}_s'$. Also, by (4.7),

$$\tilde{\theta}_g^{(s)} = (\tilde{P}_s + \sqrt{D})/\tilde{Q}_{s-1} > 1 \text{ and } -1 < \tilde{\theta}_g^{(s)\prime} < 0.$$

Futher,

$$\tilde{\phi}_{s-1} = (\tilde{P}_{s-1} + \sqrt{D})/\tilde{Q}_{s-1} > 1 \text{ and } -1 < \tilde{\phi}_{s-1}' < 0.$$

It follows that if $\mathfrak{b}_s = \mathfrak{b}_s'$, then $\tilde{\theta}_g^{(s)} = \tilde{\phi}_{s-1}$; for, we can not have two distinct minima adjacent to 1 in the lattice which corresponds to $\mathfrak{b}_s$. Thus $\tilde{P}_s = \tilde{P}_{s-1}$ if and only if $\mathfrak{b}_s = \mathfrak{b}_s'$.

If we define $\tilde{\theta}_k$ by $(L(\mathfrak{b}_1)\tilde{\theta}_k)\mathfrak{b}_k = (L(\mathfrak{b}_k))\mathfrak{b}_1$, we have $(L(\mathfrak{b}_k))\mathfrak{a}_m' = (L(\mathfrak{a}_m)\tilde{\theta}_k^2)$, from (7.5), and the results $\mathfrak{b}_k^2 = \mathfrak{b}_k\mathfrak{b}_k' = (L(\mathfrak{b}_k), L(\mathfrak{b}_1)^2 = L(\mathfrak{a}_m)$. If $\tilde{\theta}_k^2 L(\mathfrak{a}_m)/L(\mathfrak{b}_k) < 1$, then $\tilde{\theta}_k'^2 L(\mathfrak{a}_m)/L(\mathfrak{b}_k) < 1$. Since $\tilde{\theta}_k^2 L(\mathfrak{a}_m)/L(\mathfrak{b}_k) \in \mathfrak{a}_m$, a reduced ideal, this can not be; hence, $\tilde{\theta}_2^k L(\mathfrak{a}_m)/L(\mathfrak{b}_k) > 1$, $\theta_m = \tilde{\theta}_k^2 L(\mathfrak{a}_m)/L(\mathfrak{b}_k)$, and $d(\mathfrak{b}_k, \mathfrak{b}_1) = (d(\mathfrak{a}_m, \mathfrak{a}_1)/2) + \eta$, where $\eta = (1/2)\log(L(\mathfrak{b}_k)/L(\mathfrak{a}_m))$. Since $|\eta| < (1/4)\log \Delta$, we would expect, in view of (4.9), that $k \approx m/2$. Thus, in step (2) of SQUFOF, we need only go roughly half the distance in the continued fraction expansion of $\tilde{\phi}_0$ that we did in the continued fraction expansion of $\phi_0$.

It might occur that the factor $L(\mathfrak{b}_k)$ or $L(\mathfrak{b}_k)/2$ is trivial. Shanks has a way of avoiding this possibility by saving, as he proceeds through the continued fraction expansion of $\phi_0$, those values of $t$ that would lead to a trivial factorization. If $Q_{m-1}/r = t^2$ for any of these saved values of $t$, the algorithm just continues on to find another square $Q/r$ value. We can do this by noting that $\mathfrak{b}_k\mathfrak{b}_1'$ is principal, primitive, and $L(\mathfrak{b}_k\mathfrak{b}_1') < \sqrt{\Delta}/2$, when $\mathfrak{b}_k = (1)$ or $\mathfrak{r}$. Thus, $\mathfrak{a}_s = \mathfrak{b}_k\mathfrak{b}_1'$, for some $s$. Since

$$\mathfrak{a}_s^2 = (L(\mathfrak{b}_k))\mathfrak{b}_1'^2 = (L(\mathfrak{b}_k))\mathfrak{a}_m,$$

we find $\theta_m = \theta_s^2/L(\mathfrak{b}_k)$ and

$$d(\mathfrak{a}_s, \mathfrak{a}_1) = d(\mathfrak{a}_m, \mathfrak{a}_1)/2 + (\log L(\mathfrak{b}_k))/2 < d(\mathfrak{a}_m, \mathfrak{a}_1).$$

Now

$$L(\mathfrak{a}_m) = L(\mathfrak{a}_s)^2/L(\mathfrak{b}_k)^2 < \sqrt{\Delta};$$

hence, if we save those values of $t$ such that $t = Q_s/r$ for some $s$ and

$$t^2 < \begin{cases} \sqrt{\Delta}, & t \text{ odd} \\ 4\sqrt{\Delta}, & t \text{ even} \end{cases},$$

then we cannot get a trivial factorization if $Q_{m-1}/r$ does not equal any of these stored values of $t^2$.

It can also occur that the period length $p$ is too small to admit any useful $Q/r$ values. In this case one can replace $D$ by a small multiple of $D$ and try again. This algorithm would seem (see Monier [6]) to factor $D$ in $0(D^{(1/4)+\epsilon})$ operations. Note that, by (4.6), each of the numbers produced as this algorithm executes occupies about half of the storage space needed by $D$.

It might be argued that we have assumed that our $D$ here must be square-free. However, if, instead of using ideals of $\mathcal{O}_{\mathcal{K}}$ we use ideals of the integral domain $\mathcal{J}_n = [1, n\omega]$, the above theory, with minor modifications, will still go through. The only difference is that we use $n\omega$ instead of $\omega$ and $n^2\Delta$ instead of $\Delta$. Thus, if $D = f^2 d$, where $d$ is square-free, then we need only work with ideals in $\mathcal{J}_f$. That is, we still have $\omega = (r - 1 + \sqrt{D})/r$ and $\Delta = 4D/r^2$. In fact, we can work in $\mathcal{J}_{rf}$; in which case $\Delta = 4D$ and $\omega = \sqrt{D}$. If we do this, then we can assume that $r = 1$ in the SQUFOF algorithm given above. Also, we can assume that $r = 1$ in the description of the Morrison-Brillhartalgorithm given below.

Another application of these ideas can be made to the well-known factoring algorithm of Morrison and Brillhart [7], now commonly referred to as CFRAC. In this algorithm we expand $\phi_0 = \omega$ into a regular continued fraction and trial divide each of the $Q_i$ values by each prime in a set called the factor base $FB$. We usually select $FB = \{q | q \text{ prime}, (D/q) = 1, q < B\}$, where $B$ is some preselected factor bound. We attempt to find a set $Q = \{Q_{s_j - 1} | j = 1, 2, 3, \ldots, t\}$ such that, by using the primes of $FB$, we can completely factor each of the $Q_{s_j-1}$ values and

$$\prod_{j=1}^{t} (-1)^{s_j - 1} Q_{s_j - 1}/r = L^2 \quad (L \in \mathbf{Z}). \tag{7.7}$$

From (4.2) and (4.5), we know that if $G_{n-2} \equiv rA_{n-2} - (r - 1) B_{n-2} \pmod{D}$, then

$$G_{n-2}^2 \equiv (-1)^{n-1} r Q_{n-1} \pmod{D};$$

thus $M^2 \equiv N^2 \pmod{D}$, where

$$N = r^t L \text{ and } M \equiv \prod_{j=1}^{t} G_{s_j - 2} \pmod{D}.$$

If we calculate $F = \gcd(M - N, D)$ we often find that $F$ is a non-trivial factor of $D$. Pomerance [9] has shown that under reasonable heuristic assumptions we could expect to factor $D$ by this method in about

$\exp(\sqrt{2 \log D \log\log D})$ operations. This technique is one of the most powerful factoring routines currently known. Pomerance and Wagstaff [10] have used it to factor numbers of up to 54 digits.

One problem that develops in using this routine is the evaluation of the $G_{n-2}$ values and the storage of these for which $Q_{n-1}/r$ factors completely over $FB$. Shanks has pointed out that we can simply evaluate (and store) the appropriate $P_{n-1}$ values. By (4.6), these numbers require about half the storage space needed by the $G_{n-2}$ values and, since they have to be computed to obtain the $Q_{n-1}$ values, the cost of their evaluation is essentially free.

We now describe a version of Shanks' idea. If $\mathfrak{a} = \prod_{j=1}^{t} \mathfrak{a}_{s_j}$ and $(k)\mathfrak{b} = \mathfrak{a}$, where $k \in \mathbf{Z}$ and $\mathfrak{b}$ is primitive, then $L(\mathfrak{b}) = (L/k)^2$. Now, $\mathfrak{b}$ is principal and $(k)\mathfrak{b} = (\beta)$, where $\beta = \prod_{j=1}^{t} \theta'_{s_j}$. Since $N(\beta) = L^2$, we have $\mathfrak{b} = (\alpha)$, where $N(\alpha) > 0$. Since we know the values of $P_{s_j-1}$, $Q_{s_j-1}$ and we also have the complete factorization of $Q_{s_j-1}$, we can easily determine the prime ideal decomposition of $\mathfrak{a}_{s_j}$. This allows us, by using the multiplication and reduction routines, to find a reduced ideal $\mathfrak{d}$ such that $\mathfrak{d} \sim \mathfrak{c}$ and $\mathfrak{c}^2 = \mathfrak{b}$. Since $\mathfrak{a}$ is principal, we let $\mathfrak{a}_m \sim \mathfrak{a}$, where, by (6.9), we have

$$d(\mathfrak{a}_m, \mathfrak{a}_1) = \sum_{j=1}^{t} d(\mathfrak{a}_{s_j}, \mathfrak{a}_1) + \eta. \tag{7.8}$$

Here $\eta$ is likely to be small compared to $\sum_{j=1}^{t} d(\mathfrak{a}_{s_j}, \mathfrak{a}_1)$ and $d(\mathfrak{d}, \mathfrak{a}) \approx d(\mathfrak{a}_m, \mathfrak{a}_1)/2$. From (4.9) we also get $d(\mathfrak{a}_m, \mathfrak{a}_1) \approx \sum_{j=1}^{t} s_j$. If we put $u \approx (1/2) \sum_{j=1}^{t} s_j$, we can very quickly find an ideal $\mathfrak{a}_v$ where $d(\mathfrak{a}_v, \mathfrak{a}_1) \approx d(\mathfrak{a}_u, \mathfrak{a}_1)$. We simply observe from (4.9) that $d(\mathfrak{a}_{h+i}, \mathfrak{a}_i) \approx d(\mathfrak{a}_h, \mathfrak{a}_1) + d(\mathfrak{a}_i, \mathfrak{a}_1)$; thus, by using (6.9), we see that we can find $\mathfrak{a}_v$ in about $O(\log v)$ multiplication and reduction steps. We then have $d(\mathfrak{a}_v, \mathfrak{a}_1) \approx d(\mathfrak{a}_m, \mathfrak{a}_1)/2 \approx d(\mathfrak{d}, \mathfrak{a}_1)$.

Let $\mathfrak{g}_1$ be a reduced ideal equivalent to $\mathfrak{g} = \mathfrak{d}'\mathfrak{a}_v$. We note that $\mathfrak{g}^2 = (\mathfrak{d}')^2\mathfrak{a}_v^2 = (\lambda)$, where $N(\lambda) > 0$. Thus, there must exist a $\mathfrak{g}_n$ such that $\mathfrak{g}_n = \mathfrak{g}'_n$ and this will produce a factor of $D$. Further, by (6.12) and (6.14), we have

$$d(\mathfrak{g}_n, \mathfrak{g}_1) \text{ or } d(\mathfrak{g}'_n, \mathfrak{g}_1) \approx |\, d(\mathfrak{d}, \mathfrak{a}_1) - d(\mathfrak{a}_v, \mathfrak{a}_1)|,$$

which is small. Hence, after finding $\mathfrak{d}$ and $\mathfrak{a}_v$, we should not have much work to do to find $\mathfrak{g}_n$. We simply use both $\mathfrak{g}_1$ and $\mathfrak{g}'_1$ and develop two continued fractions until we find that $\mathfrak{g}_n = \mathfrak{g}'_n$ for one of them. Since all that is done here is multiplication and reduction, only the values of the $P$'s and $Q$'s are required. Also, as noted by Shanks, knowledge of the prime ideal factorization of the $\mathfrak{a}_{s_j}$'s often allows us to abort this process before we would find a trivial factor of $D$.

When Shanks first discovered this idea, the problem of generating and storing the $G_n$ values was not considered to be much of a bottleneck in the

running of CFRAC, as only sequential machines were being used and 90% of the machine time was spent in the trial division of the $Q$ values. Now, however, with the proposed use of highly parallel machines, it might be advisable to implement these ideas. Incidentally, it was through these investigations that Shanks discovered SQUFOF.

**8. The Voronoi continued fraction.** We will now deal with the problem of finding the reduced ideals in the complex cubic field $\mathscr{K} = \mathbf{Q}(\delta)$. As we have seen in §3, this is equivalent to the problem of finding the chain of minima (3.5) in a reduced lattice $\mathscr{L} = \mathscr{R}$ with basis $\{1, \mu, \nu\}$. As in the case with $\mathscr{L} = \mathscr{S}$, this can be done when we know how to find $\theta_g$, the minimum adjacent to 1, in any reduced lattice $\mathscr{R}$. From Theorem 4.1, we saw that this is an easy problem when $\mathscr{L} = \mathscr{S}$; however, when $\mathscr{L} = \mathscr{R}$, the problem is somewhat more difficult. It was solved by Voronoi [**19**] in 1896. In what follows, we will give an algorithm for finding $\theta_g$ which is similar to one given by Voronoi. For a complete discussion and proof of this algorithm we refer the reader to Williams, Cormack and Seah [**20**].

Let $\alpha \in \mathscr{R}$. We define a special projection of $\alpha$ called the *puncture* $P(\alpha)$ to be the 2-vector $(\xi_\alpha, \eta_\alpha)$, where $\xi_\alpha = (2\alpha - \alpha' - \alpha'')/2$, $\eta_\alpha = \mathrm{Im}(\alpha)$. We also define $\zeta_\alpha = \mathrm{Re}(\alpha)$. We note that $\alpha = \zeta_\alpha + \xi_\alpha$, $\xi_{\alpha+\beta} = \xi_\alpha + \xi_\beta$, $\eta_{\alpha+\beta} = \eta_\alpha + \eta_\beta$, $\zeta_{\alpha+\beta} = \zeta_\alpha + \zeta_\beta$, and, if $\beta = a + \alpha (a \in \mathbf{Z})$, then $P(\beta) = P(\alpha)$, $\zeta_\beta = a + \zeta_\alpha$. Also, $P(-\alpha) = -P(\alpha)$. Hence, the set of all punctures formed from all the elements of $\mathscr{R}$ forms a lattice $\mathscr{L}^{(p)}$ (in the more general sense mentioned at the beginning of §3) with basis $\{P(\mu), P(\nu)\}$. If $\mathscr{R}$ is a reduced lattice and $P(\mu) = (\xi_\mu, \eta_\mu)$, $P(\nu) = (\zeta_\nu, \eta_\nu)$, then Voronoi [**19**, §30] showed that

$$E_r = |\xi_\mu \eta_\nu - \xi_\nu \eta_\mu| > \sqrt{3}/2. \tag{8.1}$$

In [**20**] it is shown that there exist $\phi, \psi \in \mathscr{R}$ such that $\{P(\phi), P(\psi)\}$ is a basis of $\mathscr{L}^{(p)}$ and

$$\xi_\phi > \xi_\psi > 0; \quad \eta_\phi \eta_\psi < 0, \quad |\eta_\psi| > |\eta_\phi|,$$
$$|\eta_\psi| > \sqrt{3}/4, \quad |\eta_\phi| < 1 - \sqrt{3}/4, \quad 2|\eta_\psi| > 1 - |\eta_\phi|.$$

Further, such a pair $(\phi, \psi)$ can be found by using a continued fraction algorithm in $\mathscr{L}^{(p)}$ as described in [**2**] or [**20**] and it is easy to show that this procedure will terminate in $0(\log L(\alpha))$ operations. Actually, there exist $\phi, \psi \in \mathscr{R}$ such that $\xi_\phi > \xi_\psi > 0$, $\eta_\phi \eta_\psi < 0$, $|\eta_\psi| < 1/2$, $|\eta_\phi| > 1/2$, but these may be difficult for a computer to find because of precision problems encountered when attempting to store irrational numbers in a computer; hence, the more relaxed conditions given above are preferable for computational purposes. In [**20**] the following theorem is proved.

THEOREM 8.1. *If $\theta_g$ is the minimum adjacent to* 1 *in a reduced lattice $\mathscr{R}$, then $P(\theta_g)$ must be one of $P(\phi)$, $P(\psi)$, $P(\phi - \psi)$, $P(\phi + \psi)$, $P(2\phi + \psi)$.*

Thus, once $\phi$ and $\psi$ have been found, there are only a few choices for $P(\theta_g)$. We need only find that $\theta$ such that $P(\theta)$ is one of these choices $|\theta'| < 1$ and $\theta(> 0)$ is least. Then $\theta_g = \theta$. Since

$$|\alpha'|^2 = \eta_\alpha^2 + \zeta_\alpha^2, \tag{8.2}$$

we must have $|\zeta_\phi| < 1$; hence, $\theta$ must be $a + \beta$ where $\beta \in \{\phi, \psi, \phi - \psi, \phi + \psi, 2\phi + \psi\}$ and $a = [-\zeta_\beta]$ or $[-\zeta_\beta] + 1$. It is therefore necessary to find the least $\theta$ of these 10 possibilities for which $|\theta'| < 1$.

If $\mathscr{R}_1 = \mathscr{R}$ is reduced, then the chain (3.5) can be constructed by the repetition of the above process. By using methods developed in Williams and Dueck [**23**], it is possible to show that if $\mathscr{R}_i$ is any reduced lattice, then

$$\theta_g^{(i)}\theta_g^{(i+1)}\theta_g^{(i+2)}\theta_g^{(i+3)}\theta_g^{(i+4)} > 2.$$

Indeed, if these methods are refined somewhat, it is possible to show that

$$\theta_g^{(i)}\theta_g^{(i+1)}\theta_g^{(i+2)}\theta_g^{(i+3)} > 2.$$

This is the best result possible, however, as there are many examples where

$$\theta_g^{(i)}\theta_g^{(i+1)}\theta_g^{(i+2)} < 2.$$

Thus, we have

$$\theta_n = \prod_{i=1}^{n-1} \theta_g^{(i)} > 2^{\lfloor (n-1)/4 \rfloor}, \tag{8.3}$$

a result analogous to (4.8). While we do not at the moment have a rule like Levy's law concerning the Voronoi Continued Fraction, it seems from empirical evidence that $\log \theta_n \approx vn$ where $1.12 < v < 1.13$.

If $\varepsilon_0$ $(> 1)$ is the fundamental unit of $\mathscr{K}$ and $\mathscr{R}_1$ is the lattice that corresponds to the ideal $\mathfrak{a}_1$ of $\mathscr{O}_\mathscr{K}$, then $\varepsilon_0$ is a minimum of $\mathscr{R}_1$ and $\theta_{p+1} = \varepsilon_0$ for some $p$. Also $\mathfrak{a}_{p+t} = \mathfrak{a}_t$ $(t \geqq 1)$. Thus, this algorithm can be used to find $\varepsilon_0$. Several years ago Ray Steiner observed that Voronoi's algorithm for finding $\varepsilon_0$ is very robust in the sense that, if occasional errors are made in the selection for $\theta_g^{(n)}$ in $\mathscr{R}_n$, the algorithm will still find $\varepsilon_0$ as long as these erroneous values for $\theta_g^{(n)}$ can be embedded together with 1 in a basis of $\mathscr{R}_n$. The reason this phenomenon occurs for the algorithm given here is contained in the next theorem, a proof of which is given in [**22**] (Theorem 7.7).

THEOREM 8.2. *If $\mathscr{R}$ has* 1 *as a basis element but $\mathscr{R}$ is not reduced, then there exists $\rho_g \in \mathscr{R}$ and $\alpha \in \mathscr{R}$ such that $0 < \rho_g < 1$, $|\rho_g'| < 1$, $\{1, \rho_g, \alpha\}$ is a basis of $\mathscr{R}$, and $P(\rho_g)$ is one of $P(\phi)$, $P(\psi)$, $P(\phi - \psi)$, $P(\phi + \psi)$, $P(2\phi + \psi)$.*

In view of the remarks made in §3, Voronoi's algorithm can also be used to find $\rho_k \in \mathscr{R}_1$ and a reduced lattice $\mathscr{R}_k$ such that $\rho_k \mathscr{R}_k = \mathscr{R}_1$. Hence, Voronoi's algorithm is completely analogous to the continued fraction (4.1) above. The reason that this explains Steiner's observation is that if the $\theta_g^{(n)}$ selected for $\mathscr{R}_n$ is not correct, then $\mathscr{R}_{n+1}$ is not a reduced lattice. Since Voronoi's algorithm will, however, find $\rho^* \in \mathscr{R}_{n+1}$ and $\mathscr{R}_{n+1}^*$ such that $\rho^* \mathscr{R}_{n+1}^* = \mathscr{R}_{n+1}$ and $\mathscr{R}_{n+1}^*$ is reduced, we see that the algorithm will correct itself, provided the errors in evaluating $\theta_g^{(n)}$ are not too frequent.

In the next section we will need some results concerning elements of $\mathscr{R}$ and their punctures. We first define what we mean by $\omega^*$ for any $\omega \in \mathscr{R}$. If $P(\omega) = (\xi_\omega, \eta_\omega)$ is the puncture of $\omega$, let $\omega^*$ be that element of $\mathscr{R}$ such that $P(\omega^*) = P(\omega)$, $|\omega^{*\prime}| < 1$, and $|\omega^*|$ is minimal. We point out here that if $|\eta_\omega| > 1$, then $\omega^*$ can not exist by (8.2). Since there must be some $a \in \mathbf{Z}$ such that $|\zeta_\omega - a| \leqq 1/2$, we find that if $|\eta_\omega| < \sqrt{3}/2$, then $\omega^*$ must exist. The next two lemmas given here are proved in **[22]** as Lemmas 7.2 and 7.4, respectively.

LEMMA 8.3. *If* $\omega \in \mathscr{R}$, $|\omega'| < 1$ *and* $|\omega| < 1$, *then* $\xi_\omega < 1 + \sqrt{1 - \eta_\omega^2} < 2$.

LEMMA 8.4. *If* $\omega \in \mathscr{R}$, $\omega^*$ *exists and* $|\xi_\omega| < \sqrt{1 - \eta_\omega^2}$, *then* $|\omega^*| < 1$.

LEMMA 8.5. *Let* $\omega \in \mathscr{R}$ *and let* $\beta_\omega = 1 - \sqrt{1 - \eta_\omega^2}$. *If* $\omega^*$ *exists*, $1/2 < |\omega^*| < 1$ *and* $0 < \xi_\omega < |\omega|^*$, *then* $|\zeta_{\omega^*}| < \beta_\omega$.

PROOF. Certainly, by (8.2), we have $|\zeta_{\omega^*}| < 1$. Suppose $|\zeta_{\omega^*}| > \beta_\omega$, and consider the following two cases.

*Case* 1. $\omega^* > 0$. If $\zeta_{\omega^*} < 0$, then $|\zeta_{\omega^*}| = -\zeta_{\omega^*} > \beta_\omega$ and $\omega^* = |\omega^*| = \zeta_\omega^* + \xi_\omega < \xi_\mu - \beta_\omega$, which is not possible. If $\zeta_{\omega^*} > 0$, then $\beta_\omega < \zeta_{\omega^*} < 1$ and $(1 - \zeta_\omega^*)^2 + \eta_\omega^2 < 1$; thus, if $\chi = \omega^* - 1$, then $|\chi'| < 1$ and $|\chi| < |\omega^*|$.

*Case* 2. $\omega^* < 0$. If $\zeta_{\omega^*} > 0$, then $\omega^* = \zeta_{\omega^*} + \xi_\omega < 0$ and we get $\zeta_\omega < 0$, which is impossible; thus $|\zeta_{\omega^*}| = -\zeta_{\omega^*} > \beta_\omega$ and $-\zeta_{\omega^*} < 1$. It follows that $(1 + \zeta_{\omega^*})^2 + \eta_\omega^2 < 1$ and, if $\chi = \omega^* + 1$, we have $|\chi'| < 1$, $|\chi| < |\omega^*|$.

In both cases we produce a $\chi \in \mathscr{R}$ such that $P(\chi) = P(\omega^*)$, $|\chi'| < 1$, $|\chi| < \omega^*$. This contradicts the definition of $\omega^*$. If $|\zeta_{\omega^*}| = \beta_\omega$, then $|\chi'| = 1$ and this means that $\chi = \pm 1$, which is also not possible.

In order to get some idea of how rapidly Voronoi's algorithm will find a reduced ideal equivalent to a given primitive ideal of $\mathscr{K}$, we will need the following theorem. We first define the set $B \subset \mathbf{Z}^2$ as

$$B = \{(0, 1), (0, 2), (1, 0), (2, 0), (1, -1), (2, -1), (3, -1), (1, 1), (2, 2), (1, 2), (1, 3), (2, 3), (2, 4), (2, 1), (3, 1), (3, 2), (4, 1), (4, 2), (4, 3)\}.$$

THEOREM 8.6. *Suppose $\mathscr{R}$ is not reduced and $\rho_g$ is that element of $\mathscr{R}$ such that $|\rho_g'| < 1$, $P(\rho_g)$ is one of $P(\phi)$, $P(\psi)$, $P(\phi - \psi)$, $P(\phi + \psi)$, $P(2\phi + \psi)$, and $|\rho_g|$ is least. If $|\rho_g| > 2/3$, and $\omega(\neq 0) \in \mathscr{R}$ is such that $|\omega| < 1$, $|\omega'| < 1$, then $\pm P(\omega) = aP(\phi) + bP(\psi)$, where $(a, b) \in B$.*

PROOF. Since $-\omega \in \mathscr{R}$ and $|-\omega'| = |\omega'|$, we will only consider those values of $\omega$ such that $\xi_\omega > 0$. Since $P(\omega) \in \mathscr{L}^{(p)}$, we have $P(\omega) = aP(\phi) + bP(\psi)$, where $(a, b) \in \mathbf{Z}^2$. Now, if $a > 0$, we must have $b > 0$ or else $\xi_\omega < 0$. Since $|\eta_\omega| = |a|\,|\eta_\phi| + b\,|\eta_\psi| > 1$, for $b \geqq 2$, we can only have $b = 1$. In this case, however, $\xi_\omega < 0$; thus, we must have $a \geqq 0$. If $a = 0$, then $1 > |\eta_\omega| = |b|\,|\eta_\psi|$ and $|b| \leqq 2$. Since $\xi_\omega > 0$, we can only have $b = 1$ or 2.

If $b = 0$, then since $\xi_\omega < 2$, by Lemma 8.3, we have $\xi_\phi < 2/3$ for $a \geqq 3$. Thus, since $\phi^*$ exists, we get $|\phi^*| > 2/3$, $|\xi_\phi| < |\phi^*|$, and $\xi_\phi^2 + \eta_\phi^2 < (2/3)^2 + (1 - \sqrt{3}/4)^2 < 1$; hence, $|\phi^*| < 1$ by Lemma 8.4. Since $|\phi^*| \leqq \xi_\phi + |\zeta_{\phi^*}|$, $|\eta_\phi| = |\eta_\omega|/a$, $a\xi_\phi = \xi_\omega < 1 + \sqrt{1 - \eta_\omega^2}$, by Lemma 8.3, and $|\zeta_{\phi^*}| < \beta_\phi$, by Lemma 8.5, we find that

$$\phi^* < ((1 + \sqrt{1 - a^2\eta_\phi^2})/a) + 1 - \sqrt{1 - \eta_\phi^2} \leqq 2/a \leqq 2/3,$$

a contradiction.

If $b \leqq -2$, then $|\eta_\omega| = a|\eta_\phi| + |b|\,|\eta_\psi| > |\eta_\phi| + 2|\eta_\psi| > 1$, which is not possible. If $b = -1$ and $a \geqq 4$, we have $\xi_\phi < 2/3$ again. Further, since $|\eta_\omega| < 1$, $|\eta_\psi| > \sqrt{3}/4$, and $|\eta_\omega| = a|\eta_\phi| = |\eta_\psi|$, we have $1 > |\eta_\omega| > a|\eta_\phi| + \sqrt{3}/4$. Thus, by using Lemma 8.3, 8.4 and 8.5 as before, we find that $|\phi^*| > 2/3$ and

$$\begin{aligned} |\phi^*| < \xi_\phi + \beta_\phi &< ((1 + \sqrt{1 - (a|\eta_\phi| + \sqrt{3}/4)^2})/(a - 1)) + 1 - \sqrt{1 - \eta_\phi^2} \\ &\leqq (\sqrt{1 - 3/16} + 1)/(a - 1) < 2/3, \end{aligned}$$

a contradiction.

Suppose $b \geqq a > 0$. If $d = b - a \geqq 0$, we have $1 > |\eta_\omega| = a|\eta_\phi + \eta_\psi| + d|\eta_\psi|$; thus, $d \leqq 2$. If $d = 0$, we can use the same reasoning as that used earlier with $\phi$ replaced by $\phi + \psi$ to show that $a = 1$ or 2 only. If $|\eta_\phi + \eta_\psi| > 1/2$, then $|\eta_\psi| > 1/2$; thus, $a + d < 2$, which can not be so for $a, b > 0$. If $|\eta_\phi + \eta_\psi| < 1/2$, then $\chi = (\phi + \psi)^*$ exists. If $a \geqq 3$, then $\xi_\chi < \xi_\omega/3 < 2/3$ and $|\eta_\chi| < 1/3$; hence, $|\chi| < 1$, by Lemma 8.4, and $|\chi| \geqq |\rho_g| > 2/3$. We also have $1 > |\eta_\omega| > a|\eta_\psi| + \sqrt{3}/4$; thus, by using reasoning similar to that used in the case of $b = 1$ and $a \geqq 4$, we will find that $|\chi| < 2/3$, which is, again, a contradiction.

We need only deal now with the case of $a > b \geqq 1$. Since $\xi_\phi < 2/a$, we have $\xi_\phi < 2/3$, for $a \geqq 3$ and $2/3 < |\phi^*| < 1$. We must, then, have $|\phi^*| \leqq \xi_\phi + |\zeta_\phi^*| < 2/a + 1 + \sqrt{1 - (1 - \sqrt{3}/4)^2}$. This is less than $2/3$ when $a \geqq 5$.

**9. Ideals in $\mathbf{Q}(\delta)$.** Let $\mathfrak{a}$ be any primitive ideal of $\mathcal{O}_{\mathcal{K}}$, where $\mathcal{K} = \mathbf{Q}(\delta)$. In [18], Voronoi showed that $\mathfrak{a} = [\alpha_1, \alpha_2, \alpha_3]$, where $\alpha_1 = P = L(\mathfrak{a})$, $\alpha_2 = P'(m + \delta)/\tau$, $\alpha_3 = P''(n + n'\delta + \delta^2)/\tau^2\sigma$, $0 < m < \tau P/P'$, $0 < n < \tau\sigma P'/P''$, $0 < n < \tau^2\sigma P/P''$. He also showed how the rational integers $\sigma, \tau, P, P', P'', m, n, n'$ could be computed. The values of $\sigma$ and $\tau$ are invariant for any fixed $\mathcal{K}$ and $\tau^6\sigma^2\Delta = \Delta_p$, where $\Delta_p$ is the discriminant of $p(x)$. Also, $\gcd(P', P'') = 1$, $P'P''|P$ and $N(\mathfrak{a}) = PP'P''$.

Now, if $\mathcal{R}$ is the lattice with basis $\{1, \mu, \nu\}$, where $\mu = \alpha_2/L(\mathfrak{a})$, $\nu = \alpha_3/L(\mathfrak{a})$, we have $E = P'P''\sqrt{|\Delta|}/2P^2\tau^3\sigma$. If $\mathfrak{a}$ is a reduced ideal, then $\mathcal{R}$ is a reduced lattice and, by (8.1), we get

$$L(\mathfrak{a})^3/N(\mathfrak{a}) = P^2/P'P'' < \sqrt{|\Delta|/3}. \tag{9.1}$$

It follows that, for a reduced ideal $\mathfrak{a}$, we must have

$$L(\mathfrak{a}) < \sqrt{|\Delta|/3}, \tag{9.2}$$

a result analogous to that of Theorem 5.2. This bound is actually very good. For example, if $\delta = \sqrt[3]{D}$, where $D = k^3 + 3k$ is square-free, it can be shown that if $\alpha_1 = 3k^3 - 3k^2 + 9k - 1$, $\alpha_2 = k^3 - 2k^2 + 5k + (k - 1)^2\delta + (k + 1)\delta^2$, $\alpha_3 = 2k^3 - 3k^2 - 4k + 1 + 2(k^2 + 1)\delta + (3 - k)\delta^2$, then $\mathfrak{a} = [\alpha_1, \alpha_2, \alpha_3]$ is a reduced ideal. In this case $L(\mathfrak{a}) = 3k^3 - 3k^2 + 9k - 1$ is quite close to the value $3(k^3 + 3k)$ of $\sqrt{|\Delta|/3}$.

We also have a result analogous to that of Theorem 5.3.

THEOREM 9.1. *If $\mathfrak{a}$ is a primitive ideal and $L(\mathfrak{a})^4 < \sqrt{|\Delta|/27}\, N(\mathfrak{a})$, then $\mathfrak{a}$ must be a reduced ideal.*

PROOF. Suppose $\mathfrak{a}$ is not a reduced ideal. There must exist some $\alpha \in \mathfrak{a}$ such that $\alpha \neq 0$, $0 < \alpha < L(\mathfrak{a})$ and $|\alpha'| < L(\mathfrak{a})$. If we put $\beta = \mathrm{Re}(\alpha')$, $\gamma = \mathrm{Im}(\alpha')$, we get

$$|\alpha - \alpha'|^2 + |\alpha' - \alpha''|^2 + |\alpha'' - \alpha|^2 = 2(\beta - \alpha)^2 + 6\gamma^2.$$

Now $|\alpha'|^2 = \beta^2 + \gamma^2 < L(\mathfrak{a})^2$; hence, $|\beta| < L(\mathfrak{a})$, $|\gamma| < L(\mathfrak{a})$. If $\beta > 0$, then $|\beta - \alpha| < L(\mathfrak{a})$ and $2(\beta - \alpha)^2 + 6\gamma^2 < 8\, L(\mathfrak{a})^2$. If $\beta < 0$, then $|\beta - \alpha| < L(\mathfrak{a}) - \beta$ and $\gamma^2 < L(\mathfrak{a})^2 - \beta^2$; thus,

$$2(\beta - \alpha)^2 + 6\gamma^2 < 8L(\mathfrak{a})^2 - 4L(\mathfrak{a})\beta - 4\beta^2 < 9L(\mathfrak{a})^2.$$

If $d(\alpha) = (\alpha - \alpha')^2(\alpha' - \alpha'')^2(\alpha'' - \alpha)^2$, then, since the geometric mean can not exceed the arithmetic mean, we have $|d(\alpha)| < (9L(\mathfrak{a})^2/3)^3 = 27L(\mathfrak{a})^6$. Since $\alpha^2 \in \mathfrak{a}$, we must have $L(\mathfrak{a})^2\, d(\alpha) = \Delta[\alpha_1, \alpha_2, \alpha_3]\, |X|^2$, where $\mathfrak{a} = [\alpha_1, \alpha_2, \alpha_3]$ and $X$ is a matrix with rational integer entries. If $d(\alpha) = 0$, then $\alpha$ must be a rational integer and $L(\mathfrak{a})|\alpha$, which is not possible; thus $|X|^2 \geqq 1$. Since $\Delta[\alpha_1, \alpha_2, \alpha_3] = N(\mathfrak{a})^2\Delta$, we get $L(\mathfrak{a})^4/N(\mathfrak{a}) > \sqrt{|\Delta|/27}$ when $\mathfrak{a}$ is not reduced, and our result follows.

If $\mathfrak{a}$ is any primitive ideal of $\mathcal{O}_{\mathcal{K}}$, we know, by Theorem 3.3, and its corollary that there exists $\lambda \in \mathfrak{a}$ such that $(\lambda)\mathfrak{b} = (L(\mathfrak{b}))\mathfrak{a}$ and $\mathfrak{b}$ is a reduced ideal. Further, $\lambda = L(\mathfrak{a})\rho_n$, where

$$\rho_n = \prod_{i=1}^{n-1} |\rho_g^{(i)}|,\ |\rho_g^{(i)}| < 1,\ |\rho_g^{(i)\prime}| < 1.$$

Indeed, by Theorem 8.6, our version of Voronoi's algorithm will find $\rho_g^{(i)}$ such that $|\rho_g^{(i)}| < 2/3$ as long as $i > 2|B| = 38$. Since $N(\mathfrak{a})|N(\lambda)$ and $|N(\lambda)| = |\lambda|\,|\lambda'|^2$, we also have

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

Hence,

$$1/L(\mathfrak{a}) < |\lambda| \leqq L(\mathfrak{a}),\ 1 < |\lambda'| \leqq L(\mathfrak{a}). \tag{9.3}$$

By (3.1), we have

$$(\rho_g^{(i)} L(\mathfrak{a}_i))\mathfrak{a}_{i+1} = (L(\mathfrak{a}_{i+1}))\,\mathfrak{a}_i, \quad (\mathfrak{a}_1 = \mathfrak{a}),$$

thus,

$$N(\rho_g^{(i)}) = L(\mathfrak{a}_{i+1})^3\, N(\mathfrak{a}_i)/N(\mathfrak{a}_{i+1})\, L(\mathfrak{a}_i)^3.$$

Since $|\rho_g^{(i)\prime}| < 1$, we have $L(\mathfrak{a}_{i+1})^3\, N(\mathfrak{a}_i)/N(\mathfrak{a}_{i+1})L(\mathfrak{a}_i)^3 < 2/3$ for $i \leqq n - 39$. Thus, if $n \geqq 39$, we get

$$N(\mathfrak{a}_1)\, L(\mathfrak{a}_{n-1})^3/N(\mathfrak{a}_{n-1})\, L(\mathfrak{a}_1)^3 < (2/3)^{n-39}.$$

Since we may assume that $\mathfrak{b} = \mathfrak{a}_n$ and $\mathfrak{a}_{n-1}$ is not reduced, we have $L(\mathfrak{a}_{n-1})^4/N(\mathfrak{a}_{n-1}) > \sqrt{|\Delta|/27}$, by Theorem 9.1. Since $L(\mathfrak{a}_{n-1}) < L(\mathfrak{a}_{n-1})^3/N(\mathfrak{a}_{n-1})$, it follows that $L(\mathfrak{a}_{n-1})^3/N(\mathfrak{a}_{n-1}) > \sqrt[4]{|\Delta|/27}$. Hence, the number of ideals $n$ that our algorithm must find before finding a reduced ideal $\mathfrak{a}_n$ satisfies the inequality

$$n < 39 + (\log (L(\mathfrak{a})^3/(N(\mathfrak{a})\sqrt[4]{|\Delta|/27}))/\log (3/2)), \tag{9.4}$$

a result analogous to (5.4).

If $\mathfrak{a} = [\alpha_1, \alpha_2, \alpha_3]$ and $\mathfrak{b} = [\beta_1, \beta_2, \beta_3]$ are any two ideals of $\mathcal{O}_{\mathcal{K}}$ then $\mathfrak{c} = \mathfrak{a}\mathfrak{b} = [\alpha_1\beta_1, \alpha_2\beta_1, \ldots, \alpha_3\beta_3]$. If we let $\lambda_1, \lambda_2, \lambda_3, \ldots, \lambda_9$ represent the values of $\alpha_1\beta_1, \alpha_2\beta_1, \ldots, \alpha_3\beta_3$, then our multiplication algorithm must find $\Lambda_1, \Lambda_2, \Lambda_3$ such that $\mathfrak{c} = [\Lambda_1, \Lambda_2, \Lambda_3]$. We may certainly assume that $\lambda_i = (a_i + b_i\delta + c_i\delta^2)/m$, where $m = \sigma^2\tau$ and $a_i, b_i, c_i \in \mathbf{Z}$ $(i = 1, 2, 3, \ldots, 9)$ can be easily computed. It is not difficult to show that if

$$\Lambda_1 = A_1/m,\ \Lambda_2 = (A_2 + B_2\delta)/m,\ \Lambda_3 = (A_3 + B_3\delta + C_3\delta^2)/m,$$
$$(A_1, A_2, B_2, A_3, B_3, C_3 \in \mathbf{Z}),$$

then $C_3 = \gcd(c_1, c_2, c_3, \ldots, c_9)$.

If

$$\sum_{i=1}^{9} x_i c_i = C_3 \quad (x_i \in \mathbf{Z}),$$

then

$$B_3 = \sum_{i=1}^{9} x_i b_i, \quad A_3 = \sum_{i=1}^{9} x_i a_i.$$

Also,

$$B_2 = \gcd\{(b_i - B_3 c_i/C_3) | i = 1, 2, 3, \ldots, 9\}.$$

If

$$\sum_{i=1}^{9} y_i(b_i - B_3 c_i/C_3) = B_2 \text{ and } \sum_{i=1}^{9} y_i c_i = 0, \ (y_i \in \mathbf{Z}),$$

then $A_2 = \sum_{i=1}^{9} y_i a_i$.
Finally,

$$A_1 = \gcd\{(a_i - A_2(b_i - B_3 c_i/C_3) - A_3 c_i/C_3) | i = 1, 2, 3, \ldots, 9\}.$$

By using the results given in [18], it is often possible to shorten this procedure; however, the details can be very tedious (see [22]). In principle, though, one sees that ideal multiplication can be accomplished by finding some gcd's and solving some linear Diophantine equations, a process requiring $O(\log(\sigma\tau^2 L(\mathfrak{a})L(\mathfrak{b})))$ operations. We can also compute a basis of $\mathfrak{a}'$ from that of $\mathfrak{a}$ in $O(\log(\sigma\tau^2 L(\mathfrak{a}))$ operations. (Note that if $\mathfrak{a}$ is primitive, we must have $L(\mathfrak{a}') = L(\mathfrak{a})$.) We point out here that if $\mathfrak{a}$ is reduced, it is not necessarily the case that $\mathfrak{a}'$ is reduced, the reason why the Voronoi algorithm, starting with $\mathfrak{a}_1 = (1)$, does not have the nice symmetry properties of the regular continued fraction expansion of $\omega$.

**10. Algorithms and some numerical results.** As we have seen, many of the results concerning $\mathbf{Q}(\sqrt{D})$ given in the first part of this paper have analogues in the $\mathbf{Q}(\delta)$ case. In fact, we can define for this latter case a distance, $d(\mathfrak{a}_m, \mathfrak{a}_n)$, just as we did for ideals in $\mathbf{Q}(\sqrt{D})$. That is, we define $d(\mathfrak{a}_m, \mathfrak{a}_n) = \log(\theta_n/\theta_m)$, when $n \geqq m$ and $\mathfrak{a}_1$ is reduced. With this definition and the results proved above we can derive several facts concerning $d(\mathfrak{a}_m, \mathfrak{a}_n)$. If $\mathfrak{a}_1 = (1)$, $\mathfrak{b}_1$ is a reduced ideal and $(s)\,\mathfrak{c}_1 = \mathfrak{a}_n \mathfrak{b}_m$, where $\mathfrak{c}_1$ is primitive and $s \in \mathbf{Z}$, then there exists some reduced $\mathfrak{c}_k \sim \mathfrak{c}_1$ and $\mathfrak{c}_k = \mathfrak{b}_t$. In fact, if $(L(\mathfrak{c}_1)\rho_k)\mathfrak{c}_k = (L(\mathfrak{c}_k))\mathfrak{c}_1$, then we can show, as was done in §6, that

$$d(\mathfrak{b}_t, \mathfrak{b}_1) = d(\mathfrak{b}_m, \mathfrak{b}_1) + d(\mathfrak{a}_n, \mathfrak{a}_1) + \eta, \tag{10.1}$$

where

$$\eta = \log\left(\frac{L(\mathfrak{a}_n\mathfrak{b}_m)\rho_k}{L(\mathfrak{a}_n)L(\mathfrak{b}_m)}\right).$$

By (9.3) and (9.2), we have $-2\log|\Delta/3| < \eta < 0$.

If $\mathfrak{a}_1$ is a reduced ideal such that $\mathfrak{a}_1 = \mathfrak{a}_1'$ (e.g., $\mathfrak{a}_1 = (1)$), let $1 \leqq n \leqq p$ $(\theta_n L(\mathfrak{a}_1))\mathfrak{a}_n = (L(\mathfrak{a}_n))\mathfrak{a}_1$ and $(\tau_j L(\mathfrak{b}_1))\mathfrak{b}_j = (L(\mathfrak{b}_j))\mathfrak{b}_1$, where $\mathfrak{b}_1 = \mathfrak{a}_n'$ and $\mathfrak{b}_j$ is reduced. Since $\mathfrak{b}_j \sim \mathfrak{b}_1 = \mathfrak{a}_n' \sim \mathfrak{a}_1' = \mathfrak{a}_1$, we must have $\mathfrak{b}_j = \mathfrak{a}_q$ for some $q$. We can also show that

$$d(\mathfrak{a}_q, \mathfrak{a}_1) = R - d(\mathfrak{a}_n, \mathfrak{a}_1) + \log\left(\frac{L(\mathfrak{a}_n)\tau_j}{L(\mathfrak{a}_1)}\right), \tag{10.2}$$

when this is positive. (From (9.3) and the fact that $L(\mathfrak{b}_1) = L(\mathfrak{a}_n)$, we see that the right hand side of (10.2) must be positive when $\mathfrak{a}_1 = (1)$; for, in this case $|\theta_q'\theta_n' L(\mathfrak{a}_1)/L(\mathfrak{a}_n)\ \tau_j'| < 1$.) Also,

$$-2\log\sqrt{|\Delta|3} < \log\left(\frac{L(\mathfrak{a}_n)\tau_j}{L(\mathfrak{a}_1)}\right) < \log\sqrt{|\Delta/3|}.$$

If $\mathfrak{a}_1 = (1)$, $\mathfrak{b}_1$ is a reduced ideal and $(s)$ $\mathfrak{c}_1 = \mathfrak{a}_q\mathfrak{b}_m$, where $\mathfrak{a}_q(\sim \mathfrak{a}_n')$ is as described above, then, by combining (9.1) and (9.2), we get

$$d(\mathfrak{b}_t, \mathfrak{b}_1) = R + d(\mathfrak{b}_m, \mathfrak{b}_1) - d(\mathfrak{a}_n, \mathfrak{a}_1) + \eta,$$

where $(L(\mathfrak{c}_1)\rho_k)\mathfrak{b}_t = (L(\mathfrak{b}_t))\mathfrak{c}_1$ and $\mathfrak{b}_t$ is reduced. Here

$$-3\log|\Delta/3| < \eta = \log\left(\frac{L(\mathfrak{a}_n\mathfrak{b}_m)\rho_k\tau_j}{L(\mathfrak{b}_m)}\right) < (1/2)\log|\Delta/3|.$$

Thus, if $d(\mathfrak{b}_m, \mathfrak{b}_1) > d(\mathfrak{a}_n, \mathfrak{a}_1) + 3\log|\Delta/3|$, we get

$$d(\mathfrak{b}_t, \mathfrak{b}_1) = d(\mathfrak{b}_m, \mathfrak{b}_1) - d(\mathfrak{a}_n, \mathfrak{a}_1) + \eta, \tag{10.3}$$

when $\mathfrak{b}_t \sim \mathfrak{b}_m\mathfrak{a}_n'$ and $\mathfrak{b}_t$ is computed in the manner described above using our version of Voronoi's algorithm.

With these results we see that the algorithm of §6 can be modified to solve the problem of determining when a given ideal $\mathfrak{b}$ in $\mathbf{Q}(\delta)$ is principal. We need only replace (6.15) by

$$d(\mathfrak{a}_t, \mathfrak{a}_1) > 3\log|\Delta/3| + d(\mathfrak{a}_s, \mathfrak{a}_1)$$

and (6.16) by

$$i < R/(d(\mathfrak{a}_s, \mathfrak{a}_1) - (1/2)\log|\Delta/3|).$$

Now Landau [4] has shown that $R = O(|\Delta|^{1/2+\varepsilon})$; hence, by (9.4) and (8.3) we see that once we find $\mathfrak{b}_m \sim \mathfrak{b}$ with $\mathfrak{b}_m$ reduced (a process requiring $O(\log L(\mathfrak{b}))$ steps by (9.4)), we require a further $O(|\Delta|^{(1/4)+\varepsilon})$ steps to solve the problem.

We can also, as was done in §6, develop algorithms for finding $R$ and $h$, the $\gcd(\alpha, \beta)$ when $h = 1$, $\alpha, \beta \in \mathcal{O}_{\mathcal{K}}$, and the class group structure of $\mathcal{K}$. Further, we can determine $R$ and $h$ in $O(|\Delta|^{(1/5)+\varepsilon})$ operations under generalized Riemann Hypotheses. For the complete details of finding $R$ by this technique when $\delta = \sqrt[3]{D}$ $(D \in \mathbf{Z})$, we refer the reader to the voluminous [22]. As an example, we mention that we were able, by means of this technique, to find that when $D = 2124689657$, we have $R = 6127255313.478815$ and $h = 1$. This result required only 15 minutes of computer time to calculate. Had Voronoi's continued fraction algorithm only been used to find $R$, it would have required about 80 days of time on the same machine. Somewhat whimsically we point out that if $\{x, y, z\} \neq \{1, 0, 0\}$ is any solution set of the Diophantine equation

$$x^3 + Dy^3 + D^2z^3 - 3Dxyz = 1, \tag{10.4}$$

for the above $D$, the value of $R$ here means that

$$\min\{|x|, |y|, |z|\} > 10^{10^9}.$$

A lower bound of this magnitude on the solutions of a Diophantine equation would ordinarily cause us to regard the equation as having no further solution. But, of course, we know that (10.4) has an infinitude of solutions.

We have also written a computer program which determines the class group $G$ for any pure cubic field. This was done by using the results developed here together with the ideas of [12], [17], and [11] as they apply to the $\mathbf{Q}(\delta)$ case. The only real difference in the techniques is in the computation of a stock of ideals from which to develop $G$. This was done by using the results of Voronoi [18] to find ideals $\mathfrak{a}$ with $L(\mathfrak{a})$ a prime. A method of finding cube roots modulo $L(\mathfrak{a})$ wad developed from the idea of Shanks [14]. With this program we were able to find the structure of all $G$ for each pure cubic field $\mathbf{Q}(\sqrt[3]{D})$ with $D < 30000$. This has allowed us to complete the table of 2-types of the class groups for all $D < 10000$ begun by Eisenbeis, Frey and Ommerborn [1]. (There were 39 cases that they could not compute by their methods.)

Let $G = C(n_1) \times C(n_2) \times \cdots \times C(n_k)$, where $C(n)$ is a cyclic group of order $n$, be the essentially unique canonical form of $G$; that is $n_i \mid n_j$ if $i > j$. We say that $r_m$ is the *m-rank* of $G$ if $m$ divides exactly $r_m$ of these numbers. Up to $D = 30000$ we have found that $r_p \leqq 1$ for all primes $p > 5$. We have only one example of $r_5 = 2$ and that occurs for $D = 10263$, where $G = C(90) \times C(5)$. The largest 2-rank found is 3 and the largest 3-rank found is 4. We found 27 values of $D$ for which the 9-rank is 2 and we found 24 values of $D$ for which the 4-rank is 2. We found no other values of $n$ for which $r_n \geqq 2$. We mention, in conclusion, that the

largest value of $h$ which we found is $h = 2412$, for $D = 28365$ and $G = C(804) \times C(3)$.

## References


**1.** H. Eisenbeis, G. Frey, B. Ommerborn, *Computation of the 2-rank of pure cubic fields*, Math. Comp. **32** (1968), 559–569.

**2.** B. N. Delone and D. K. Faddeev, *The Theory of Irrationalities of the Third Degree*, Amer. Math. Soc., Providence, R. I., 1964.

**3.** L. K. Hua, *Introduction to Number Theory*, Springer-Verlag, New York, 1982.

**4.** E. Landau, *Verallgemeinerungen eines polyaschen Sätzes auf algebraische Zahlkörper*, Nachr. Ges. Wiss. Göttingen (1918), 478–488.

**5.** H. W. Lenstra, Jr., *On the calculation of regulators and class numbers of quadratic fields*, Lond. Math. Soc. Lect. Note Ser. **56** (1982), 123–150.

**6.** L. Monier, *Algorithmes de factorisation d'entiers*, Thèse de 3$^{me}$ cycle, Orsay, 1980.

**7.** M. A. Morrison and J. Brillhart, *A method of factoring and the factorization of* $F_7$, Math. Comp. **29** (1975), 183–205.

**8.** O. Perron, *Die Lehre von den Kettenbrüchen*, Stuttgart 1977, Reprint Chelsea, N.Y.

**9.** C. Pomerance, *Analysis and comparison of some integer factoring algorithms*, Computational Methods in Number Theory (H. W. Lenstra Jr., and R. Tijdeman, eds.), Math. Centrum Tracts, Number 154, Part I, Amsterdam, 1983, pp. 89–139.

**10.** C. Pomerance and S. S. Wagstaff Jr., *Implementation of the continued fraction integer factoring algorithm*, Proc. 12th Winnipeg Conf. on Numerical Methods and Computing, (1982), to appear.

**11.** R. J. Schoof, *Quadratic Fields and Factorization, Computational Methods in Number Theory* (H. W. Lenstra, Jr., and R. Tijdeman, eds.), Math. Centrum Tracts, Number 155, Part II, Amsterdam, 1983, pp. 235–286.

**12.** D. Shanks, *Class number, a theory of factorization and genera*, Proc. Symp. Pure Math. 20 AMS (1971), 415–440.

**13.** ———, *The infrastructure of a real quadratic field and its applications*, Proc. 1972 Number Theory Conference, Boulder, (1972), 217–224.

**14.** ———, *Five number-theoretic algorithms*, Proceedings of the Second Manitoba Conference on Numerical Mathematics, Congressus Numerantium **7** (1972), 51–70.

**15.** ———, *A survey of quadratic, cubic and quartic algebraic number fields (from a computational point of view)*, Congressus Numerantium **17** (1976), 15–40.

**16.** ———, *A new factorization algorithm*, to appear.

**17.** J. T. Solderitsch, *Imaginary Quadratic Number Fields with Special Class Groups*, Ph.D. Thesis, Lehigh University, (1977).

**18.** G. F. Voronoi, *Concerning Algebraic Derivable from a Root of an Equation of the Third Degree*, Master's Thesis, St. Petersburg, (1894), (Russian).

**19.** ———, *On a Generalization of the Algorithm of Continued Fractions*, Doctoral Dissertation, Warsaw, (1896), (Russian).

**20.** H. C. Williams, G. Cormack and E. Seah, *Calculation of the regulator of a pure cubic field*, Math. Comp. **34** (1980), 567–611.

**21.** H. C. Williams, *A numerical investigation into the length of the period of the continued fraction of* $\sqrt{D}$, Math. Comp. **36** (1981), 593–601.

**22.** H. C. Williams, G. W. Dueck and B. K. Schmid, *A rapid method of evaluating the regulator and class number of a pure cubic field*, Math. Comp. **41** (1983), 235–286.

**23.** H. C. Williams and G. Dueck, *An Analogue of the Nearest Integer Continued Fraction for Certain Cubic Irrationalities*, Math. Comp. **42** (1984), 683–705.

DEPARTMENT OF COMPUTER SCIENCE, UNIVERSITY OF MANITOBA, WINNIPEG, MANITOBA
CANADA R3T 2N2