MATHEMATICS OF COMPUTATION
VOLUME 50, NUMBER 182
APRIL 1988, PAGES 569-579

On the Infrastructure of the Principal Ideal Class of an Algebraic Number Field of Unit Rank One

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

Abstract. Let R be the regulator and let D be the absolute value of the discriminant of an order $\mathcal{O}$ of an algebraic number field of unit rank 1. It is shown how the infrastructure idea of Shanks can be used to decrease the number of binary operations needed to compute R from the best known $O(RD^{\varepsilon})$ for most continued fraction methods to $O(R^{1/2}D^{\varepsilon})$. These ideas can also be applied to significantly decrease the number of operations needed to determine whether or not any fractional ideal of $\mathcal{O}$ is principal.

1. Introduction. In [16] Shanks introduced an idea which has since been modified and extended by Lenstra [13], Schoof [15] and Williams [17]. This idea can be used to decrease the number of binary operations needed to compute the regulator of a real quadratic order of discriminant D from $O(D^{1/2+\varepsilon})$ to $O(D^{1/4+\varepsilon})$ for every $\varepsilon > 0$. In [21] and [17] Williams et al. showed that Shanks' idea could be extended to complex cubic fields. In this note we show that it can be further extended to any order $\mathcal{O}$ of an algebraic number field $\mathcal{F}$ of unit rank one, i.e., to orders of real quadratic, complex cubic, and totally complex quartic fields.

We present an algorithm which computes the regulator R of $\mathcal{O}$ in $O(R^{1/2}D^{\varepsilon})$ binary operations. Here, D is the absolute value of the discriminant of $\mathcal{O}$. We also describe a method for testing an arbitrary (fractional) ideal $\mathfrak{a}$ of $\mathcal{O}$ for principality. This technique requires a number of binary operations that is $O(R^{1/2}D^{\varepsilon} + p(m))$, where $p(m)$ is a polynomial in the input length m of $\mathfrak{a}$.

2. The Baby Step Algorithm. Let $\mathcal{F}$ have degree n over the rationals $\mathcal{Q}$, and suppose $\mathcal{F}$ has s real $\mathcal{Q}$-isomorphisms $\sigma_1, \sigma_2, \ldots, \sigma_s$ and t pairs of complex $\mathcal{Q}$-isomorphisms $\sigma_{s+1}, \bar{\sigma}_{s+1}, \ldots, \sigma_m, \bar{\sigma}_m$ into $\mathcal{C}$, $m = s + t$. Since $\mathcal{F}$ has unit rank 1, we have $m = 2$, and we have only two normalized Archimedian valuations on $\mathcal{F}$, $|\ |_1$ and $|\ |_2$, where by $|\xi|_i$ we denote $|\sigma_i(\xi)|^{e_i}$. Here, $e_i = 1$ when σ_i is real and $e_i = 2$ when σ_i is complex. As is usual in the unit theory, we introduce the logarithm mapping

$$\begin{aligned} \mathrm{Log}\colon\ & \mathcal{F}^{\times} \to \mathcal{R} \\ & \xi \mapsto \mathrm{Log}\,\xi = \log|\xi|_1. \end{aligned}$$

Received June 22, 1987.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 11R11, 11R16, 11Y16, 11Y40.
*Research supported by Deutsche Forschungsgemeinschaft.
**Research supported by NSERC of Canada Grant A7649.

0025-5718/88 $1.00 + $.25 per page

Since $m = 2$, the image $\mathcal{L} = \mathrm{Log}(U)$ of the unit group U in $\mathcal{O}$ is a one-dimensional lattice on the real line $\mathcal{R}$. The regulator R is a basis of this lattice. It can be determined by

PROPOSITION 2.1. *Let η be a unit in $\mathcal{O}$ such that $\mathrm{Log}\,\eta$ is the smallest positive value in $\mathcal{L}$. Then η is a fundamental unit of $\mathcal{O}$, and $\mathrm{Log}\,\eta$ is the regulator of $\mathcal{O}$.*

Proof. Since $\mathcal{L}$ is a lattice of dimension one, each shortest nonzero vector in $\mathcal{L}$ generates $\mathcal{L}$. □

A first "naive" method for finding R is to walk in what we will call "baby steps" (cf. [11]) along the real line, starting at the origin O until we reach R. We will now explain what is meant by these "baby steps".

Units η in $\mathcal{O}$ have the property that there is no α ($\neq 0$) in $\mathcal{O}$ such that $|\alpha|_i < |\eta|_i$ for $i = 1$ and 2. This is true because $|N(\alpha)| = |\alpha|_1|\alpha|_2$ ($\alpha \in \mathcal{O}$), $N(\alpha) \in \mathbf{Z}$, and $|N(\eta)| = 1$. This property, however, does not completely characterize units, as there are many more elements of $\mathcal{O}$ with this feature. Indeed, we now present

Definition 2.2. Let $\mathfrak{a}$ be a (fractional) ideal of $\mathcal{O}$. We call $\mu \in \mathfrak{a}$ a *minimum* of $\mathfrak{a}$ if there is no α ($\neq 0$) in $\mathfrak{a}$ with $|\alpha_i| < |\mu_i|$ for $i = 1$ and 2. The set of all minima of $\mathfrak{a}$ is denoted by $M_{\mathfrak{a}}$.

These minima have several important properties.

PROPOSITION 2.3. *Let $\mathfrak{a}$ be a fractional ideal of $\mathcal{O}$, let $\xi \in \mathcal{F}^{\times}$, and let $\mu \in M_{\mathfrak{a}}$. Then $\xi\mu$ is a minimum of $\xi\mathfrak{a}$. In particular, if ε is a unit of $\mathcal{O}$, then $\varepsilon\mu$ is a minimum of $\mathfrak{a}$; that is, the unit group of $\mathcal{O}$ acts on $M_{\mathfrak{a}}$.*

Proof. Clear. □

PROPOSITION 2.4. *Let $\mathfrak{a}$ be a fractional ideal of $\mathcal{O}$ and let $\mu \in M_{\mathfrak{a}}$; then $|N(\mu)| \leq \sqrt{D}N(\mathfrak{a})$, where $N(\cdot)$ denotes the norm.*

Proof. As pointed out in Buchmann [5, Proposition 2.2], this statement is a consequence of Minkowski's convex body theorem. □

PROPOSITION 2.5. *Let $\mathfrak{a}$ be a fractional ideal of $\mathcal{O}$. Then $\mathrm{Log}\,M_{\mathfrak{a}}$ is a discrete set on the real line $\mathcal{R}^{>0}$; and, for each point x on the real line, there are only finitely many minima $\mu \in M_{\mathfrak{a}}$ with $\mathrm{Log}\,\mu \leq x$.*

Proof. Select a constant $c \in \mathcal{R}^{>0}$ and consider all the minima $\mu \in M_{\mathfrak{a}}$ with $|\mathrm{Log}\,\mu| \leq c$. For any such minimum we have

$$\exp(-c) \leq |\mu|_1 \leq \exp(c). \tag{2.1}$$

But, from Proposition 2.4, we also know that

$$|N(\mu)| = |\mu|_1|\mu|_2 \leq \sqrt{D}N(\mathfrak{a}). \tag{2.2}$$

Hence, from (2.1) and (2.2) we get

$$|\mu|_1 \leq \exp(c) \quad \text{and} \quad |\mu|_2 \leq \sqrt{D}N(\mathfrak{a})\exp(c). \tag{2.3}$$

Since $\mathfrak{a}$ is a free $\mathbf{Z}$ module of rank n, only a finite number of elements of $\mathfrak{a}$ can satisfy (2.3). □

In particular, the set $\Lambda = \mathrm{Log}\,M_{\mathcal{O}}$ is a discrete set in $\mathcal{R}$ with subset $\mathcal{L}$. Thus, we can write Λ as a sequence:

$$\Lambda = (\lambda_{j \in \mathbf{Z}}).$$

The ordering of the elements Λ given in this sequence is uniquely determined by the condition

$$\lambda_i < \lambda_j \Leftrightarrow i < j \quad \text{for } i, j \in \mathbf{Z}. \tag{2.4}$$

Taking a "baby step" means going from λ_i to λ_{i+1}. Before we explain in further detail how this is done, we first note

PROPOSITION 2.6. *The sequence (λ_i) is purely periodic modulo the regulator R of $\mathcal{O}$.*

Proof. Since the absolute norms of the minima of $\mathcal{O}$ are bounded by $\sqrt{D}$, there can only be finitely many pairwise, nonassociated minima. This means that Λ modulo R is finite. But, since by Proposition 2.3, U acts on $M_{\mathcal{L}}$, the sequence must be purely periodic modulo R. □

We remark here that Lenstra [13] and Schoof [15] in their description of the real quadratic case immediately consider the sequence $(\lambda_i) \bmod R$. As, in this paper, it is R which we wish to compute, we will approach this sequence in a somewhat different fashion.

We now describe the geometry of the sequence (λ_i) somewhat further.

PROPOSITION 2.7. (i) *For every $k \in \mathbf{Z}$ we have $\lambda_{k+1} - \lambda_k < \log \sqrt{D}$.*

(ii) *For every $k \in \mathbf{Z}$ we have $\lambda_{k+j} - \lambda_k > c_1$ with*

$$j = \begin{cases} 2, & n = 2, \\ 7, & n = 3, \\ 30, & n = 4, \end{cases}$$

and

$$c_1 = \begin{cases} \log 2, & n = 2, \\ \log 4, & n = 3, \\ \log(2\cos(\pi/5)), & n = 4. \end{cases}$$

Proof. The proof of (i) is given in Buchmann [7]; the proof of (ii) can be found in [17] $n = 2$, Williams [18] $n = 3$, and Buchmann [4] $n = 4$. □

COROLLARY 2.8. *Let p be the number of points in $(\lambda_i) \pmod R$; then*

$$R/(\log \sqrt{D}) < p < jR/c_1. \quad \square$$

Corollary 2.8 shows that the number of baby steps necessary to compute R is $O(R)$. In order to perform these baby steps we must first be able to answer

Questions 2.9. (i) How can one compute λ_{k+1} from λ_k?

(ii) How can one decide whether or not $\lambda_k = R$?

To facilitate answering these questions, we introduce the mapping

$$\phi\colon \mathcal{F}^{\times} \to \mathcal{P}(\mathcal{O}) \times \mathcal{R},$$
$$\alpha \mapsto \phi(\alpha) = (\phi_1(\alpha), \phi_2(\alpha)) = ((1/\alpha)\mathcal{O}, \operatorname{Log} \alpha),$$

where by $\mathcal{P}(\mathcal{O})$ we denote the group of all nonzero principal ideals of $\mathcal{O}$. That is, we represent the elements in $\mathcal{F}^{\times}$ by a principal ideal of $\mathcal{O}$ and a real number. This representation has the following properties.

PROPOSITION 2.10. (i) *ϕ is a group homomorphism whose kernel is the group of the roots of unity in $\mathcal{O}$.*

(ii) *The kernel of ϕ_1 is the unit group U of $\mathcal{O}$.*

Proof. Since ϕ_1 and ϕ_2 are group homomorphisms, it follows that ϕ is a group homomorphism. Now if $\phi_1(\alpha) = \mathcal{O}$, then $(1/\alpha)\mathcal{O} = \mathcal{O}$, and we see that both $1/\alpha$ and α belong to $\mathcal{O}$. Hence $\alpha \in U$. If, moreover, $\phi_2(\alpha) = 0$, then $|\alpha|_1 = 1$; but, since α is a unit, this means that $|\alpha|_2 = 1$ and that α is a root of unity. □

The last statement shows that ϕ represents each element of $\mathcal{F}^\times$ uniquely up to a root of unity. By looking at $\phi_1(\alpha)$, we can also tell whether α is a unit of $\mathcal{O}$; and, if α is a fundamental unit, then $|\phi_2(\alpha)|$ will be the regulator of $\mathcal{O}$.

When performing calculations, we represent the principal ideal $\phi_1(\alpha)$ by a $\mathbf{Z}$-basis. More precisely, we fix a $\mathbf{Z}$-basis $\omega_1, \omega_2, \ldots, \omega_n$ of $\mathcal{O}$. Then $\mathfrak{a} = \phi_1(\alpha)$ is given by its denominator

$$d(\mathfrak{a}) = \min\{d' \in \mathbf{Z}^{>0} \mid d'\mathfrak{a} \subseteq \mathcal{O}\}$$

and an integral transformation matrix $A = (a_{ij}) \in \mathbf{Z}^{n\times n}$ with the property that the elements

$$\alpha_j = \left(\sum_{k=1}^{n} a_{jk}\omega_k\right)/d(\mathfrak{a}) \qquad (1 \le j \le n)$$

form a $\mathbf{Z}$-basis of $\mathfrak{a}$. This matrix is uniquely determined up to a unimodular transformation from the left. We make the matrix A unique by choosing it in some normal form, for example, Hermite normal form. In this case we write $A = \mathrm{HNF}(\mathfrak{a})$, and we have $0 \le a_{ij} < a_{jj}$ $(i < j)$, $a_{ij} = 0$ for $i > j$. Since A and d are unique for $\mathfrak{a}$, we write $\mathfrak{a}$ as $\mathfrak{a}(A, d)$. The advantage of this representation is that we can represent minima of $\mathcal{O}$ by small numbers.

PROPOSITION 2.11. *Let μ be a minimum of $\mathcal{O}$, let $d = d(\phi_1(\mu))$, and let $A = \mathrm{HNF}(\phi_1(\mu))$. Then*

$$d \le \sqrt{D} \quad \text{and} \quad |A|_\infty < \sqrt{D}.$$

Proof. The fractional ideal $\mathfrak{a} = (1/\mu)\mathcal{O}$ contains 1 as a minimum. Hence the ideal $\mathfrak{a}' = d\mathfrak{a}$ is an integral primitive ideal which contains d as a minimum. Moreover, d must be the smallest positive integer contained in $\mathfrak{a}'$, and we therefore find by Proposition 2.4 and the reasoning of Theorem 6.3 of [6] that

$$N(d) = d^n \le N(\mathfrak{a}')\sqrt{D} \le d^{n-1}\sqrt{D},$$

which means that $d \le \sqrt{D}$. Since $d\omega_j \in \mathfrak{a}'$ and the numbers α_j $(j = 1, 2, \ldots, n)$ form a basis of $\mathfrak{a}$, we have $a_{jj} \mid d$ $(j = 1, 2, 3, \ldots, n)$. □

We remark that the order of magnitude of a minimum can be as large as $\exp\sqrt{D}$ (see, for example, Patterson and Williams [14]), which shows that the representation of a minimum μ by using ϕ is much better than the representation by means of the coefficients of the basis elements $\omega_1, \omega_2, \ldots, \omega_n$ of $\mathcal{O}$. Given this representation $\phi(\mu)$ of μ, we are now able to answer Questions 2.9. We first prove

PROPOSITION 2.12. *Let $k \in \mathbf{Z}$ and let $\mu_k \in M_\mathcal{O}$ with $\mathrm{Log}\,\mu_k = \lambda_k$. Further, let η be a minimum in $\phi_1(\mu_k)$ with minimal positive $\mathrm{Log}\,\eta$. Then $\mu_{k+1} = \eta\mu_k \in M_\mathcal{O}$ and $\mathrm{Log}(\mu_{k+1}) = \lambda_{k+1}$.*

Proof. Follows easily from Proposition 2.3. □

We are now able to present

ALGORITHM 2.13 (The baby step method)

Initialization

$A \leftarrow I_n$ (Identity matrix of order n)

$d \leftarrow 1$

$R \leftarrow 0$

Step 1 (Baby step)

Compute in the ideal $\mathfrak{a} = \mathfrak{a}(A, d)$ a minimum η with minimal positive $\operatorname{Log}\eta$. Set $d \leftarrow d((1/\eta)\mathfrak{a})$, $A \leftarrow \operatorname{HNF}((1/\eta)\mathfrak{a})$, $R \leftarrow R + \operatorname{Log}\eta$.

Step 2 (Ready ?)

If $d = 1$ and $A = I_n$, then R is the regulator of $\mathcal{O}$ and the algorithm terminates; otherwise, go to Step 1.

The computation of η in Step 1 has been explained for $n = 2$ in [13], [15] and [17], for $n = 3$ in [17] and for $n = 4$ in Buchmann [5].

PROPOSITION 2.14. *Algorithm* 2.13 *computes the regulator* R *of* $\mathcal{O}$ *in* $O(RD^{\varepsilon})$ *binary operations on numbers of size* $O(D^{\varepsilon})$.

Proof. By Corollary 2.8 the number of iterations in Algorithm 2.13 is $O(R)$. By [17] and [5] it takes $O(D^{\varepsilon})$ binary operations to compute η in Step 1. Finally, by Proposition 2.11, the binary length of the numbers involved is $O(D^{\varepsilon})$. □

3. The Giant Step Algorithm. Algorithm 2.13 is a very effective algorithm as long as D is small. It has been used, for example, by Williams and Broere [19] in the real quadratic case and by Angell [1] and Williams, Cormack and Seah [20] in the complex cubic case and Buchmann [5] in the totally complex quartic case. Other types of baby step algorithms have been used by Ince [11], Hendy [10] and Atkin (see Buell [3]). Unfortunately, as the values of D become very large, these methods become much too time-consuming. In fact, if $\mathcal{O}$ is the maximal order of $\mathcal{F}$ and if the class number of $\mathcal{O}$ is small, then by the Brauer-Siegel Theorem [2] the regulator R of $\mathcal{O}$ will be approximately of the same order of magnitude as $\sqrt{D}$. By Corollary 2.8 this means that the number of iterations of Algorithm 2.13 will be approximately of the same order of magnitude as $\sqrt{D}$. For example, in [14] it was found that for the maximal order of $\mathcal{Q}(\sqrt{D})$ with $D = 350240722763374$, the number of iterations is $p = 70400728$. Shanks [16] was the first to observe in the real quadratic case that it is possible to skip a large number of the baby steps by taking what we will call "giant steps". In this section we will show that his idea applies to the unit rank 1 case in general.

Assume that we know the representations $\phi(\mu_1)$ and $\phi(\mu_2)$ of two minima μ_1, μ_2 in $\mathcal{O}$, where, as before, $\mathcal{O}$ is any order of $\mathcal{F}$. Now we form $\psi = \phi(\mu_1)\phi(\mu_2)$. Using a Hermite reduction, ψ can be computed in $O(D^{\varepsilon})$ binary operations (see Kannan and Bachem [12]). In general, ψ will not be the representation of a minimum of $\mathcal{O}$; but, we can apply a certain reduction procedure to $\psi = (\mathfrak{a}, \delta)$ in order to make it the representation of a minimum. For this purpose, we use one of the algorithms of [17] or Buchmann and Williams [8], [9] to obtain a minimum η in $\mathfrak{a}$. Then we

put $\mathfrak{a}^* = (1/\eta)\mathfrak{a}$ and $\delta^* = \delta + \operatorname{Log}\eta$ and we define the operation * by

$$\begin{aligned}\phi(\mu_1)^*\phi(\mu_2) &= (\phi_1(\mu_1)^*\phi_1(\mu_2), \phi_2(\mu_1)^*\phi_2(\mu_2)) \\ &= (\mathfrak{a}^*, \delta^*).\end{aligned}$$

PROPOSITION 3.1. *Let* $\mu_1, \mu_2 \in M_{\mathcal{O}}$.

(i) *There is a minimum* μ^* *in* $\mathcal{O}$ *such that* $\phi(\mu_1)^*\phi(\mu_2) = \phi(\mu^*)$.

(ii) *We have* $-c_4 < \phi_2(\mu^*) - \phi_2(\mu_1\mu_2) \le c_5$ *with*

$$c_4 = \begin{cases} \log D, & \text{for } n = 2, \\ 2\log(D/3), & n = 3, \\ \log 16D^5, & n = 4, \end{cases}$$

and

$$c_5 = \begin{cases} 0, & \text{for } n = 2, \\ 0, & n = 3, \\ \log 16D, & n = 4. \end{cases}$$

Proof. Since η is a minimum in $\mathfrak{a} = (1/\mu_1\mu_2)\mathcal{O}$, the element $\mu^* = \eta\mu_1\mu_2$ must by Proposition 2.3 be a minimum in $\mathcal{O}$, and $\phi(\mu^*) = \phi(\mu_1)^*\phi(\mu_2)$. The bounds in (ii) for $n = 2, 3$ follow from estimates given in [17].

When $n = 4$, we note that $\phi_1(\mu_1)$ and $\phi_1(\mu_2)$ are reduced ideals; thus,

$$d(\mathfrak{a}) = d(\phi_1(\mu_1)\phi_2(\mu_2)) \le D.$$

If we put $d = d(\mathfrak{a})$ and $\mathfrak{a}' = d\mathfrak{a}$, then $N(\mathfrak{a}') \le d^4$. Thus, by using the algorithm of [8] we can find a minimum μ' of $\mathfrak{a}'$ such that

$$|\mu'^{(i)}| \le 4Wd. \tag{3.1}$$

The latter inequality follows from (4.3) of [8]. By (3.1) we now have

$$|\mu'|_i \le 16W^2d^2;$$

but, since $|N(\mu')| = |\mu'|_1|\mu'|_2 \ge 1$, we get

$$|\mu'|_i \ge (16W^2d^2)^{-1}.$$

Now $\eta = \mu'/d$ is a minimum in $\mathfrak{a}$; hence,

$$(16W^2d^4)^{-1} \le |\eta|_i \le 16W^2.$$

Since $d < D, W < \sqrt{D}$ (see (2.2) of [8]), we find that

$$(16D^5)^{-1} \le |\eta|_i \le 16D. \quad \square$$

Thus, we see that if we are given the representations $\phi(\mu_1)$ and $\phi(\mu_2)$ for two minima μ_1, μ_2 of $\mathcal{O}$, we can make the *giant step* $\phi(\mu_1)^*\phi(\mu_2)$; and, by Proposition 3.1(ii), we can almost precisely predict the value of $\phi_2(\mu_1)^*\phi_2(\mu_2)$. This information is now used in

ALGORITHM 3.2 (The giant step algorithm)

Initialization

$\kappa \leftarrow 2c_4, K \leftarrow [\kappa]$

Step 1 (Baby steps)

By the method of Algorithm 2.13, compute the representations of the minima μ in $\mathcal{O}$ with

$$\phi_2(\mu) \leq \kappa + c_5 + \log \sqrt{D}. \tag{3.2}$$

If R is found, then terminate the algorithm. If not, store all these representations and sort them such that the denominators d and the HNF's, representing the first component of $\phi(\mu)$, are in lexicographical order. We denote these representations by $\phi^{(1)}, \phi^{(2)}, \ldots, \phi^{(j)}$, where $\phi^{(i)} = (\phi_1^{(i)}, \phi_2^{(i)})$.

Step 2 (Choice of width of giant step)

From $\phi^{(1)}, \phi^{(2)}, \ldots, \phi^{(j)}$ choose ψ^* with

$$\kappa \leq \psi_2^* < \kappa + \log \sqrt{D}$$

(This is possible by Proposition 2.7(i).) Set $\Psi^{(0)} \leftarrow \psi^*, i \leftarrow 0$.

Step 3 (Giant step)

Compute

$$\Psi^{(i+1)} = \Psi^{(i)} * \psi^*$$

and put $i \leftarrow i + 1$.

Step 4 (Test)

If $\Psi_1^{(i)} = \phi_1^{(k)}$ for some $k \in \{1, 2, 3, \ldots, j\}$, then set $R = \Psi_2^{(i)} - \phi_2^{(k)}$ and terminate the algorithm. (Of course, we determine whether or not $\Psi_1^{(i)} = \phi_1^{(k)}$ by conducting a binary search of the first components of the *baby stock* $\phi^{(1)}, \phi^{(2)}, \ldots, \phi^{(j)}$.)

Step 5 (Increase κ)

If $i = K$, then put $\kappa \leftarrow 2\kappa$, $K = [\kappa]$ and go to Step 1; otherwise, go to Step 3.

THEOREM 3.3. *Algorithm* 3.2 *computes the regulator* R *of* $\mathcal{O}$ *in* $O(R^{1/2}D^{\varepsilon})$ *binary operations.*

Proof. For a fixed κ, and ψ^* fixed by Step 2, we have by Proposition 3.1 (ii)

$$\Psi_2^{(j)} = (j+1)\psi_2^* + \sum_{r=1}^{j} \varepsilon_r,$$

where $-c_4 < \varepsilon_r \leq c_5$ and $j \leq K = [\kappa]$. It follows that

$$\Psi_2^{(k)} > \kappa^2 - c_4\kappa.$$

Thus, if

$$\kappa > (R + c_4^2/4)^{1/2} + c_4/2, \tag{3.3}$$

we must have $\Psi_2^{(k)} > R$. Thus, the first time we have a κ satisfying (3.3), we must have some i $(1 \leq i \leq K)$ such that

$$\Psi_2^{(i)} > R \quad \text{and} \quad \Psi_2^{(i-1)} < R.$$

Since

$$\Psi_2^{(i)} = \Psi_2^{(i-1)} + \psi_2^* + \varepsilon_i,$$

we get

$$R < \Psi_2^{(i)} < R + \kappa + \log\sqrt{D} + c_5.$$

It follows from (3.2), Proposition 2.6, and Proposition 2.10 that there must be some $k \in \{1, 2, \ldots, j\}$ such that

$$\Psi_2^{(i)} = \phi_1^{(k)} \quad \text{and} \quad R = \Psi_2^{(i)} - \phi_2^{(k)}.$$

For a fixed value of κ, the number of binary operations performed by Step 1 of Algorithm 3.2 is, by the argument of the proof of Proposition 2.14, $O(\kappa D^{\varepsilon})$. Also, the number of binary operations needed to compute a giant step is $O(D^{\varepsilon})$; hence, for a fixed value of κ the entire algorithm performs $O(\kappa D^{\varepsilon})$ binary operations. Since $R = O(D^{1/4+\varepsilon})$, we know that we need to increase κ $O(D^{\varepsilon})$ times until (3.3) first holds. It follows that in order to find R, Algorithm 3.2 performs a total of $O(R^{1/2}D^{\varepsilon})$ binary operations. □

4. Principal Ideal Testing. As already mentioned in [17] and [8], it is possible to modify the previous algorithm in order to produce a principal ideal test. To this end, we introduce the notion of a reduced ideal.

Definition 4.1. A (fractional) ideal $\mathfrak{a}$ of $\mathcal{O}$ is said to be reduced if 1 is a minimum in $\mathfrak{a}$.

PROPOSITION 4.2. *Let $\mathfrak{a}$ be any fractional ideal of $\mathcal{O}$ and let μ be a minimum in $\mathfrak{a}$; then $(1/\mu)\mathfrak{a}$ is reduced.*

Proof. Follows as a direct consequence of Proposition 2.3. □

Proposition 4.2 provides us with a method for computing a reduced ideal in the ideal class of any given ideal of $\mathcal{O}$. Algorithms for doing this have been given in [17] and [8].

PROPOSITION 4.3. *Let $\mathfrak{a}$ be a reduced ideal of $\mathcal{O}$. Then $\mathfrak{a}$ is principal if and only if there is a minimum μ of $\mathcal{O}$ with $\phi_1(\mu) = \mathfrak{a}$ and $0 \le \phi_2(\mu) < R$.*

Proof. Buchmann [6, Theorem 6.2]. □

We are now able to present the following method for testing a given ideal $\mathfrak{a}$ of $\mathcal{O}$ for principality.

ALGORITHM 4.4 (Principal ideal testing with baby steps)

Step 1 (Computation of the reduced principal ideals)
By the method of Algorithm 2.13 compute $\phi_1(\mu)$ for every minimum μ of $\mathcal{O}$ with $0 \le \phi_2(\mu) < R$. Store all these representations in terms of their denominators and their HNF's and order them lexicographically.

Step 2 (Reduction of $\mathfrak{a}$)
Compute a minimum μ in $\mathfrak{a}$ and put $\mathfrak{a}^* = (1/\mu)\mathfrak{a}$. Store this ideal in terms of its denominator and HNF.

Step 3 (Comparison)
If $\mathfrak{a}^* = \phi_1(\mu)$ for one of the representations computed in Step 1, then $\mathfrak{a}$ is principal; otherwise, $\mathfrak{a}$ is not principal.

As already proved in [8] we have

PROPOSITION 4.5. *Let* $\mathfrak{a}$ *be a fractional ideal of* $\mathcal{O}$. *Algorithm* 4.4 *tests* $\mathfrak{a}$ *for principality in*

$$O(\log(|\mathrm{HNF}(\mathfrak{a})|_\infty d(\mathfrak{a})) + D^\varepsilon \log(d(\mathfrak{a})^n N(\mathfrak{a})) + RD^\varepsilon)$$

binary operations. □

It is clear that Algorithm 4.4 will run very quickly when the number of reduced principal ideals of $\mathcal{O}$ is small. If this is not the case, then we can again use the giant step technique to improve considerably the speed of this algorithm. We do this in

ALGORITHM 4.6 (Principal ideal test with giant steps)

Step 1 (Determination of the baby stock)

By the method of Algorithm 2.13 compute the representations of all the minima $\mu \in \mathcal{O}$ with

$$\phi_2(\mu) \le \sqrt{R} + c_4 + c_5 + \log\sqrt{D}.$$

Store all these representations in terms of their denominators and their HNF's and order them lexicographically. Denote these representations by $\phi^{(1)}, \phi^{(2)}, \ldots, \phi^{(j)}$, where $\phi^{(i)} = (\phi_1^{(i)}, \phi_2^{(i)})$.

Step 2 (Reduction of $\mathfrak{a}$)

Compute a minimum μ in $\mathfrak{a}$ and put $\mathfrak{a}^* = (1/\mu)\mathfrak{a}$. Store this ideal in terms of its denominator and HNF.

Step 3 (Initialize giant step procedure)

Put $i \leftarrow 0, K = [\sqrt{R}] + 1$. Find ϕ^* in the baby stock such that

$$\sqrt{R} + c_4 \le \phi_2^* < \sqrt{R} + c_4 + \log\sqrt{D}.$$

Put $\Psi_1^{(0)} \leftarrow \mathfrak{a}^*$.

Step 4 (Test)

If $i > K$, then $\mathfrak{a}$ is not a principal ideal and we terminate the algorithm. If $i \le K$ and $\Psi_1^{(i)} = \phi_1^{(k)}$ for some $k \in \{1, 2, 3, \ldots, j\}$, then $\mathfrak{a}$ is principal and we terminate the algorithm.

Step 5 (Giant Step)

Put

$$\Psi_1^{(i+1)} \leftarrow \Psi_1^{(i)} * \phi_1^*$$
$$i \leftarrow i + 1$$

Go to Step 4.

THEOREM 4.7. *Let* $\mathfrak{a}$ *be a fractional ideal of* $\mathcal{O}$. *Algorithm* 4.6 *tests* $\mathfrak{a}$ *for principality in*

$$O(\log(|\mathrm{HNF}(\mathfrak{a})|_\infty d(\mathfrak{a})) + D^\varepsilon \log(d(\mathfrak{a})^n N(\mathfrak{a})) + R^{1/2} D^\varepsilon)$$

binary operations.

Proof. Assume $\mathfrak{a}$ is principal. By Propositions 4.2 and 4.3 there must be a minimum μ of $\mathcal{O}$ such that $\phi_1(\mu) = \mathfrak{a}^*$ and $0 \le \phi_2(\mu) < R$. We also have

$$\Psi_2^{(k+1)} = k\phi_2^* + \phi_2(\mu) + \sum_{r=1}^{k} \varepsilon_r,$$

where $-c_4 < \varepsilon_r \leq c_5$. If $\phi_2(\mu) < \sqrt{R} + c_4 + c_5 + \log\sqrt{D}$, then Algorithm 4.6 will determine that $\mathfrak{a}$ is principal when $k = 0$. Otherwise,

$$\Psi_2^{(k+1)} = \sum_{r=1}^{k}(\phi_2^* + \varepsilon_r) + \phi_2(\mu) > (k+1)\sqrt{R}.$$

Thus, when $k = [\sqrt{R}]$ we have $\Psi_2^{(k+1)} > R$. It follows that there must exist some i $(1 \leq i \leq [\sqrt{R}] + 1 = K)$ such that

$$\Psi^{(i-1)} \leq R \quad \text{and} \quad \Psi_2^{(i)} > R.$$

Since

$$\Psi_2^{(i)} = \Psi_2^{(i-1)} + \phi_2^* + \varepsilon_i,$$

we get

$$R < \Psi_2^{(i)} < R + \sqrt{R} + c_4 + \log\sqrt{D} + c_5.$$

It follows by Propositions 2.6 and 2.10 that

$$\Psi_1^{(i)} = \phi_1^{(k)} \quad \text{for some } k \in \{1, 2, 3, \ldots, j\}.$$

On the other hand, if $\mathfrak{a}$ is not principal, then $\Psi_1^{(i)}$ $(\sim \mathfrak{a})$ cannot be principal; thus, $\Psi_1^{(i)} \neq \phi_1^{(k)}$ for any i or k.

By the same arguments as those used in the proofs of Proposition 4.5 and Theorem 3.3 we see that Algorithm 4.6 will execute in

$$O(\log(|\mathrm{HNF}(\mathfrak{a})|_\infty d(\mathfrak{a})) + D^\varepsilon \log(d(\mathfrak{a})^n N(\mathfrak{a})) + R^{1/2} D^\varepsilon)$$

binary operations. □

Mathematisches Institut
Universität Düsseldorf
4000 Düsseldorf 1, West Germany

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

1. I. O. ANGELL, "A table of complex cubic fields," *Bull. London Math. Soc.*, v. 5, 1973, pp. 37–38.

2. R. BRAUER, "On the zeta-functions of algebraic number fields," *Amer. J. Math.*, v. 69, 1947, pp. 243–250.

3. D. A. BUELL, "Computer computation of class groups in quadratic number fields," *Congr. Numer.*, v. 22, 1978, pp. 3–12.

4. J. BUCHMANN, "Abschätzung der Periodenlänge einer verallgemeinerten Kettenbruchentwicklung," *J. Reine Angew. Math.*, v. 361, 1985, pp. 27–34.

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

6. J. BUCHMANN, "On the computation of units and class numbers by a generalization of Lagrange's algorithm," *J. Number Theory*, v. 26, 1987, pp. 8–30.

7. J. BUCHMANN, "On the period length of the generalized Lagrange algorithm," *J. Number Theory*, v. 26, 1987, pp. 31–37.

8. J. BUCHMANN & H. C. WILLIAMS, "On principal ideal testing in totally complex quartic fields and the determination of certain cyclotomic constants," *Math. Comp.*, v. 48, 1987, pp. 55–66.

9. J. BUCHMANN & H. C. WILLIAMS, "On principal ideal testing in algebraic number fields," *J. Symb. Comput.*, v. 4, 1987, pp. 11–19.

10. M. D. HENDY, "The distribution of ideal class numbers of real quadratic fields," *Math. Comp.*, v. 29, 1975, pp. 1129–1134.

11. E. L. INCE, "Cycles of reduced ideals in quadratic fields," *Mathematical Tables*, Vol. IV, British Association for the Advancement of Science, London, 1934.

12. R. KANNAN & A. BACHEM, "Polynomial algorithms for computing the Smith and Hermite normal forms of an integer matrix," *SIAM J. Comput.*, v. 8, 1979, pp. 499–507.

13. H. W. LENSTRA, JR., "On the calculation of class numbers and regulators of quadratic fields," *Lond. Math. Soc. Lecture Note Ser.*, v. 56, 1982, pp. 123–150.

14. C. D. PATTERSON & H. C. WILLIAMS, "Some periodic continued fractions with long periods," *Math. Comp.*, v. 44, 1985, pp. 523–532.

15. R. J. SCHOOF, "Quadratic fields and factorization," in *Computational Methods in Number Theory* (H. W. Lenstra, Jr. and R. Tijdemann, eds.), Math. Centrum Tracts, Number 155, Part II, Amsterdam, 1982, pp. 235–286.

16. D. SHANKS, *The Infrastructure of Real Quadratic Fields and Its Applications*, Proc. 1972 Number Theory Conf., Boulder, 1972, pp. 217–224.

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

18. H. C. WILLIAMS, "The spacing of the minima in certain cubic lattices," *Pacific J. Math.*, v. 124, 1986, pp. 483–496.

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

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

21. H. C. WILLIAMS, G. W. DUECK & B. K. SCHMID, "A rapid method of evaluating the regulator and class number of a pure cubic field," *Math. Comp.*, v. 41, 1983, pp. 235–286.