

Compact Representation in Real Quadratic Congruence Function Fields

R. Scheidler

March 15, 1999

Abstract

A real quadratic congruence function field $K = \mathbb{F}_q(x)(\sqrt{D})$ typically contains many elements α of large height $H(\alpha) = \max\{|\alpha|, |\bar{\alpha}|\}$ and small norm (in absolute value) $|N(\alpha)| = |\alpha\bar{\alpha}|$. A prominent example for this kind of behavior is the fundamental unit η_K whose norm has absolute value 1, but whose height is often exponential in $|D|$. Hence it requires exponential time to even write down η_K , let alone perform computations on η_K . In this paper, we present a shorter representation for elements α in any quadratic order $\mathcal{O} = \mathbb{F}_q[x][\sqrt{D}]$ of K . This representation is analogous to the one for quadratic integers developed by Buchmann, Thiel, and Williams, and is polynomially bounded in $\log |N(\alpha)|$, $\log \deg H(\alpha)$, and $\log |D|$. For the fundamental unit η_K of K , such a representation requires $O((\log |D|)^2)$ bits of storage. We show how to perform arithmetic with compact representations and prove that the problems of principal ideal testing, ideal equivalence, and the discrete logarithm problem for ideal classes belong to the complexity class NP.

1 Introduction

For a general introduction to the topic of real quadratic congruence function fields, see [1] and [3]. Let $k = \mathbb{F}_q$ be a finite field of odd characteristic with q elements. A *quadratic congruence function field* over the field k of *constants* is a quadratic extension K of the rational function field $k(x)$ with a transcendental element $x \in K$. We say that K is a *real quadratic congruence function field* (of odd characteristic) if K is of the form $K = k(x)(\sqrt{D}) = k(x) + k(x)\sqrt{D}$, where $D \in k[x]$ is a squarefree polynomial of even degree whose leading coefficient is a square in $k^* = k \setminus \{0\}$. (This is in analogy to the case of a real quadratic number field $\mathbb{Q}(\sqrt{D})$, where D is a positive, squarefree integer). The *ring of integers of K* is $\mathcal{O}_K = k[x][\sqrt{D}] = k[x] + k[x]\sqrt{D}$.

In contrast to the number field case, there are two places of K at infinity. We know from [9] that the place at infinity \mathfrak{P}_∞ of $k(x)$ with respect to x splits in K as $\mathfrak{P}_\infty = \mathfrak{P}_1 \cdot \mathfrak{P}_2$. Furthermore, the completions of K with respect to \mathfrak{P}_1 and \mathfrak{P}_2 , $K_{\mathfrak{P}_1}$ and $K_{\mathfrak{P}_2}$, respectively, are isomorphic to $k(x)_{\mathfrak{P}_\infty} = \mathbb{F}_q((1/x))$, the field of power series in $1/x$. By explicitly taking square roots of D , we see that K is a subfield of $\mathbb{F}_q((1/x))$. Let \mathfrak{P}_1 be the place which corresponds to the case where $\sqrt{1} = 1$. Then we consider elements of K as Laurent series at \mathfrak{P}_1 in the variable $1/x$. Let $\alpha \in k((1/x))$ be a non-zero element. Then $\alpha = \sum_{i=-\infty}^m c_i x^i$ with $c_m \neq 0$. Denote by

$$\begin{aligned} \deg(\alpha) &= m && \text{the degree of } \alpha, \\ |\alpha| &= q^m && \text{the absolute value of } \alpha, \\ \text{sgn}(\alpha) &= c_m && \text{the sign of } \alpha, \end{aligned}$$

$$[\alpha] = \sum_{i=0}^m c_i x^i \quad \text{the principal part of } \alpha.$$

If m is negative, then $[\alpha] = 0$. We set $\deg(0) = -\infty$ and $|0| = 0$.

In analogy to the case of a real quadratic number field, the *unit group* E_K of K is of the form $E_K = k^* \times \langle \eta_K \rangle$, where $\eta_K \in K$ is a *fundamental unit* of K , so every unit $\epsilon \in K$ can be written as $\epsilon = c\eta_K^m$ for some $c \in k^*$ and $m \in \mathbb{Z}$. We choose η_K so that $|\eta_K| > 1$. Then the positive integer $R_K = \deg(\eta_K)$ is called the *regulator* of K with respect to \mathcal{O}_K .

A (*quadratic*) *order* \mathcal{O} of K is a subring of K that contains $k[x]$ and has K as its field of quotients. Every order \mathcal{O} in K is a free $k[x]$ -module of rank 2 and has a $k[x]$ -basis of the form $\{1, \sqrt{\Delta}\}$ where $\Delta = F^2 D$ for some non-zero $F \in k[x]$. If F is chosen to be monic, then it is unique and is called the *conductor* of \mathcal{O} . Write

$$\mathcal{O} = \mathcal{O}_\Delta = [1, \sqrt{\Delta}] = k[x] + k[x]\sqrt{\Delta}.$$

We have $\mathcal{O}_\Delta \subseteq \mathcal{O}_{\Delta'}$ if and only if Δ/Δ' is a square in $k[x]$. The maximal order (with respect to inclusion) is \mathcal{O}_K , the ring of integers of K .

Let $\mathcal{O} = \mathcal{O}_\Delta$ be a quadratic order of K and let $\alpha = A + B\sqrt{\Delta} \in \mathcal{O}$ ($A, B \in k[x]$). Denote by

$$\begin{aligned} \alpha &= A + B\sqrt{\Delta} && \text{the standard representation of } \alpha, \\ \bar{\alpha} &= A - B\sqrt{\Delta} && \text{the conjugate of } \alpha, \\ N(\alpha) &= \alpha\bar{\alpha} = A^2 - B^2\Delta && \text{the norm of } \alpha, \\ H(\alpha) &= \max\{|\alpha|, |\bar{\alpha}|\} = \max\{|A|, |B\sqrt{\Delta}|\} && \text{the height of } \alpha. \end{aligned}$$

For $\alpha \in \mathcal{O}$ and $Q \in k[x]$, set $H(\alpha/Q) = H(\alpha)/Q$.

In general, a quadratic order contains many elements of large height, whose norm is at the same time comparatively small in absolute value. For example, the fundamental unit η_K of K often has degree of order $|\sqrt{D}|$ (and thus an enormous height of approximately $q^{|\sqrt{D}|} = q^{q^{1/2 \deg(D)}}$!), while its norm has absolute value 1. Hence it requires exponential time in $\log |D|$ to write down the standard representation of η_K , and any algorithm using the standard representation of η_K has at least exponential running time in $\log |D|$. It is therefore desirable to have a shorter representation for elements of K with large height and small norm (in absolute value) and to be able to determine such a representation quickly. A representation of this type was first introduced by Buchmann, Thiel and Williams [2] in the case of real quadratic number fields. The object of this paper is to describe a similar representation in real quadratic congruence function fields and to show how to obtain and use it efficiently.

Theorem 1.1 (Main Theorem) *Let $\mathcal{O} = \mathcal{O}_\Delta$ be a quadratic order of K and let $\alpha \in \mathcal{O}$. A compact representation of α is a representation*

$$\alpha = \frac{\alpha_0}{A_0} \prod_{j=1}^l \left(\frac{\alpha_j}{A_j} \right)^{2^{l-j}} \quad (1.1)$$

where

$$a_0, \alpha_1, \dots, \alpha_l \in \mathcal{O}, \quad A_0, A_1, \dots, A_l \in k[x],$$

$$\begin{aligned}
H(\alpha_0) &\leq |N(\alpha)|, & H(\alpha_j) &\leq |\Delta|^{3/2} \text{ for } 1 \leq j \leq l, \\
|A_0| &< |\sqrt{\Delta}|, & |A_j| &< |\Delta| \text{ for } 1 \leq j \leq l, \\
l &\leq \max\{0, \log \deg H(\alpha) - \log \deg(\Delta) + 2\}, & \text{and} \\
\gamma_i &= \prod_{j=1}^i \left(\frac{\alpha_j}{A_j}\right)^{2^{i-j}} \in \mathcal{O} \text{ for } 1 \leq i \leq l.
\end{aligned}$$

The computation of a compact representation of α requires no more than $O(\max\{\deg(\Delta), \log \deg H(\alpha)\})$ arithmetic operations on polynomials in $k[x]$.

Note that

$$\deg(\alpha) = \deg\left(\frac{a_0}{A_0}\right) + \sum_{j=1}^l \deg\left(\frac{\alpha_j}{A_0}\right) 2^{l-j}.$$

The above equality resembles a binary representation of ordinary integers, except that the coefficients are not bits, but small integers.

Suppose that $\alpha_j = G_j + B_j\sqrt{\Delta}$ for $0 \leq j \leq l$ in (1.1), then $|G_j|, |B_j| \leq H(\alpha_j)$ ($0 \leq j \leq l$). Any polynomial $F \in k[x]$ requires $O(\deg(F) \log q) = O(\log |F|)$ bits of storage, so if the compact representation of α is stored as the vector

$$(\Delta, G_0, B_0, A_0, G_1, B_1, A_1, \dots, G_l, B_l, A_l) \in k[x]^{3l+4},$$

then it requires $O(\log |N(\alpha)| + \log \deg H(\alpha) \log |\Delta|)$ bits of storage. For example, for the fundamental unit η_K of K , we have $|N(\eta_K)| = 1$ and $\log \deg H(\eta_K) = \log R_K = O(\log |D|)$ (see (2.2) below), so any compact representation of η_K requires $O((\log |D|)^2)$ bits of storage, as opposed to up to $O(|\sqrt{D}|)$ for the standard representation.

Since the computation of compact representations involves algorithms on ideals, we give a brief introduction to the theory of reduced ideals in quadratic orders in the next section. Section 3 presents the algorithms required for computing compact representations and analyzes their running times. We show how to perform basic computations with compact representations in Section 4. Finally, we prove that three important decision problems concerning ideals belong to the complexity class NP, namely principal ideal testing, ideal equivalence, and the discrete logarithm problem for ideal classes.

2 Ideals

For an overview of the theory of continued fractions and reduced ideals in real quadratic congruence function fields, refer to [7], [8], and [9]. These sources discuss ideals in the ring of integers only, but the material can be extended to any quadratic order. For more on ideals in quadratic orders, see [5].

Let $\mathcal{O} = \mathcal{O}_\Delta$ be a fixed quadratic order. An (*integral \mathcal{O} -*)ideal \mathfrak{a} is an additive subgroup of \mathcal{O} such that $\alpha\mathfrak{a} \subseteq \mathfrak{a}$ for all $\alpha \in \mathcal{O}$. Every ideal in \mathcal{O} is a free $k[x]$ -submodule of \mathcal{O} of rank 2, and there exists a $k[x]$ -basis of \mathfrak{a} of the form $\{SQ, SP + S\sqrt{\Delta}\}$ where $S, Q, P \in k[x]$ and $Q \mid \Delta - P^2$. Write

$$\mathfrak{a} = S[Q, P + \sqrt{\Delta}] = k[x](SQ) + k[x](SP + S\sqrt{\Delta}).$$

A basis $\{SQ, SP + S\sqrt{\Delta}\}$ of an ideal \mathfrak{a} can be made unique up to constant factors if we replace P by the remainder of $P \pmod{Q}$ of least non-negative degree. In this case, if S and Q are chosen

to be monic, then we say that \mathfrak{a} is in *adapted form* with *adapted basis* $\{SQ, SP + S\sqrt{\Delta}\}$, where $Q \mid \Delta - P^2$, $\deg(P) < \deg(Q)$, and $\text{sgn}(S) = \text{sgn}(Q) = 1$. \mathfrak{a} is *primitive* if S in its basis can be chosen to be 1.

The *product* of two ideals \mathfrak{a} , \mathfrak{b} is the ideal $\mathfrak{a}\mathfrak{b}$ consisting of all finite sums of products $\alpha\beta$ where $\alpha \in \mathfrak{a}$ and $\beta \in \mathfrak{b}$. It is easy to determine a $k[x]$ -basis for $\mathfrak{a}\mathfrak{b}$ from $k[x]$ -bases for \mathfrak{a} and \mathfrak{b} , respectively, using Algorithm MULT given below. The *norm* of an ideal $\mathfrak{a} = S[Q, P + \sqrt{\Delta}]$ is the monic polynomial $N(\mathfrak{a}) = S^2Q/\text{sgn}(S^2Q)$. An ideal \mathfrak{a} is *principal* if it is of the form $\mathfrak{a} = (\alpha) = \alpha\mathcal{O}$ for some $\alpha \in \mathcal{O}$. α is a *generator* of \mathfrak{a} . In this case, $N(\mathfrak{a}) = N(\alpha)/\text{sgn}(N(\alpha))$. Two ideals \mathfrak{a} , \mathfrak{b} are *equivalent* if there exist non-zero $\alpha, \beta \in \mathcal{O}$ such that $(\alpha)\mathfrak{a} = (\beta)\mathfrak{b}$, or equivalently, if there exists $\lambda \in K^* = K \setminus \{0\}$ such that $\mathfrak{a} = \lambda\mathfrak{b}$. If \mathfrak{a} and \mathfrak{b} are equivalent ideals, then there exists $\gamma \in \mathfrak{a}$ such that $\gamma\mathfrak{a} = N(\mathfrak{b})\mathfrak{b}$ and $0 < |\gamma| \leq |N(\alpha)|$ (see [7], Lemma II.3.1). Ideal equivalence partitions the set of ideals in \mathcal{O} into equivalence classes which form a finite group under ideal multiplication, called the *class group* of \mathcal{O} . The order h'_Δ of the class group of \mathcal{O} is the *ideal class number* of \mathcal{O} . For the ideal class number h'_K of O_K and the regulator R_K , the following bounds hold (see [4], pp. 299-307).

$$(\sqrt{q} - 1)^{\deg(D)-2} \leq h'_K R_K \leq (\sqrt{q} + 1)^{\deg(D)-2}. \quad (2.2)$$

An ideal \mathfrak{a} in \mathcal{O} is *reduced* if \mathfrak{a} is primitive and there exists a $k[x]$ -basis $\{Q, P + \sqrt{\Delta}\}$ of \mathfrak{a} such that $|P - \sqrt{\Delta}| < |Q| < |P + \sqrt{\Delta}|$. Such a basis is a *reduced basis* of \mathfrak{a} and is unique up to constant factors. The following lemma summarizes properties of reduced ideals.

Lemma 2.1 1. Let $\mathfrak{a} = [Q, P + \sqrt{\Delta}]$ be a primitive ideal. Then \mathfrak{a} is reduced if and only if $|Q| = |N(\mathfrak{a})| < |\sqrt{\Delta}|$.

2. Let \mathfrak{a} be a reduced ideal with reduced basis $\{Q, P + \sqrt{\Delta}\}$. Then the following properties hold.

(a) $|P| = |P + \sqrt{\Delta}| = |\sqrt{\Delta}|$.

(b) $\text{sgn}(P) = \text{sgn}(\Delta)$. In fact, the two highest coefficients of P and $\sqrt{\Delta}$ are equal.

(c) If $a = \left\lfloor \frac{P + \sqrt{\Delta}}{Q} \right\rfloor$, then $|aQ| = |\sqrt{\Delta}|$. In particular, $1 < |a| \leq |\sqrt{\Delta}|$ and $1 \leq |Q| < |\sqrt{\Delta}|$.

Let $\mathfrak{a}_1 = [Q_0, P_0 + \sqrt{\Delta}]$ be a primitive ideal and consider the ideal sequence $(\mathfrak{a}_i)_{i \in \mathbb{N}}$ where

$$\mathfrak{a}_i = [Q_{i-1}, P_{i-1} + \sqrt{\Delta}] \quad (2.3)$$

is recursively defined as follows.

$$\begin{aligned} a_{i-1} &= \left\lfloor \frac{P_{i-1} + \sqrt{\Delta}}{Q} \right\rfloor \\ P_i &= a_{i-1}Q_{i-1} - P_{i-1} \\ Q_i &= \frac{\Delta - P_i^2}{Q_{i-1}} \end{aligned} \quad (i \in \mathbb{N}) \quad (2.4)$$

Here, the polynomials a_i ($i \in \mathbb{N}_0$) are exactly the partial quotients in the continued fraction expansion of $\alpha_0 = \frac{P_0 + \sqrt{\Delta}}{Q_0}$. The process of obtaining \mathfrak{a}_{i+1} from \mathfrak{a}_i ($i \in \mathbb{N}$) is called a *baby step*.

For $i \in \mathbb{N}$, define

$$\alpha_i = \frac{P_i + \sqrt{\Delta}}{Q_i}, \quad \theta_1 = 1, \quad \theta_{i+1} = \prod_{j=1}^i \frac{1}{\alpha_j}.$$

Then $\theta_{i+1} = \frac{1}{\alpha_i} \theta_i$ where $\frac{1}{\alpha_i} = \frac{\sqrt{\Delta} - P_i}{Q_{i-1}}$ for $i \in \mathbb{N}$ by (2.4), and the following properties hold.

Lemma 2.2 For $i \in \mathbb{N}$:

1. $\theta_{i+1}Q_0, \bar{\theta}_{i+1}Q_0 \in \mathfrak{a}_1$.
2. $\mathfrak{a}_{i+1} = \bar{\theta}_{i+1}\mathfrak{a}_1 = \frac{\sqrt{\Delta} + P_i}{Q_{i-1}}\mathfrak{a}_1$. In particular, all \mathfrak{a}_j ($j \in \mathbb{N}$) are equivalent.
3. $\theta_{i+1}\bar{\theta}_{i+1} = (-1)^i \frac{Q_i}{Q_0}$, so $\deg(\bar{\theta}_{i+1}) = \deg(Q_i) - \deg(Q_0) + \sum_{j=1}^i \deg(a_j)$.
4. $\deg(\bar{\theta}_{i+1}) = \deg(\bar{\theta}_i) + \deg(a_{i-1})$ for $i \geq 2$.
5. $\theta_{i+1} = (-1)^i \frac{G_{i-1} - B_{i-1}\sqrt{\Delta}}{Q_0}$ where $B_{-2} = 1, B_{-1} = 0, B_{j-1} = a_{j-1}B_{j-2} + B_{j-3}$ for $1 \leq j \leq i$, and $G_{i-1} = P_i B_{i-1} + Q_i B_{i-2}$.

Lemma 2.3 Let $\mathfrak{a} = [Q, P + \sqrt{\Delta}]$ be a primitive ideal and let $\mathfrak{a} = \mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3, \dots$ be the sequence of ideals given by (2.3) and (2.4).

1. \mathfrak{a}_i is reduced for $i > \max\{1, \deg(Q_0)/2 - \deg(\Delta)/4 + 2\}$.
2. If \mathfrak{a}_j is reduced for some $j \in \mathbb{N}$, then \mathfrak{a}_i is reduced for all $i \geq j$ and the reduced basis of \mathfrak{a}_i is given by (2.3) and (2.4).
3. Suppose \mathfrak{a}_j is reduced for some $j \in \mathbb{N}$. Then the sequence $(\mathfrak{a}_i)_{i \geq j}$ is purely periodic, i.e. there exists $m \in \mathbb{N}$ such that $\mathfrak{a}_{i+m} = \mathfrak{a}_i$ for all $i \geq j$. Furthermore, the entire collection of distinct reduced ideals in the ideal class of \mathfrak{a} is finite and is given by $\{\mathfrak{a}_j, \mathfrak{a}_{j+1}, \dots, \mathfrak{a}_{j+m-1}\}$.

Suppose $\mathfrak{a}_1 = \mathcal{O}$, then $\mathfrak{a}_i = (\bar{\theta}_i)$ is a reduced principal ideal for $i \in \mathbb{N}$. The distance of \mathfrak{a}_i is

$$\delta_i = \delta(\mathfrak{a}_i) = \deg(\bar{\theta}_i).$$

Then

$$\delta_1 = 0, \quad \delta_i = \frac{1}{2} \deg(\Delta) + \sum_{j=1}^{i-2} \deg(a_j) \text{ for } i \geq 2,$$

$$\delta_{i+1} = \delta_i + \deg(a_{i-1}) \geq i, \quad 1 \leq \delta_{i+1} - \delta_i \leq \frac{1}{2} \deg(\Delta) \text{ for } i \in \mathbb{N}.$$

Note that ideal distances are integers (as opposed to irrational numbers in the number field case), so we need not resort to rational approximations here. This means that it is somewhat easier and faster to compute compact representations in quadratic function fields than it is to obtain them in quadratic number fields.

For any $s \in \mathbb{N}_0$, there exists a unique reduced principal ideal \mathfrak{a}_k such that $\delta_k \leq s < \delta_{k+1}$. We say that \mathfrak{a}_k is the reduced principal ideal below s and write $\mathfrak{a}_k = \mathfrak{a}(s)$. For $i \in \mathbb{N}$, $\mathfrak{a}_i = \mathfrak{a}(s)$ if and only if $\delta_i \leq s < \delta_i + \deg(\Delta)/2$.

3 Algorithms

Let $s \in \mathbb{N}$. The key ingredient for computing compact representations is a fast algorithm for determining from the reduced principal ideal $\mathfrak{a}(s)$ below s the ideal $\mathfrak{a}(2s)$. It is possible to find $\mathfrak{a}(2s)$ by repeatedly applying (2.4), starting at $\mathfrak{a}_1 = \mathfrak{a}(s)$, but this could require as many as s baby steps and is very inefficient for large values of s . Instead, we apply the following method which achieves our goal much faster.

Let $\mathfrak{a} = \mathfrak{a}(s)$. Compute the primitive principal ideal \mathfrak{c} where $S\mathfrak{c} = \mathfrak{a}^2$, using the algorithm *SQUARE* given below. \mathfrak{c} is generally not reduced, but by Lemma 2.3, part 1, we can find a reduced principal ideal $\mathfrak{r} = \alpha\mathfrak{c} = (\alpha/S)\mathfrak{a}^2$ after approximately $\deg(\Delta)/2$ many baby steps. The process of computing \mathfrak{r} from \mathfrak{a} is a *giant step*. \mathfrak{r} is “not too far” below $2s$ but it need not be immediately below $2s$, so we continue to perform baby steps until $\mathfrak{a}(2s)$ is reached, which will happen after $O(\deg(\Delta))$ many more baby steps. This is another difference between our setting and the number field case, where it may happen in rare cases that in computing \mathfrak{r} , we might have “overshot” our target ideal $\mathfrak{a}(2s)$ and thus need to perform “backward” baby steps in order to reach $\mathfrak{a}(2s)$. In quadratic number fields, one needs to check for this possibility after each giant step.

Before we give a more detailed description and analysis of the required algorithms, a note on running times. We measure the time complexity of our algorithms in terms of polynomial operations over $k = \mathbb{F}_q$ (additions, subtractions, multiplications, divisions with remainder, degree comparisons, and assignments).

Our first two algorithms are a method for multiplying two reduced ideals (see for example Algorithm II.2.1 in [7] or Section 7 in [8]) and its special case of squaring a reduced ideal, the only situation required for computing compact representations. They are followed by ideal reduction (see Algorithm II.4.1 in [7] or Section 8 in [8]) and a technique of “doubling” the ideal $\mathfrak{a}(s)$ below some $s \in \mathbb{N}$ to obtain $\mathfrak{a}(2s)$.

Algorithm *MULT*

Input: Two reduced ideals $\mathfrak{a} = (Q_a, P_a)$, $\mathfrak{b} = (Q_b, P_b)$.

Output: (\mathfrak{c}, S) where $\mathfrak{c} = [Q, P + \sqrt{\Delta}]$ is a primitive ideal, $S \in k[x]$, and $S\mathfrak{c} = \mathfrak{a}\mathfrak{b}$.

Algorithm:

1. $S_1 := \gcd(Q_a, Q_b) \equiv: X_1 Q_a \pmod{Q_b}$ ($S_1, X_1 \in k[x]$).
2. $S := \gcd(S_1, P_a + P_b) \equiv: X_2 S_1 + Y_2 (P_a + P_b)$ ($S, X_2, Y_2 \in k[x]$).
(If $S_1 = 1$, then set $X_2 := 1$, $Y_2 := 0$, $S := 1$).
3. $Q := \frac{Q_a Q_b}{S^2}$.
4. $P \equiv: P_a + \frac{Q_a}{S} \left(X_2 X_1 (P_b - P_a) + Y_2 \frac{D - P_a^2}{Q_a} \right) \pmod{Q}$.

Lemma 3.1 *Algorithm *MULT* is correct and performs $O(\deg \Delta)$ polynomial operations. Furthermore, $|S| < \sqrt{\Delta}$, $|P| < |Q| < |\Delta|$.*

Algorithm *SQUARE*

Input: A reduced ideal $\mathfrak{a} = [Q, P + \sqrt{\Delta}]$.

Output: (\mathfrak{c}, S) where $\mathfrak{c} = [Q', P' + \sqrt{\Delta}]$ is a primitive ideal, $S \in k[x]$, and $S\mathfrak{c} = \mathfrak{a}^2$.

Algorithm:

1. $S := \gcd(P, Q) \equiv: YP \pmod{Q}$ ($Y \in k[x]$).
2. $Q' := \left(\frac{Q}{S}\right)^2$.
3. $P' \equiv: P + Y \frac{\Delta - P^2}{Q} \pmod{Q'}$.

Algorithm REDUCE

Input: A primitive ideal $\mathfrak{a} = [Q, P + \sqrt{\Delta}]$ in adapted form.

Output: (\mathfrak{b}, λ) where $\mathfrak{b} = \lambda\mathfrak{a} = [Q', P' + \sqrt{\Delta}]$ is reduced and $\lambda = \frac{G + B\sqrt{\Delta}}{Q} \in K$ ($G, B \in k[x]$).

Algorithm:

1. $j := 0$, $P_0 := P$, $Q_0 := Q$, $B_{-2} := 1$, $B_{-1} := 0$.
2. While $\deg(Q_j) \geq \deg(\Delta)/2$ do { baby steps }

$$a_{j-1} := \left\lfloor \frac{P_{j-1} + \sqrt{\Delta}}{Q_{j-1}} \right\rfloor, \quad P_j := a_{j-1}Q_{j-1} - P_{j-1}, \quad Q_j := \frac{\Delta - P_j^2}{Q_{j-1}},$$

$$B_{j-1} := a_{j-1}B_{j-2} + B_{j-3}.$$
3. $Q' := Q_j$, $P' := P_j$, $\mathfrak{b} := [Q', P' + \sqrt{\Delta}]$, $B := B_{j-1}$,

$$G := P_j B_{j-1} + Q_j B_{j-2}, \quad \lambda = \frac{G + B\sqrt{\Delta}}{Q}.$$

Lemma 3.2 *Algorithm REDUCE is correct and performs $O(\deg \Delta)$ polynomial operations. Furthermore, $|Q_j|, |P_j| \leq |Q_0|$, $|B_{j-2}| < |B_{j-1}| < |Q_0|/|\sqrt{\Delta}|$ throughout the algorithm, and $H(\lambda) \leq 1$.*

Proof: By Lemma 8.5 of [8], \mathfrak{b} is reduced and $|\bar{\lambda}| \leq 1$, hence $H(\lambda) \leq 1$ as $|\lambda| < 1$ always holds. Suppose the algorithm stops after l iterations of step 2, i.e. $\mathfrak{b} = \mathfrak{a}_{l+1}$. Then $|B_{j-2}| < |B_{j-1}|$ follows from $|a_{j-1}| > 1$ ($1 \leq j \leq l$). Using techniques similar to those employed in the proofs of Theorem 4.1, Corollary 4.1.1 and Theorem 4.2 of [10], we can show that $|Q_j|, |P_j| \leq |Q_0|$ for $0 \leq j \leq l$ and $|B_{l-1}| \leq |Q_0|/|\sqrt{\Delta}|$. \diamond

Algorithm DOUBLE

Input: $s \in \mathbb{N}$, $\mathfrak{a}(s) = [Q, P + \sqrt{\Delta}]$, $\delta = \delta(\mathfrak{a}(s))$.

Output: $\mathfrak{a}(2s) = [Q', P' + \sqrt{\Delta}] = \frac{\alpha}{A}\mathfrak{a}(s)^2$ where $\alpha = G + B\sqrt{\Delta}$ ($G, B, A \in k[x]$), $\delta(\mathfrak{a}(2s))$.

Algorithm:

1. $(\mathfrak{c}, S) := \text{SQUARE}(\mathfrak{a}(s))$, $\mathfrak{c} = [Q_c, P_c + \sqrt{\Delta}]$.

2. (a) $j := 0$, $P_0 := P$, $Q_0 := Q$, $B_{-2} := 1$, $B_{-1} := 0$,
 $d_2 := 2\delta - \deg(S) - \deg(Q_0)$.
- (b) While $\deg(Q_j) \geq \deg(\Delta)/2$ do { baby steps }
Increment j by 1;
 $a_{j-1} := \left\lfloor \frac{P_{j-1} + \sqrt{\Delta}}{Q_{j-1}} \right\rfloor$, $P_j := a_{j-1}Q_{j-1} - P_{j-1}$, $Q_j := \frac{\Delta - P_j^2}{Q_{j-1}}$;
 $B_{j-1} := a_{j-1}B_{j-2} + B_{j-3}$, $d_{j+1} := d_j + \deg(a_{j-1})$.
3. While $d_{j+1} + \deg(Q_j) \leq 2s$ do { more baby steps }
Increment j by 1;
 $a_{j-1} := \left\lfloor \frac{P_{j-1} + \sqrt{\Delta}}{Q_{j-1}} \right\rfloor$, $P_j := a_{j-1}Q_{j-1} - P_{j-1}$, $Q_j := \frac{\Delta - P_j^2}{Q_{j-1}}$;
 $B_{j-1} := a_{j-1}B_{j-2} + B_{j-3}$, $d_{j+1} := d_j + \deg(a_{j-1})$.
4. $Q' := Q_j$, $P' := P_j$, $\mathfrak{a}(2s) := [Q', P' + \sqrt{\Delta}]$,
 $\delta(\mathfrak{a}(2s)) := d_{j+1} + \deg(Q_j)$,
 $B := B_{j-1}$, $G := P_j B_{j-1} + Q_j B_{j-2}$, $\alpha := G + B\sqrt{\Delta}$, $A := \frac{Q^2}{S}$.

Theorem 3.3 *Algorithm DOUBLE is correct and performs $O(\deg \Delta)$ polynomial operations. Furthermore, $|P_j|, |Q_j| < |\Delta|$ throughout step 2, $|P_j|, |Q_j| < |\sqrt{\Delta}|$ throughout step 3, $2s - 2\deg(\Delta) < d_j < d_{j+1} < 2s + \deg(\Delta)/2$ and $1 \leq |B_{j-2}| < |B_{j-1}| < |\Delta|^{3/2}$ throughout steps 2 and 3, $|G| < |\Delta|^2$, so $H(\alpha) < |\Delta|^2$, and $|A| < |\Delta|$.*

Proof: Step 1 is correct and requires $O(\deg \Delta)$ polynomial operations, and $|S| < |\sqrt{\Delta}|$, $|P_c|, |Q_c| < |\Delta|$ by Lemma 3.1. Let $\mathfrak{a}_{m+1} = [Q_m, P_m + \sqrt{\Delta}]$ be the ideal computed at the end of step 2. Then \mathfrak{a}_{m+1} is reduced and the bounds for $|P_j|$ and $|Q_j|$ ($0 \leq j \leq m$) follow from Lemma 3.2.

Now it is known (see Theorem 9.2 in [8]) that if $\mathfrak{a}_0 = \mathfrak{c}$, then $\mathfrak{a}_{m+1} = \bar{\theta}_{m+1}\mathfrak{c} = (\bar{\theta}_{m+1}/S)\mathfrak{a}(s)^2$ where $2 - \deg(\Delta) \leq \deg(\bar{\theta}_{m+1}/S) \leq 0$, so $2\delta + 2 - \deg(\Delta) \leq \delta_{m+1} \leq 2\delta \leq 2s$. Hence, unless \mathfrak{a}_{m+1} is already the ideal below $2s$, more baby steps are required to increase δ_{m+1} and compute $\mathfrak{a}(2s)$. This is done in step 3.

Assume the algorithm halts at index $j = l$, i.e. the last ideal computed in step 3 is \mathfrak{a}_{l+1} . Then the ideals $\mathfrak{a}_{m+2}, \mathfrak{a}_{m+3}, \dots, \mathfrak{a}_{l+1}$ are reduced, whence follow the bounds on $|P_j|$ and $|Q_j|$ for $m+1 \leq j \leq l$. Furthermore, since $\delta \geq s - \deg(\Delta)/2$, we have $2s - 2\deg(\Delta) < d_2 \leq d_j < d_j + \deg(a_{j-1}) = d_{j+1} \leq d_{m+1} \leq 2s + \deg(Q_m) < 2s + \deg(\Delta)/2$ for $2 \leq j \leq m$. Now $|B_{j-2}| < |B_{j-1}| \leq |B|$ for $0 \leq j \leq m-1$ and $|G| < |B||\sqrt{\Delta}|$. Since $\mathfrak{a}_{l+1} = \frac{G_{l-1} + B_{l-1}\sqrt{\Delta}}{Q_0}\mathfrak{c}$ by Lemma 2.2, part 5, we have $\alpha = B_{l-1} + G_{l-1}\sqrt{\Delta}$ and $A = SQ_0 = Q^2/S$ by step 2 of Algorithm SQUARE. Then $|A| \leq |Q|^2 < |\Delta|$ and

$$\begin{aligned}
\delta_{j+1} &= \deg(\bar{\theta}_{j+1}) - \deg(S) + 2\delta \\
&= \deg(Q_j) - \deg(Q_0) + \sum_{i=1}^j \deg(a_i) - \deg(S) + 2\delta \\
&= \deg(Q_j) + \sum_{i=1}^j \deg(a_i) + d_2 = \deg(Q_j) + d_{j+1},
\end{aligned}$$

hence the algorithm stops when j is maximal such that $\delta_{j+1} \leq 2s$, so $\mathfrak{a}(2s) = \mathfrak{a}_{l+1}$. Therefore, $\deg(\alpha/A) = \delta_{l+1} - 2\delta \leq 2(s - \delta) < \deg(\Delta)$ and $|\alpha| < |A||\Delta| < |\Delta|^2$. On the other hand, $\deg(\alpha/A) > \delta_{l+1} - \deg(\Delta)/2 - 2\delta > 2(s - \delta) - \deg(\Delta)/2 > -\deg(\Delta)/2$, so $|\alpha| \geq |\alpha|/|A| > 1/\sqrt{|\Delta|}$. But

$$\frac{|\alpha||\bar{\alpha}|}{|A|^2} = \frac{|Q_l|}{|Q_0||S|^2} = \frac{|Q_l|}{|Q|^2} = \frac{|Q_l|}{|S||A|},$$

so $|\bar{\alpha}| \leq |A||Q_l|/|\alpha| < |\Delta|^2$. Therefore, $|G| < |\Delta|^2$, $|B| < |\Delta|^{3/2}$, and $H(\alpha) < |\Delta|^2$. \diamond

In order to determine a compact representation for an element $\alpha \in \mathcal{O}$, we first need to compute a $k[x]$ -basis for the principal ideal generated by α .

Algorithm IDEAL

Input: $\alpha = A + B\sqrt{\Delta} \in \mathcal{O} \setminus \{0\}$ in standard representation ($A, B \in k[x]$).

Output: $\mathfrak{a} = (\alpha) = S[Q, P + \sqrt{\Delta}]$ ($S, Q, P \in k[x]$, $Q \mid \Delta - P^2$).

Algorithm:

1. $S := \gcd(A, B) = XA + YB$, ($X, Y \in k[x]$).

2. $P := Y\frac{A}{S} + X\Delta\frac{B}{S}$, $Q := \frac{A^2 - B^2\Delta}{S^2} = \frac{N(\alpha)}{S^2}$.

Lemma 3.4 *Algorithm IDEAL is correct and performs $O(\max\{\deg(A), \deg(B)\})$ polynomial operations.*

Proof: Let $\mathfrak{a} = S[Q, P + \sqrt{\Delta}]$ where S, Q , and P are computed by the algorithm. We need to show that $\mathfrak{a} = (\alpha)$. We have

$$\begin{aligned} S^2 \left(XQ + \frac{B}{S}(P + \sqrt{\Delta}) \right) &= X(A^2 - B^2\Delta) + B(YA + XB\Delta + S\sqrt{\Delta}) \\ &= XA^2 + YAB + SB\sqrt{\Delta} \\ &= A(XA + YB) + SB\sqrt{\Delta} \\ &= S(A + B\sqrt{\Delta}) \\ &= S\alpha, \end{aligned}$$

so $\alpha = S \left(XQ + \frac{B}{S}(P + \sqrt{\Delta}) \right) \in \mathfrak{a}$. Conversely, $SQ = \frac{\bar{\alpha}}{S}\alpha \in (\alpha)$ and

$$\begin{aligned} S(P + \sqrt{\Delta}) &= (YA + X\Delta B) + (XA + YB)\sqrt{\Delta} \\ &= (Y + X\sqrt{\Delta})(A + B\sqrt{\Delta}) \\ &= (Y + X\sqrt{\Delta})\alpha \in (\alpha). \end{aligned}$$

Finally, $N(P + \sqrt{\Delta}) = N(Y + X\sqrt{\Delta})N(\alpha/S)$ or $P^2 - \Delta = (Y^2 - X^2\Delta)Q$, so $Q \mid \Delta - P^2$ and $\{SQ, SP + S\sqrt{\Delta}\}$ is a $k[x]$ -basis of (α) . \diamond

We are now prepared to provide the algorithm for computing compact representations. Given $\alpha \in \mathcal{O}$, we determine a $k[x]$ -basis of (α) , using the algorithm *IDEAL*, before calling the algorithm described below.

Algorithm COMPACT-REPRESENTATION

Input: A non-zero principal ideal $\mathfrak{a} = (\alpha) = S[Q, P + \sqrt{\Delta}]$ ($S, Q, P \in k[x]$, $Q \mid \Delta - P^2$, $\alpha \in \mathcal{O}$).

Output: $l \in \mathbb{N}$, $\alpha_0, \alpha_1, \dots, \alpha_l \in \mathcal{O}$, $A_0, A_1, \dots, A_l \in k[x]$ such that

$$\alpha = \frac{\alpha_0}{A_0} \prod_{j=1}^l \left(\frac{\alpha_j}{A_j} \right)^{2^{l-j}}$$

is a compact representation of α .

Algorithm:

1. $(\mathfrak{b}, \gamma) := \text{REDUCE} \left(\frac{1}{S} \mathfrak{a} \right)$, $\mathfrak{b} = [Q', P' + \sqrt{\Delta}]$.
2. $l := \min \left\{ j \in \mathbb{N}_0 \mid 2^{j-1} > \frac{\deg(\rho)}{\deg(\Delta)} \right\}$, $s_0 := \frac{\deg(\rho)}{2^l}$ where $\rho = \gamma \frac{\alpha}{S}$;
 $\mathfrak{a}(s_0) := \mathcal{O}$, $A_0 := Q'$, $\alpha_0 := \bar{\gamma} Q S$, $\epsilon_0 := 1$.
3. For $j := 1$ to l do

$$\begin{aligned} s_j &:= 2s_{j-1} \\ (\alpha_j, A_j, \mathfrak{a}(s_j)) &:= \text{DOUBLE}(\mathfrak{a}(s_{j-1})) \\ \epsilon_j &:= \text{sgn} \left(\frac{\alpha_j}{A_j} \right) \epsilon_{j-1}^2 \end{aligned}$$

4. Replace α_0 by $\epsilon^{-1} \text{sgn}(\alpha) \alpha_0$ where $\epsilon = \text{sgn} \left(\frac{\alpha_0}{A_0} \right) \epsilon_l$.

Theorem 3.5 *Algorithm COMPACT-REPRESENTATION is correct and performs $O(\max\{\deg(\Delta), \log \deg H(\alpha)\})$ polynomial operations.*

Proof: We have $\mathfrak{b} = (\gamma\alpha/S) = (\rho)$, so $\rho \in \mathcal{O}$. By Lemma 2.2, part 3, we have $\gamma\bar{\gamma} = \pm Q'/Q$, so $S/\gamma = \pm SQ\bar{\gamma}/Q' = \pm \alpha_0/A_0$. Hence there exists $c \in k^*$ such that $\alpha = c\rho\alpha_0/A_0$. Furthermore, since $H(\gamma) \leq 1$ by Lemma 3.2, we have $H(\alpha_0) = |S||Q|H(\gamma) \leq |S||Q| = |N(\alpha)|/|S| \leq |N(\alpha)|$ and $|A_0| = |Q'| < \sqrt{\Delta}$.

If $l = 0$, then $\deg(\rho) < \deg(\Delta)/2$, so since $\mathfrak{b} = (\rho)$ is a reduced ideal with distance $\delta(\mathfrak{b}) = \deg(\rho)$, we must have $(\rho) = \mathcal{O}$, $\rho \in k^*$, the loop in step 4 is never executed, and $\rho\alpha_0/A_0$ is the compact representation of α up to sign.

Suppose $l \geq 1$, then $2^{l-1} > \deg(\rho)/\deg(\Delta) \geq 2^{l-2}$, so $\deg(\Delta)/2 > s_0 \geq \deg(\Delta)/4 \geq 0$. We have $\delta(\mathcal{O}) = 0 \leq s_0 < \delta(\mathcal{O}) + \deg(\Delta)/2$, so setting $\mathfrak{a}(s_0)$ to be \mathcal{O} in step 2 is correct. Let $\gamma_0 = 1$, $\gamma_j = (\alpha_j/A_j)\gamma_{j-1}^2$ for $1 \leq j \leq l$. Then

$$\gamma_j = \prod_{i=1}^j \left(\frac{\alpha_i}{A_i} \right)^{2^{j-i}}, \quad \mathfrak{a}(s_j) = (\gamma_j) \quad (0 \leq j \leq l),$$

hence $\gamma_j \in \mathcal{O}$ for $0 \leq j \leq l$. By Theorem 3.3, $H(\alpha_j) < |\Delta|^2$ and $|A_j| < |\Delta|$. Furthermore, since (ρ) is the reduced principal ideal below $\deg(\rho) = s_l$, we have $(\rho) = \mathfrak{a}(s_l) = (\gamma_l)$, so α and $(\alpha_0/A_0)\gamma_l$ differ only in sign. Now $\epsilon_j = \text{sgn}(\gamma_j)$ for $0 \leq j \leq l$, so after step 4, the compact representation of α has the correct sign.

Finally, if $l \geq 1$, then $l \leq \log \deg(\rho) - \log \deg(\Delta) + 2$, and since $|\rho| \leq H(\rho) \leq H(\gamma)H(\alpha)/|S| \leq H(\alpha)$, we have $l \leq \max\{0, \log \deg H(\alpha) - \log \deg(\Delta) + 2\}$, and step 4 requires $O(\log \deg H(\alpha))$ many doubling steps. \diamond

4 Applications

Lemma 4.1 *Let $\alpha \in \mathcal{O} \setminus \{0\}$ be given in compact representation. Using no more than $O(\max\{\deg(\Delta), \log \deg H(\alpha)\})$ polynomial operations, we can compute*

1. *a compact representation of $\bar{\alpha}$,*
2. *the degree of α ,*
3. *the sign of α ,*
4. *a $k[x]$ -basis of the principal ideal (α) ,*
5. *the norm of α .*

If $\beta \in \mathcal{O} \setminus \{0\}$ is also given in compact representation, we can

6. *compute a compact representation of $\alpha\beta$,*
7. *determine whether β divides α and if yes, compute a compact representation of α/β ,*
8. *determine whether $\alpha = \beta$.*

using no more than $O(\max\{\deg(\Delta), \log \deg H(\alpha), \log \deg H(\beta)\})$ polynomial operations.

Proof: 1-3 is obvious. For 4, write $\alpha = (\alpha_0/A_0)\rho$. Use step 3 of algorithm *COMPACT-REPRESENTATION* to successively compute $k[x]$ -bases of the ideals $\mathfrak{a}(s_0), \mathfrak{a}(s_1), \dots, \mathfrak{a}(s_l) = (\rho)$. Then compute $\mathfrak{b} = IDEAL(\alpha_0)$. Finally, use Algorithm *MULT* to compute a $k[x]$ -basis $\{SQ, SP + S\sqrt{\Delta}\}$ for the ideal $(\rho)\mathfrak{b}$. Then $A_0(\alpha) = (\rho)\mathfrak{b}$, so A_0 must divide S . Hence $(\alpha) = (S/A_0)[Q, P + \sqrt{\Delta}]$. In 5, to obtain $N(\alpha)$, compute $\alpha(s_0), \dots, \alpha(s_l)$ as before. If $\mathfrak{a}(s_l) = S[Q, P + \sqrt{\Delta}]$, then $N(\alpha)$ is equal to $N(\alpha_0)QS^2/N(A_0)$ up to sign.

For 6-8, compute $k[x]$ -bases $\{SQ, SP + S\sqrt{\Delta}\}$ and $\{S'Q', S'P' + S'\sqrt{\Delta}\}$ of (α) and (β) , respectively. To obtain a compact representation of the product $\alpha\beta$, compute a $k[x]$ -basis of the ideal $(\alpha\beta)$ using Algorithm *MULT* and apply Algorithm *COMPACT-REPRESENTATION* to this basis. Then match the sign of the compact representation to be equal to $\text{sgn}(\alpha\beta) = \text{sgn}(\alpha)\text{sgn}(\beta)$. To compute a compact representation of the quotient, observe that $(\bar{\beta}) = S'[Q', -P' + \sqrt{\Delta}]$. Use Algorithm *MULT* to compute a $k[x]$ -basis of the product ideal $(\alpha\bar{\beta})$, say $(\alpha\bar{\beta}) = S''[Q'', P'' + \sqrt{\Delta}]$. Now $\beta \mid \alpha$ if and only if $N(\beta) \mid \alpha\bar{\beta}$. Since the ideal $[Q'', P'' + \sqrt{\Delta}]$ is primitive, this happens if and only if $Q'S''^2 \mid S''$. Check whether this is true. If yes, apply Algorithm *COMPACT-REPRESENTATION* to the ideal $(\alpha/\beta) = (S''/Q'S''^2)[Q'', P'' + \sqrt{\Delta}]$ and again, match the sign to be equal to that of α/β . Finally, for 8, note that $\alpha = \beta$ if and only if $\text{sgn}(\alpha) = \text{sgn}(\beta)$, $\beta \mid \alpha$, and $\deg(\alpha) = \deg(\beta)$. \diamond

Henceforth, we only consider the case $\mathcal{O} = \mathcal{O}_K$, i.e. $\Delta = D$.

Lemma 4.2 *Every principal ideal in \mathcal{O}_K has a generator α such that $\deg H(\alpha) \leq \max\{(\sqrt{q} + 1)^{\deg(D)-2}, \deg N(\alpha)\}$.*

Proof: Clear for the zero ideal. Let \mathfrak{a} be a non-zero principal ideal with a generator β with $|\beta| \geq 1$. There exists $m \in \mathbb{Z}$ such that $0 \leq \deg(\beta) + mR_K < R_K$. Then $\alpha = \beta\eta_K^m$ is also a generator of \mathfrak{a} and $\deg(\alpha) < R_K \leq (\sqrt{q} + 1)^{\deg(D)-2}$ by (2.2). Furthermore, since $\bar{\alpha} = N(\alpha)/\alpha$, we have $\deg(\bar{\alpha}) \leq \deg N(\alpha)$. \diamond

We conclude with an investigation of three important computational questions regarding ideals. Recall that a decision problem is said to belong to the class NP if and only if a certificate for the problem can be verified in time polynomial to the size of the input.

Theorem 4.3 *The following problems belong to NP.*

(PIT) *Principal Ideal Testing.*

Instance: An ideal \mathfrak{a} in \mathcal{O}_K , given in adapted form.

Question: Is \mathfrak{a} principal?

(EI) *Ideal Equivalence.*

Instance: Two ideals $\mathfrak{a}, \mathfrak{b}$ in \mathcal{O}_K , given in adapted form.

Question: Are \mathfrak{a} and \mathfrak{b} equivalent?

(DLP) *Discrete Logarithm Problem for Ideal Classes.*

Instance: Two ideals $\mathfrak{a}, \mathfrak{b}$ in \mathcal{O}_K , given in adapted form.

Question: Are \mathfrak{a}^l and \mathfrak{b} equivalent for some $l \in \mathbb{N}_0$.

Proof: The size of an ideal $\mathfrak{a} = S[Q, P + \sqrt{D}]$ in \mathcal{O}_K is linear in $\log |S|$, $\log |Q|$, $\log |P|$, and $\log |D|$. By Lemma 4.2, there exist a generator α of \mathfrak{a} such that $\deg H(\alpha) \leq \max\{|D|, \deg(QS^2)\}$.

For (PIT), a compact representation of such a generator α of \mathfrak{a} is a certificate, as its size is polynomially bounded by $\log |N(\alpha)| = \log |QS^2|$, $\log |D|$, and $l \leq \max\{\log |D|, \log \deg(QS^2)\}$. Simply compute the adapted representation of the ideal (α) as in Lemma 4.1, part 4, and compare it with the basis of \mathfrak{a} .

For (EI), an element $\gamma \in \mathfrak{a}$ given in compact representation such that $\gamma\mathfrak{a} = N(\mathfrak{b})\mathfrak{b}$ and $0 < |\gamma| \leq |N(\mathfrak{a})|$ represents a certificate. First, find a $k[x]$ -basis of the ideal (γ) . From this basis and the basis for \mathfrak{a} , compute an adapted $k[x]$ -basis for the ideal $(\gamma)\mathfrak{a}$ and compare it with the adapted basis of $N(\mathfrak{b})\mathfrak{b}$.

Finally, a *discrete logarithm*, i.e. a pair $(\gamma, l) \in \mathfrak{a} \times \{0, 1, \dots, h'_K - 1\}$ such that $\gamma\mathfrak{a}^l = N(\mathfrak{b})\mathfrak{b}$ and $0 < |\gamma| \leq |N(\mathfrak{a})|$ is a certificate. By (2.2), the size of l is bounded by $\log |D|$. Using a technique analogous to the repeated squaring method used for exponentiation of integers (see for example [6], p. 442), we can compute an adapted $k[x]$ -basis of the ideal \mathfrak{a}^l , using no more than $O(\log l)$ ideal multiplications and squarings. Then we proceed in a fashion similar to (EI). \diamond

References

- [1] Artin, E.: Quadratische Körper im Gebiete der höheren Kongruenzen I, II. *Math. Zeitschr.* **19** (1924) 153–206
- [2] Buchmann, J. A., Thiel, C., Williams, H. C.: Short representation of quadratic integers. *Computational Algebra and Number Theory*, A. van der Poorten and W. Bosma (ed.), *Mathematics and Its Applications*, **325**, Dordrecht/Boston/London (1995), 159–186
- [3] Deuring, M.: *Lectures on the Theory of Algebraic Functions of One Variable. Lecture Notes in Mathematics* **314**, Berlin 1973
- [4] Eichler, M.: *Introduction to the Theory of Algebraic Numbers and Functions*. Academic Press, New York (1966)
- [5] Hayes, D. R.: Real quadratic function fields. *Canadian Mathematical Society Conference Proceedings* **7**, (1987), 203–236.
- [6] Knuth, D. E.: *The Art of Computer Programming*, vol. 2: *Seminumerical Algorithms*, Addison-Wesley, Reading (Mass.) (1981)

- [7] Stein, A.: *Baby step-Giant step-Verfahren in reell-quadratischen Kongruenzfunktionenkörpern mit Charakteristik ungleich 2*. Diplomarbeit, Universität des Saarlandes, Saarbrücken (1992)
- [8] Stein, A., Williams, H. C.: Baby step giant step in real quadratic function fields. *Unpublished Manuscript*
- [9] Weis, B., Zimmer, H. G.: Artin's Theorie der quadratischen Kongruenzfunktionenkörper und ihre Anwendung auf die Berechnung der Einheiten- und Klassengruppen. *Mitt. Math. Ges. Hamburg, Sond. XII*, 2 (1991) 261–286
- [10] Stephens, A. J., Williams, H. C.: Some computational results on a problem concerning powerful numbers. *Math. Comp.*, **50** (1988) 619–632