MATHEMATICS OF COMPUTATION
VOLUME 48, NUMBER 177
JANUARY 1987, PAGES 55-66

On Principal Ideal Testing in Totally Complex Quartic Fields and the Determination of Certain Cyclotomic Constants

By Johannes Buchmann* and H. C. Williams**

Dedicated to Daniel Shanks on the occasion of his 70th birthday

Abstract. Let $\mathscr{L}$ be any totally complex quartic field. Two algorithms are described for determining whether or not any given ideal in $\mathscr{L}$ is principal. One of these algorithms is very efficient in practice, but its complexity is difficult to analyze; the other algorithm is computationally more elaborate but, in this case, a complexity analysis can be provided.

These ideas are applied to the problem of determining the cyclotomic numbers of order 5 for a prime $p \equiv 1 \pmod 5$. Given any quadratic (or quintic) nonresidue of p, it is shown that these cyclotomic numbers can be efficiently computed in $O((\log p)^3)$ binary operations.

1. Introduction. In general, the question of whether an ideal in an algebraic number field $\mathscr{L}$ is principal seems to be very difficult to answer. Nevertheless, in order to solve several important problems concerning $\mathscr{L}$, for example the determination of the class group of $\mathscr{L}$, we must be able to answer this question. In the case when $\mathscr{L}$ is a real quadratic field, one can use the well-known continued fraction algorithm (see [3]) or a refinement of this idea due to Shanks [21] and extended by Lenstra [16] and Schoof [20] (see also Williams [25]). When $\mathscr{L}$ is a cubic field, the problem can be solved by using Voronoi's generalized continued fraction algorithm (see [7]). Williams [25] has shown that, in the case when $\mathscr{L}$ is a complex cubic field, this technique can be improved by extending Shanks' [21] idea. The Generalized Voronoi Algorithm (GVA) described by Buchmann [4] can be applied in all fields of unit rank 1 and 2.

For a general $\mathscr{L}$ we can employ the method due to Pohst and Zassenhaus [19]. Unfortunately, it is not yet known how efficient this method is. Other procedures, for example that of Billevich [2], do not appear to be computationally efficient. In fact, complexity results are known only for the quadratic and complex cubic fields, cf. Williams [25], Dueck and Williams [9].

In this paper we discuss the problem of principal ideal testing in totally complex quadratic fields. We derive an algorithm which makes use of the GVA, describe its implementation, and prove that its complexity is of the same order as that of the

Received March 13, 1986.

1980 *Mathematics Subject Classification.* Primary 12A30, 12C20.

*Research supported by a Feodor Lynen Research Fellowship of the Alexander von Humboldt Foundation.

**Research supported by NSERC of Canada Grant A7649.

0025-5718/87 $1.00 + $.25 per page

continued fraction and Voronoi method applied to real quadratic and complex cubic fields, respectively. Actually, we give two algorithms: one which is efficient in practice but for which we are unable to supply a complexity analysis, and one which is rather more elaborate but for which we can provide a complexity analysis.

As an application of our ideas, we show that in the cyclotomic field $\mathcal{Q}(\zeta)$, where ζ is a primitive fifth root of unity, we can find a generator for any prime ideal of norm p, where p is a rational prime and $p \equiv 1 \pmod 5$, in $O((\log p)^3)$ binary operations, provided that we know either a quadratic or quintic nonresidue of p. This means, in practice, that we have a very efficient method for determining a solution (x, u, v, w) of Dickson's [8] well-known Diophantine system

$$\begin{aligned} 16p &= x^2 + 50u^2 + 50v^2 + 125w^2, \\ xw &= v^2 - 4uv - u^2, \\ x &= 1 \pmod 5, \end{aligned} \tag{1.1}$$

even when p is very large. These numbers x, u, v, w are of great importance in cyclotomy when $e = (p-1)/f = 5$.

We intend, in a subsequent paper, to show that the ideas of Shanks [21] can also be used to improve our algorithm.

2. Notation and Preliminary Results. Let $\mathcal{L} = \mathcal{Q}(\rho)$ be a totally complex quartic field, where id, $\overline{\mathrm{id}}$, σ, $\bar{\sigma}$, are the $\mathcal{Q}$ isomorphisms of $\mathcal{L}$. We write $\mathcal{L}^{(1)} = \mathcal{L}$, $\mathcal{L}^{(2)} = \sigma(\mathcal{L})$, and for $\xi \in \mathcal{L}$, $\xi^{(1)} = \xi$, $\xi^{(2)} = \sigma(\xi)$, $\xi^{(3)} = \bar{\xi}$, $\xi^{(4)} = \overline{\sigma(\xi)}$. We denote the norm of $\xi^{(i)}$ by $N(\xi^{(i)})$ or $N_{\mathcal{L}^{(i)}/\mathcal{Q}}(\xi^{(i)}) = \xi^{(1)}\xi^{(2)}\xi^{(3)}\xi^{(4)}$ and the trace of ξ by

$$\mathrm{Tr}(\xi) = \xi^{(1)} + \xi^{(2)} + \xi^{(3)} + \xi^{(4)}.$$

Also, set

$$S(\xi) = \sum_{i>j} \xi^{(i)}\xi^{(j)}.$$

We will require the following simple results.

PROPOSITION 2.1. *Let* $\xi_1, \xi_2 \in \mathcal{L}$; *then* $|\xi_1| = |\xi_2|$ *if and only if* $|\sigma(\xi_1)| = |\sigma(\xi_2)|$.

Proof. Suppose $|\xi_1| = |\xi_2|$ and define $\eta = \xi_1/\xi_2$. We have $\eta\bar{\eta} = 1$, $\bar{\eta} = 1/\eta \in \mathcal{L}$, and $1 = \sigma(\eta\bar{\eta}) = \sigma(\eta)\sigma(\bar{\eta})$. Hence,

$$\sigma(\eta) = 1/\sigma(\bar{\eta}). \tag{2.1}$$

On the other hand, since $\eta\bar{\eta} = 1$, it follows that

$$r = N(\eta) = \sigma(\eta)\,\overline{\sigma(\eta)} \geqslant 0$$

and $r \in \mathcal{Q}$. By using (2.1) we see that

$$N(\sigma(\bar{\eta})) = N(\sigma(\eta))^{-1} = N(\eta)^{-1} = r^{-1} \quad \text{and} \quad \sigma(\bar{\eta})r = \overline{\sigma(\eta)}.$$

By taking the norm of both sides, we must have $r = 1$; hence, $|\sigma(\xi_1)| = |\sigma(\xi_2)|$. The second part of this result can be proved in a similar fashion. □

PROPOSITION 2.2. *If* $\xi \in \mathcal{L}$, *then* $\xi\bar{\xi} = 1$ *if and only if all of the following hold*:

(i) $N(\xi) = 1$,

(ii) $\mathrm{Tr}(\xi) = \mathrm{Tr}(\xi^{-1})$,

(iii) $\mathrm{Tr}(\xi)^2 \geqslant 4S(\xi) - 8$.

Proof. Let $P(x) = x^4 - ax^3 + bx^2 - cx + d$, $a, b, c, d \in \mathcal{Q}$, be the characteristic polynomial of ξ. We have $a = \mathrm{Tr}(\xi)$, $b = S(\xi)$, $c = N(\xi)\mathrm{Tr}(\xi^{-1})$, $d = N(\xi)$.

If $\xi\bar{\xi} = 1$ then by Proposition 2.1, $N(\xi) = 1$, $\xi^{-1} = \bar{\xi}$ and $\mathrm{Tr}(\xi^{-1}) = \mathrm{Tr}(\bar{\xi}) = \mathrm{Tr}(\xi)$. Also,

$$P(x) = g_1(x)g_2(x),$$

where $g_i(x) = x^2 + h_i x + 1$ $(i = 1, 2)$, $h_1 = \xi + \bar{\xi}$, $h_2 = \sigma(\xi) + \overline{\sigma(\xi)}$. It follows that, since $c = a$ and $d = 1$, we must have $h_1 h_2 = b - 2$ and $h_1 + h_2 = -a$. Since h_1 and h_2 are real, we must also have $a^2 > 4(b - 2)$.

If (i), (ii), (iii) hold, then $a = c$, $d = 1$, and $a^2 \geqslant 4(b - 2)$. Putting

$$h_1 = (-a + k)/2, \qquad h_2 = (-a - k)/2,$$

where $k^2 = a^2 - 4(b - 2)$, we have $P(x) = g_1(x)g_2(x)$, where $g_i(x)$ $(i = 1, 2)$ is defined above. With no loss of generality we may assume that $g_1(\xi) = 0$. Since h_1 is real, we must have $g_1(\bar{\xi}) = 0$ and $\xi\bar{\xi} = 1$. □

Let $\mathcal{O}_{\mathcal{L}}$ be the ring of algebraic integers in $\mathcal{L}$ and let $\{\omega_1, \omega_2, \omega_3, \omega_4\}$ be a $\mathbf{Z}$-basis of $\mathcal{O}_{\mathcal{L}}$. We also let $\{\omega_1^*, \omega_2^*, \omega_3^*, \omega_4^*\}$ be the dual basis of $\mathcal{O}_{\mathcal{L}}$ (see [2, pp. 403]); that is,

$$\mathrm{Tr}\left(\omega_i \omega_j^*\right) = \delta_{ij} \qquad (1 \leqslant i, j \leqslant 4).$$

Since $N(\omega_j) \geqslant 1$, we have

$$W = \max\left\{ \left|\omega_j^{(i)}\right| \middle| 1 \leqslant i, j \leqslant 4 \right\} \geqslant 1,$$

$$W^* = \max\left\{ \left|\omega_j^{*(i)}\right| \middle| i \leqslant i, j \leqslant 4 \right\} \geqslant 1.$$

Let D be the absolute value of the discriminant of $\mathcal{L}$. We may assume that

$$W \leqslant \sqrt{D}. \tag{2.2}$$

Such a basis can be computed by using the basis reduction algorithm of Lenstra, Lenstra, and Lovász [15] in the Minkowski lattice corresponding to $\mathcal{O}_{\mathcal{L}}$. It follows from (2.2) and the definition of W^* that

$$W^* \leqslant 6D. \tag{2.3}$$

Suppose $\mathfrak{b}$ is an ideal of $\mathcal{O}_{\mathcal{L}}$ and we wish to test whether or not $\mathfrak{b}$ is a principal ideal*** of $\mathcal{O}_{\mathcal{L}}$. Without loss of generality we will assume that $\mathfrak{b}$ is an integral ideal and that $\{\tilde{\beta}_1, \tilde{\beta}_2, \tilde{\beta}_3, \tilde{\beta}_4\}$ is a $\mathbf{Z}$-basis of $\mathfrak{b}$, where

$$\tilde{\beta}_j = \sum_{k=1}^{4} \tilde{b}_{kj}\omega_k. \tag{2.4}$$

We also use $N(\mathfrak{b})$ to denote the norm of the ideal $\mathfrak{b}$.

3. The Method. The method which we will employ here was developed in Buchmann [5]. We will now review the main ideas of this technique.

For any (fractional) ideal $\mathfrak{a}$ of $\mathcal{O}_{\mathcal{L}}$ we set

$$d(\mathfrak{a}) = \min\{d \in \mathbf{Z}^+ \mid d\mathfrak{a} \subseteq \mathcal{O}_{\mathcal{L}}\}$$

and

$$L(\mathfrak{a}) = \min\{k \in \mathbf{Z}^+ \mid k \in d(\mathfrak{a})\mathfrak{a}\}.$$

***We assume our ideals are nonzero ideals.

A number $\alpha \in \mathfrak{a}$ $(\alpha \neq 0)$ is called a *minimum* in $\mathfrak{a}$ if there is no $\alpha' \in \mathfrak{a}$ $(\alpha' \neq 0)$ with $|\alpha'^{(i)}| < |\alpha^{(i)}|$ for $i = 1$ and 2. An integral ideal $\mathfrak{a}$ in $\mathcal{O}_{\mathscr{L}}$ is called *reduced* if $\mathfrak{a}$ is primitive and $L(\mathfrak{a})$ is a minimum in $\mathfrak{a}$. The number of reduced ideals in $\mathcal{O}_{\mathscr{L}}$ is finite and every ideal class in $\mathcal{O}_{\mathscr{L}}$ contains at least one reduced ideal.

From these remarks we can derive the following procedure for testing whether or not $\mathfrak{b}$ is principal.

ALGORITHM 3.1.

1. Compute the cycle $\mathscr{I} = \{(\alpha_1), \ldots, (\alpha_p)\}$ of all reduced principal ideals in $\mathcal{O}_{\mathscr{L}}$. (It is often more convenient to compute these ideals by computing their **Z**-bases rather than their generators.)

2. Compute a reduced ideal $\mathfrak{b}' = (1/\beta)\mathfrak{b}$ in the ideal class $\mathfrak{b}$.

3. The ideal $\mathfrak{b}$ is principal if and only if $\mathfrak{b}' \in \mathscr{I}$, i.e., $\mathfrak{b} = (\beta\alpha_k)$ for some $k \in \{1, 2, \ldots, p\}$.

In order to carry out steps 2 and 3 we use the following results of [5]. Let $\mathfrak{a}$ be any integral ideal of $\mathcal{O}_{\mathscr{L}}$ and let μ be a minimum in $\mathfrak{a}$. Then $d\mu^{-1}\mathfrak{a}$ with $d = d(\mu^{-1}\mathfrak{a})$ is a reduced ideal equivalent to $\mathfrak{a}$. Moreover, if $\mathscr{C} = \{\mu_1, \mu_2, \ldots, \mu_k\}$ is a maximal system of pairwise nonassociated minima in $\mathfrak{a}$, then

$$\mathscr{I} = \left\{ d_i\mu_i^{-1}\mathfrak{a} \mid d_i = d\left(\mu_i^{-1}\mathfrak{a}\right), 1 \leqslant i \leqslant k \right\}$$

is a cycle of reduced ideals in the ideal class of $\mathfrak{a}$. $\mathscr{I}$ can be computed by using Algorithm 4.1 of [6].

Thus, it is now necessary to show how a minimum μ of $\mathfrak{b}$ can be computed.

4. Reduction of the Ideal $\mathfrak{b}$. Let $\{\tilde{\beta}_1, \tilde{\beta}_2, \tilde{\beta}_3, \tilde{\beta}_4\}$ be a **Z**-basis of $\mathfrak{b}$ and let $\tilde{B}$ be the matrix $(\tilde{b}_{kj})$, where the $\tilde{b}_{kj}$ $(1 \leqslant k, j \leqslant 4)$ are given in (2.4). If we apply the reduction algorithm of [15] to the columns of $\tilde{B}$, we obtain the so-called LLL-matrix $B = (b_{kj})$ of $\mathfrak{b}$. The numbers

$$\beta_j = \sum_{k=1} b_{kj}\omega_k \qquad (1 \leqslant j \leqslant 4)$$

form another **Z**-basis of $\mathfrak{b}$. Further, if we denote the columns of B by $\vec{b}_1, \ldots, \vec{b}_4$, then we can deduce from [6, Proposition 6.3] that

$$|\vec{b}_j| \leqslant c_1 D^{3/2} N(\mathfrak{b})^{1/4} \qquad (1 \leqslant j \leqslant 4), \tag{4.1}$$

where c_1 is a constant which is independent of $\mathscr{L}$. Indeed, from [15, (1.8)] we get

$$|\vec{b}_1| \leqslant 2N(\mathfrak{b})^{1/4}; \tag{4.2}$$

hence, by definition of W, we can derive

$$|\beta_1^{(i)}| \leqslant 4WN(\mathfrak{b})^{1/4} \qquad (1 \leqslant i \leqslant 2). \tag{4.3}$$

In many cases this β_1 is a minimum of $\mathfrak{b}$. If it is not, we search for a minimum μ such that $|\mu^{(i)}| < |\beta_1^{(i)}|$, $i = 1, 2$. Thus, having found β_1, our next problem is to find some minimum μ satisfying

$$|\mu^{(i)}| \leqslant |\beta_1^{(i)}| \qquad (1 \leqslant i \leqslant 2).$$

For $\vec{x} = (x_1, x_2, x_3, x_4)^t \in \mathbf{Z}^4$ and $1 \leqslant i \leqslant 2$, we set

$$\mu^{(i)}(\vec{x}) = \sum_{j=1}^{4} x_j\beta_j^{(i)} = \sum_{k=1}^{4} \left(\sum_{j=1}^{4} b_{kj}x_j \right) \omega_k^{(i)}. \tag{4.4}$$

We compute μ by using

ALGORITHM 4.1.

1. Initialize $\vec{x}_2 \leftarrow (1,0,0,0)^t$, $f \leftarrow 2$.

2. Try to find $\vec{x}_1 \in \mathbf{Z}^4$ ($\vec{x}_1 \neq \vec{0}$) such that

$$|\mu^{(i)}(\vec{x}_1)| < |\mu^{(i)}(\vec{x}_2)|/f \qquad (1 \leqslant i \leqslant 2). \tag{4.5}$$

If this search is successful, set

$\vec{x}_2 \leftarrow \vec{x}_1$;

else,

if $f = 2$, then set $f \leftarrow 1$; otherwise return $\mu = \mu^{(1)}(\vec{x}_2)$.

Because of Proposition 2.1, this algorithm must find a minimum of $\mathfrak{b}$.

Notice that for all $\vec{x} \in \mathbf{Z}^4$ with

$$|\mu^{(i)}(\vec{x})| \leqslant |\beta_1^{(i)}| \qquad (1 \leqslant i \leqslant 2), \tag{4.6}$$

we have

$$\left| \sum_{j=1}^{4} b_{kj} x_j \right| \leqslant 16WW^*N(\mathfrak{b})^{1/4} \qquad (1 \leqslant k \leqslant 4). \tag{4.7}$$

This can be easily seen by using the well-known dual basis argument [3, p. 403] and (4.3).

Now in order to carry out the comparisons in (4.5), we are compelled to use rational approximations $\hat{\omega}_k^{(i)}$ to $\omega_k^{(i)}$ for $1 \leqslant k, i \leqslant 4$. We must therefore discuss the question of how this is to be done. We let $\varepsilon > 0$ be such that

$$\max\left\{ |\omega_k^{(i)} - \hat{\omega}_k^{(i)}| \,\middle|\, 1 \leqslant i, k \leqslant 4 \right\} < \varepsilon;$$

and, for $\vec{x} \in \mathbf{Z}^4$ we denote by $\hat{\mu}^{(i)}(\vec{x})$ ($i = 1,2$) the approximation obtained by substituting $\hat{\omega}_k^{(i)}$ for $\omega_k^{(i)}$ in (4.4).

On putting

$$\delta = \left(64W^2W^*N(\mathfrak{b})^{1/4} + \delta_1/4\right)\delta_1, \tag{4.8}$$

where $\delta_1 = 128\varepsilon WW^*N(\mathfrak{b})^{1/4}$, it is a simple matter to show that for every $x \in \mathbf{Z}^4$ subject to (4.7), we get

$$|\mu^{(i)}(\vec{x}) - \hat{\mu}^{(i)}(\vec{x})| < \delta_1/2 \qquad (i = 1,2).$$

Hence,

$$|\mu^{(i)}(\vec{x})^2 - \hat{\mu}^{(i)}(\vec{x})^2| < \delta/2. \tag{4.9}$$

Thus (4.5) can be true only if

$$|\hat{\mu}^{(1)}(\vec{x}_1)|^2 + |\hat{\mu}^{(2)}(\vec{x}_1)|^2 \leqslant |\hat{\mu}^{(1)}(\vec{x}_2)|^2/f^2 + |\hat{\mu}^{(2)}(\vec{x}_2)|^2/f^2 + 2\delta. \tag{4.10}$$

We see, then, that the search for $\vec{x}_1$ can be conducted by using an algorithm of Fincke and Pohst [10]. This algorithm computes all the solutions $\vec{x}$ of an inequality

$$Q(\vec{x}) \leqslant K,$$

where Q is a positive definite n-dimensional rational quadratic form and $K \geqslant 0$ is a constant. By (4.9) we can check whether a pair $\vec{x}_1$, $\vec{x}_2$ subject to (4.7) satisfies (4.5) as long as

$$\left| |\hat{\mu}^{(i)}(\vec{x}_1)|^2 - |\hat{\mu}^{(i)}(\vec{x}_2)|^2/f^2 \right| \geqslant \delta \tag{4.11}$$

for $1 \leqslant i \leqslant 2$. We conclude these remarks by describing how the search for $\vec{x}_1$ in the second step of Algorithm 4.1 should be conducted.

We determine the solutions of (4.10) by using the method of [10]. Suppose $\vec{x}_1$ is any such solution. If the components of $\vec{x}_1$ do not satisfy (4.7), then this $\vec{x}_1$ must be rejected as a possible solution of (4.5). If $\vec{x}_1$ is not rejected, we next check whether

$$|\hat{\mu}^{(i)}(\vec{x}_1)|^2 \leqslant |\hat{\mu}^{(i)}(\vec{x}_2)|^2/f^2 - \delta \tag{4.12}$$

or

$$|\hat{\mu}^{(i)}(\vec{x}_1)|^2 \geqslant |\hat{\mu}^{(i)}(\vec{x}_2)|^2/f^2 + \delta. \tag{4.13}$$

In the first case, we have found a solution $\vec{x}_1$ of (4.5); in the second case, we must reject $\vec{x}_1$ as a possible solution of (4.5).

If neither (4.12) nor (4.13) holds (a situation which we never encountered in any of our computing), we must check whether

$$|\mu^{(i)}(\vec{x}_1)| = |\mu^{(i)}(\vec{x}_2)|/f \qquad (i = 1, 2). \tag{4.14}$$

This can be done by computing the characteristic polynomial of $\eta = \mu^{(1)}(\vec{x}_1)/\mu^{(1)}(\vec{x}_2)$ and using Proposition 2.2. If (4.14) holds, we reject $\vec{x}_1$; if (4.14) does not hold, we must increase the precision of our approximations to $\omega_k^{(i)}$; that is, we have to decrease ε and repeat this part of step 2. During our calculations, we found, on using a value of $\varepsilon \approx 10^{-12}$, that one of (4.12) or (4.13) held.

If we have tested all the solutions of (4.10) without finding a solution of (4.5), then no such solution exists.

In our complexity analysis in the next section it is necessary to be able to prove that there exists a value of ε such that one of (4.12), (4.13) or (4.14) must hold whenever $\vec{x}_1$ and $\vec{x}_2$ satisfy (4.7). We do this in

PROPOSITION 4.1. *There exists a constant c_2 independent of $\mathscr{L}$ such that if $\vec{x}_1$ and $\vec{x}_2$ both satisfy* (4.7), *$\varepsilon \leqslant c_2 D^{-29/2}$, and δ is defined by* (4.8), *then* (4.5) *is true if and only if*

$$|\hat{\mu}^{(i)}(\vec{x}_1)|^2 \leqslant |\hat{\mu}^{(i)}(\vec{x}_2)|^2/f^2 - \delta \qquad (i = 1, 2). \tag{4.15}$$

Proof. If (4.15) is true, then by (4.9),

$$\begin{aligned}\delta &\leqslant |\hat{\mu}^{(i)}(\vec{x}_2)|^2/f^2 - |\hat{\mu}^{(i)}(\vec{x}_1)|^2 \leqslant \left| |\hat{\mu}^{(i)}(\vec{x}_2)|^2/f^2 - |\mu^{(i)}(\vec{x}_2)|/f^2 \right| \\ &\quad + |\mu^{(i)}(\vec{x}_2)|^2/f^2 - |\mu^{(i)}(\vec{x}_1)|^2 + \left| |\mu^{(i)}(\vec{x}_1)|^2 - |\hat{\mu}^{(i)}(\vec{x}_1)|^2 \right| \\ &< \delta + |\mu^{(i)}(\vec{x}_2)|^2/f^2 - |\mu^{(i)}(\vec{x}_1)|^2\end{aligned}$$

and (4.5) follows.

If (4.5) holds, let

$$\gamma_i = |\mu^{(i)}(\vec{x}_1)|^2 - |\mu^{(i)}(\vec{x}_2)|^2/f^2 \qquad (i = 1, 2).$$

Now γ_i belongs to the product of the extension ideals $\mathfrak{b}^{(i)}/f = \{\beta^{(i)}/f \mid \beta \in \mathfrak{b}\}$ and $\overline{\mathfrak{b}^{(i)}/f}$ in the field $\mathscr{F} = \mathscr{L}^{(i)}(\overline{\rho^{(i)}})$. This product ideal is of norm $(N(\mathfrak{b}/f))^{2k}$, where $k = [\mathscr{F}:\mathscr{L}^{(i)}] \leqslant 3$; therefore, by (4.3) we get

$$\begin{aligned}(N(\mathfrak{b}/f))^{2k} &\leqslant |N_{\mathscr{F}/\mathscr{Q}}(\gamma_i)| \\ &\leqslant \left| |\mu^{(i)}(\vec{x}_1)|^2 - |\mu^{(i)}(\vec{x}_2)|^2/f^2 \right| (32W^2)^{4k-1} f^{2-8k} N(\mathfrak{b})^{2k-1/2},\end{aligned}$$

because each of the $4k-1$ factors in the norm of γ_i different from γ_i must be bounded by $32W^2N(\mathfrak{b})^{1/2}/f^2$. Hence,

$$\left| \left|\mu^{(i)}(\vec{x}_1)\right|^2 - \left|\mu^{(i)}(\vec{x}_2)\right|^2 \right| \geqslant sN(\mathfrak{b})^{1/2}, \tag{4.16}$$

where

$$s = f^{6k-2}/(32W^2)^{4k-1} < 1.$$

If we put $r = s/(2^{14}W^3W^{*2})$, then by (2.2) and (2.3) we have $r \geqslant c_2 D^{-29/2}$, where c_2 is a constant which is independent of $\mathscr{L}$. If we select any $\varepsilon \leqslant r$, then from (4.8) and the fact that $W > 1$, we get

$$2\delta \leqslant sN(\mathfrak{b})^{1/2}.$$

It follows from (4.5) and (4.16) that

$$\begin{aligned} 2\delta &\leqslant \left|\mu^{(i)}(\vec{x}_2)\right|^2/f^2 - \left|\mu^{(i)}(\vec{x}_1)\right|^2 \\ &\leqslant \left| \left|\mu^{(i)}(\vec{x}_2)\right|^2/f^2 - \left|\hat{\mu}^{(i)}(\vec{x}_2)\right|^2 \right| + \left|\hat{\mu}^{(i)}(\vec{x}_2)\right|^2/f^2 - \left|\hat{\mu}^{(i)}(\vec{x}_1)\right|^2 \\ &\quad + \left| \left|\hat{\mu}^{(i)}(\vec{x}_1)\right|^2 - \left|\mu^{(i)}(\vec{x}_1)\right|^2 \right| \\ &< \delta + \left|\hat{\mu}^{(i)}(x_2)\right|^2/f^2 - \left|\hat{\mu}^{(i)}(\vec{x}_1)\right|^2 \end{aligned}$$

by (4.9). □

5. The Complexity. By using the results of [6] we see that the complexity of the computation of bases for all reduced principal ideals in $\mathcal{O}_{\mathscr{L}}$ is $O(RD^{\varepsilon})$, where R is the regulator of $\mathscr{L}$ and by $O(D^{\varepsilon})$ we mean $O(D^{\varepsilon})$ for all $\varepsilon > 0$. The computation of a generator of any of these reduced ideals also requires that $O(RD^{\varepsilon})$ binary operations be performed. By [15, Proposition 1.26] the running time for the computation of an LLL-matrix of $\mathfrak{b}$ is $O(\log|\tilde{B}|_{\infty})$.

We must now analyze Algorithm 4.1. Since the norms of all elements of $\underline{b}$ are at least $N(\mathfrak{b})$, it follows from the bound in (4.3) on the initial values of $|\mu^{(i)}(\vec{x}_2)|$ $(1 \leqslant i \leqslant 2)$ that the number of iterations when $f = 2$ is $O(\log D)$. When the convex body $\mathscr{K}$ described by (4.5) with $f = 2$ contains no nonzero point of the lattice, the algorithm changes f to 1. Now the corresponding convex body with $f = 1$ can be covered by $O(1)$ bodies congruent to $\mathscr{K}$. Also, each of these covering bodies can only contain one lattice point; for, if it contained two, then the difference of these points would be a nonzero point in $\mathscr{K}$. Hence, after Algorithm 4.1 changes f to 1, there can only be $O(1)$ possible solutions of (4.5); thus, the number of iterations needed by this algorithm is $O(\log D)$.

It remains to analyze the complexity of the search for $\vec{x}_1$ in Algorithm 4.1. Since $|\det(b_{kj})| = N(\mathfrak{b})$, we see by (4.1), (2.2) and (2.3) that, if $\vec{x}$ satisfies (4.7), then there exists a constant c_3 independent of $\mathscr{L}$ such that

$$|\vec{x}| \leqslant c_3 D^6. \tag{5.1}$$

It follows from Proposition 4.1 that we can search the convex body described by (5.1) and (4.15), which has rational constraints, rather than the one described by (4.5), which has irrational constraints. Though the algorithm of Fincke and Pohst

[10] has turned out to be very efficient in practice, we cannot use the complexity analysis provided in [10] for this algorithm. Therefore, we replace this method by a procedure of Lenstra [18] which, unfortunately, is too complicated for practical implementation. Lenstra proves that the search for a lattice point in a convex set which is solvable in the sense of [11, Sections 1 and 3] can be carried out in polynomial time in the binary length of the input data; cf. [18, Section 10, Remark (d)]. It can be easily verified that the convex set described by (5.1) and (4.15) is solvable. In view of (2.2), (4.1), (4.3), (5.1), and Proposition 4.1, the input data length is $O(\log D)$; hence, Algorithm 4.1 computes a minimum in $\mathfrak{b}$ in terms of the $\mathbf{Z}$-basis $\{\beta_1, \beta_2, \beta_3, \beta_4\}$ in $O(D^\varepsilon)$ operations.

The computation of a basis of a reduced ideal in the class containing $\mathfrak{b}$ takes another $O(D^\varepsilon \log N(\mathfrak{b}))$ operations. Finally, we can compare the reduced ideal equivalent to $\mathfrak{b}$ to all the principal reduced ideals in $O(RD^\varepsilon)$ operations; and, if $\mathfrak{b}$ is a principal ideal, a generator of $\mathfrak{b}$ can be computed in $O(RD^\varepsilon \log N(\mathfrak{b}))$ operations. We have proved

THEOREM 5.1. (i) *A reduced ideal in the class containing* $\mathfrak{b}$ *can be computed in* $O(\log|\tilde{B}|_\infty + D^\varepsilon \log N(\mathfrak{b}))$ *binary operations.*

(ii) *It can be determined whether or not an ideal* $\mathfrak{b}$ *is principal in*

$$O\big(\log|\tilde{B}|_\infty + D^\varepsilon \log N(\mathfrak{b}) + RD^\varepsilon\big)$$

binary operations.

(iii) *If* $\mathfrak{b}$ *is principal, a generator of* $\mathfrak{b}$ *can be computed in*

$$O\big(\log|\tilde{B}|_\infty + RD^\varepsilon \log N(\mathfrak{b})\big)$$

binary operations.

6. Application: The Computation of Certain Cyclotomic Constants. Let p be a prime such that $p = ef + 1$. A central problem in the theory of cyclotomy is that of determining values for the cyclotomic numbers (h, k), where (h, k) is, for a given primitive root g of p, the number of solutions s, t of the congruence

$$1 + g^{es+h} \equiv g^{et+k} \pmod{p}, \tag{6.1}$$

where $0 \leqslant s, t \leqslant f - 1$. Note that if $h \equiv h_1$, $k \equiv k_1 \pmod{e}$, then $(h, k) = (h_1, k_1)$. It must, of course, be emphasized here that one cannot define the numbers (h, k) in terms of p alone, because they also depend for their values on g, and there are $\phi(p - 1)$ choices for g. Indeed, if g' is another primitive root of p, then $g' = g^m$ for some m such that $\gcd(m, p - 1) = 1$. The values for $(h, k)'$ (using g' for g in (6.1)) are $(mh, mk) = (h', k')$, where $h' \equiv mh$, $k' \equiv mk' \pmod{e}$.

In [8] Dickson showed how the problem of evaluating the cyclotomic numbers for p when $e = 5$ could be related to that of finding integer solutions to the Diophantine system (1.1). In this section we will show how the methods developed in the previous sections can be used to provide a very efficient method for solving (1.1). Further, we show how the cyclotomic numbers can be computed for a given g.

Since $p \equiv 1 \pmod 5$, there must exist four distinct solutions of the congruence

$$x^4 + x^3 + x^2 + x + 1 \equiv 0 \pmod{p}. \tag{6.2}$$

If r is any one of these solutions, then r^2, r^3, r^4 are the others. If we know in advance a quintic nonresidue n modulo p, then

$$r \equiv n^{(p-1)/5} \pmod{p},$$

is a solution of (6.2). If we know any quadratic nonresidue of p, we can use Shanks' [22] algorithm to solve

$$x^2 \equiv a \pmod{p}$$

when $(a/p) = 1$. This algorithm will find a value for x in $O((\log p)^2)$ binary operations. Thus, we can find a value for r by solving the sequence of linear and quadratic congruences

$$\begin{aligned} x^2 &\equiv 5 \pmod{p}, \\ 2y &\equiv x - 1 \pmod{p}, \\ z^2 &\equiv -y - 3 \pmod{p}, \\ 2r &\equiv y + z \pmod{p}, \end{aligned}$$

in $O((\log p)^2)$ binary operations.

In practice, the problem of determining a quadratic or quintic nonresidue of any prime p is simply solved by trial (3/4 of all p have either -1 or 2 as a quadratic nonresidue); however, in general it is very difficult to show theoretically that this process will succeed in finding a nonresidue in polynomial time. Lenstra [17] has pointed out that under the Extended Riemann Hypothesis (ERH) we would have a least quadratic nonresidue $q \leqslant 70 (\log p)^2$ and Bach [1] has recently improved this to $q < 2(\log p)^2$. Indeed, Bach shows that if G is any proper multiplicative subgroup of the integers (mod m), then the least positive integer x outside G satisfies

$$x \leqslant 2(\log m)^2 \qquad (m > 1000),$$

assuming the ERH. Hence, under this assumption, we know that if $p > 1000$ there must exist a quintic nonresidue $n < 2(\log p)^2$. It follows that, under the ERH, we can solve (6.2) in $O((\log p)^3)$ binary operations. (It requires $O(\log p)$ binary operations for each of $O((\log p)^2)$ trials.)

Let ζ be a primitive 5th root of unity, let $\mathscr{L} = \mathscr{Q}(\zeta)$ be the (totally complex) cyclotomic field formed by adjoining ζ to $\mathscr{Q}$, and let r be any fixed solution of (6.2). It is well known that the ideal $\mathfrak{p}$ with $\mathbf{Z}$-basis $\{p, \zeta - r, (\zeta - r)^2, (\zeta - r)^3\}$ is a prime ideal of $\mathbf{Z}(\zeta)$ $(= \mathcal{O}_{\mathscr{L}})$ and $\mathfrak{p} \mid (p)$. Since $\mathscr{L}$ has class number 1 and (we found that) there is only one reduced ideal of $\mathbf{Z}(\zeta)$, we see by our previous results that we can compute a generator for $\mathfrak{p}$ in $O(\log p)$ binary operations.

Let $\pi = \pi(\zeta) = a_1\zeta + a_2\zeta^2 + a_3\zeta^3 + a_4\zeta^4$ be this generator of $\mathfrak{p}$. We note that since $\pi \in \mathfrak{p}$, we must have

$$\pi(r) = a_1 r + a_2 r^2 + a_3 r^3 + a_4 r^3 \equiv 0 \pmod{p}. \tag{6.3}$$

Also, $(p) = \pi_1\pi_2\pi_3\pi_4$, where π_i is the prime ideal generated by $\pi(\zeta^i)$.

There are $\phi(p-1)/4$ primitive roots g of p such that $g^{(p-1)/5} \equiv r \pmod{p}$. Let g be any one of them and define the Gauss sum

$$\tau(\beta) = \sum_{j=0}^{p-2} \beta^j \xi^{g^j},$$

where β is a primitive 5th root of unity and ξ is a primitive pth root of unity. It is well known (see [8]) that the Jacobi function

$$\psi_m(\zeta) = \frac{\tau(\zeta)\tau(\zeta^m)}{\tau(\zeta^{m+1})} \qquad (5 \nmid m(m+1))$$

can be written in terms of ζ only. Indeed,

$$\psi_m(\zeta) = \sum_{j=1}^{p-2} \zeta^{\operatorname{ind}(j)-(m+1)\operatorname{ind}(j+1)},$$

where $g^{\operatorname{ind}(k)} \equiv k \pmod p$. Thus, $\psi_i(\zeta) \in \mathscr{L}$ $(i = 1, 2, 3, 4)$ and we also have $p = \psi_i(\zeta)\psi_i(\zeta^4) = \psi_i(\zeta^2)\psi_i(\zeta^3)$. In fact, by (6.3) and a theorem of Kummer (see, for example, Smith [23, Art. 60]), we know that

$$\psi_1(\zeta) = \pm\zeta^s\pi(\zeta)\pi(\zeta^3),$$

where $\pm\zeta^s$ is selected such that

$$\psi_1(\zeta) \equiv -1 \bmod (1-\zeta)^2.$$

If we put

$$\psi_1(\zeta) = b_1\zeta + b_2\zeta^2 + b_3\zeta^3 + b_4\zeta^4,$$

the values of x, u, v, w can be computed [8] by using

$$\begin{aligned} -x &= b_1 + b_2 + b_3 + b_4, \\ 5u &= b_1 + 2b_2 - 2b_3 - b_4, \\ 5v &= 2b_1 - b_2 + b_3 - 2b_4, \\ 5w &= b_1 - b_2 - b_3 + b_4. \end{aligned}$$

Furthermore, we can compute the cyclotomic numbers for any value of g such that $g^{(p-1)/5} \equiv r \pmod p$ by using (see Whiteman [24, pp. 95–111])

$$\begin{aligned} 25(0,0) &= p - 14 + 3x, \\ 100(0,1) &= 4p - 16 - 3x + 50v + 25w, \\ 100(0,2) &= 4p - 16 - 3x + 50u - 25w, \\ 100(0,3) &= 4p - 16 - 3x - 50u - 25w, \\ 100(0,4) &= 4p - 16 - 3x - 50v + 25w, \\ 100(1,2) &= 4p + 4 + 2x - 50w, \\ 100(1,3) &= 4p + 4 + 2x + 50w. \end{aligned}$$

The remaining 18 cyclotomic numbers can be computed by using the symmetry property $(h, k) = (k, h)$ and the result that $(h, k) = (5 - h, k - h)$.

The solution sets $\{x, u, v, w\}$ of the system (1.1) are very important in cyclotomy. For example, they can be used for deriving the coefficients of the period equation (Lehmer [13]) and its discriminant (Lehmer [14]), and for determining certain quintic residuacity conditions (Lehmer [12], Williams [26], [27], [28]). We now know that they can be efficiently computed. In fact, a FORTRAN program was written to do

this and run on a VAX 11/785 in the Electrical Engineering Department at Ohio State University. In a total of about an hour of CPU time we were able to compute a solution set for each of the 18347 primes p with $50{,}000 < p < 1{,}000{,}000$.

We conclude this section by pointing out that we can now determine the number of solutions of

$$ax^5 + by^5 \equiv c \pmod{p} \qquad (p \nmid xyabc) \tag{6.4}$$

in polynomial time when we are given a solution r of (6.2). We let g be any primitive root satisfying $r \equiv g^{(p-1)/5}$. Put $A \equiv ac^{-1}$, $B \equiv -bc^{-1}$ and let $\operatorname{ind}_g A = k$, $\operatorname{ind}_g B = h \pmod{p}$. Then (6.4) can be transformed into

$$g^{5s+h} + 1 \equiv g^{5t+k}, \tag{6.5}$$

and the number of solutions of (6.5) is (h, k). The difficulty here is that we cannot compute h and k; however, we only need to know k and $h \pmod 5$ and this we can easily do by observing that

$$A^{(p-1)/5} \equiv r^k, \qquad B^{(p-1)/5} \equiv r^h \pmod{p}.$$

Hence, h and k may be easily computed modulo 5 and we can enumerate the solutions of (6.4).

Department of Mathematics
Ohio State University
Columbus, Ohio 43210

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

1. ERIC BACH, *What to Do Until the Witness Comes: Explicit Bounds for Primality Testing and Related Problems*, Ph.D. Thesis, Univ. of California, Berkeley, Calif., 1984.

2. K. K. BILLEVICH, "On the equivalence of two ideals in an algebraic number field of order n," *Mat. Sb.* (*N.S.*), v. 58 (100), 1962, pp. 17–28.

3. Z. I. BOREVICH & I. R. SHAFAREVICH, *Number Theory*, Academic Press, New York, 1966.

4. J. BUCHMANN, "A criterion for the equivalence of two ideals," in *EUROSAM* 84 *Proceedings*, Lecture Notes in Comput. Sci., vol. 174, 1984, pp. 333–340.

5. J. BUCHMANN, "On the computation of units and class numbers by a generalization of Lagrange's algorithm," *J. Number Theory*. (To appear.)

6. J. BUCHMANN, "The computation of the fundamental unit of totally complex quartic orders," *Math. Comp.*, v. 48, 1987, pp. 39–54.

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

→ L. E. DICKSON, "Cyclotomy, higher congruences, and Waring's problem," *Amer. J. Math.*, v. 57, 1935, pp. 391–424.

9. G. DUECK & H. C. WILLIAMS, "Computation of the class number and class group of a complex cubic field," *Math. Comp.*, v. 45, 1985, pp. 223–231.

10. U. FINCKE & M. POHST, "Improved methods for calculating vectors of short length in a lattice, including a complexity analysis," *Math. Comp.*, v. 44, 1985, pp. 463–471.

→ M. GRÖTSCHEL, L. LOVÁSZ & A. SCHRIJVER, "The ellipsoid method and its consequences in combinatorial optimization," *Combinatorica*, v. 1, 1981, pp. 169–197.

12. EMMA LEHMER, "The quintic character of 2 and 3," *Duke Math. J.*, v. 18, 1951, pp. 11–18.

→ EMMA LEHMER, "On the location of Gauss sums," *M.T.A.C.*, v. 10, 1956, pp. 194–202.

→ EMMA LEHMER, "On the divisors of the discriminant of the period equation," *Amer. J. Math.*, v. 90, 1968, pp. 375–379.

→ A. K. LENSTRA, H. W. LENSTRA, JR. & L. LOVÁSZ, "Factoring polynomials with rational coefficients," *Math. Ann.*, v. 261, 1982, pp. 515–534.

16. H. W. LENSTRA, JR., *On the Calculation of Regulators and Class Numbers of Quadratic Fields*, London Math. Soc. Lecture Note Ser., vol. 56, 1982, pp. 123–150.

17. H. W. LENSTRA, JR., "Primality testing," *Computational Methods in Number Theory*, Math. Centrum Tracts, Number 154, part I, Amsterdam, 1983, pp. 55–77.

18. H. W. LENSTRA, JR., "Integer programming with a fixed number of variables," *Math. Oper. Res.*, v. 8, 1983, pp. 538–548.

19. M. POHST & H. ZASSENHAUS, "Über die Berechnung von Klassenzahlen und Klassengruppen algebraischer Zahlkörper, *J. Reine Angew. Math.*, v. 361, 1985, pp. 50–72.

20. R. J. SCHOOF, "Quadratic fields and factorization," *Computational Methods in Number Theory*, Math. Centrum Tracts, Number 155, part II, Amsterdam, 1983, pp. 235–286.

21. D. SHANKS, "The infrastructure of real quadratic fields and its application," *Proc.* 1972 *Number Theory Conf.*, Boulder, Colorado, 1973, pp. 217–224.

22. D. SHANKS, "Five number theoretic algorithms," *Proc. Second Manitoba Conference on Numerical Mathematics* (Univ. of Manitoba, Winnipeg, Man., 1972), *Congressus Numerantium*, VII, Utilitas Math., Winnipeg, Manitoba, 1973, pp. 51–70.

23. H. J. S. SMITH, *Report on the Theory of Numbers*, Chelsea, New York, 1965.

24. A. L. WHITEMAN, *The Cyclotomic Numbers of Order Ten*, Proc. Sympos. Appl. Math., vol. 10, Amer. Math. Soc., Providence, R. I., 1960.

25. H. C. WILLIAMS, "Continued fractions and number-theoretic computations," *Rocky Mountain J. Math.*, v. 15, 1985, pp. 621–655.

26. K. S. WILLIAMS, "On Euler's criterion for quintic nonresidues," *Pacific J. Math.*, v. 61, 1975, pp. 543–550.

27. K. S. WILLIAMS, "Explicit forms of Kummer's complementary theorems to his law of quintic reciprocity," *J. Reine Angew. Math.*, v. 288, 1976, pp. 207–210.

28. K. S. WILLIAMS, "Explicit criteria for quintic residuacity," *Math. Comp.*, v. 30, 1976, pp. 847–853.