Decision Problems in Quadratic Function Fields of High Genus

R. Scheidler
Department of Mathematical Sciences
University of Delaware
Newark DE 19716, USA
scheidle@math.udel.edu

May 3, 2000

Abstract

This paper provides verification procedures for a number of decision problems in quadratic function fields of odd characteristic, thereby establishing membership of these problems in both NP and co-NP. The problems include determining the ideal and divisor class numbers of the field, the regulator of the field (in the real case), a generating system of the ideal class group, a basis of the ideal class group, the pricipality of an ideal, the equivalence of two ideals, the discrete logarithm of an ideal class with respect to another ideal class, and the order of a class in the ideal class group. While several of these problems belong to the aforementioned complexity classes unconditionally, others require a certain assumption to ensure that the verification procedures can be done in polynomial time; so far, this assumption has only been verified for fields of high genus.

1 Introduction

A number of invariants of quadratic function fields, such as the ideal and divisor class number and, in the real case, the regulator, can currently only be determined in exponential or, at best, subexponential time (see [1, 2, 16]). The same is true for certain computations involving ideals in quadratic function fields, such as extracting discrete logarithms in the ideal class group and, in the real setting, finding a generator of a principal ideal. It is therefore natural to pose the following question: Suppose an all-knowing entity (or number theorist) provides a candidate for one of these quantities, how difficult is it to verify the correctness (or falseness if the number theorist is mean-spirited) of this answer? A number of analogous problems in quadratic number fields have previously been shown to belong to both the complexity classes NP and co-NP under the assumption of the extended Riemann hypothesis ([5, 6, 9]).

We investigate the following nine decision problems in quadratic function fields:

(P)	Is a given ideal principal?
(E)	Are two given ideals equivalent (i.e. do they belong to the same ideal class)?
(DL)	Given two ideal classes $[\mathfrak{a}]$ and $[\mathfrak{b}]$, is there a "discrete logarithm" $l \in \mathbb{N}_0$ such that $[\mathfrak{a}]^l = [\mathfrak{b}]$?
(O)	Given $l \in \mathbb{N}_0$ and an ideal class $[\mathfrak{a}]$, is l the order of $[\mathfrak{a}]$?
(R)	Is $R \in \mathbb{N}$ the regulator of the field (for real fields only)?
(IC)	Is $h' \in \mathbb{N}$ the ideal class number of the field?
(DC)	Is $h \in \mathbb{N}$ the divisor class number of the field?
(G)	Does a given set of ideal classes generate the ideal class group?
(B)	Does a given set of ideal classes form a basis of the ideal class group?

In imaginary quadratic function fields, the unique identification of an ideal class by its reduced representative trivially implies that (P), (E) $\in$ P, DL $\in$ NP, and (O) $\in$ NP $\cap$ co-NP. In [13], it was shown that (P), (E), (DL) $\in$ NP in the real setting. We will establish that (R) $\in$ NP $\cap$ co-NP and, for a certain infinite class of quadratic function fields, that (P), (E) $\in$ co-NP and (O) in NP $\cap$ co-NP in the real case. In addition, for these fields (both real and imaginary), we show that (DL) $\in$ co-NP and (DC), (IC), (G), (B) $\in$ NP $\cap$ co-NP. The conditional results require that a generating system of polynomial size for the ideal class group of the field be known. For quadratic number fields, such a generating system is given by all the non-inert prime ideals whose norm is bounded by $12(\log D)^2$ (see [4]), provided the extended Riemann hypothesis holds. In the function field case, an analogous generating system is available, but it is proven to be of polynomial size only in fields of very large genus.

In the next section, we reiterate some basics about quadratic function fields. Section 3 establishes some required facts about lattices and finite Abelian groups. Our complexity results are given in Section 4. All our conclusions are summarized in Tables 1 and 2 at the end of the paper.

2 Quadratic Function Fields

For an introduction to algebraic function fields, we refer the reader to [18]. Quadratic function fields are discussed in considerable detail in [3, 15, 17]. Let $k = \mathbb{F}_q$ be a finite field of odd characteristic with q elements and let x be an element that is transcendental over k. Denote by $k(x)$ and $k[x]$, respectively, the rational function field and the ring of polynomials over k in the indeterminate x. For ease of notation, we omit the variable x in rational functions and polynomials, writing $F = F(x)$. For $F = G/H \in k(x)$ with $G, H \in k[x]$ and $H \neq 0$, set $\deg F = \deg G - \deg H$ and $|F| = q^{\deg F}$ where $\deg f$ denotes the degree of a polynomial $f \in k[x]$.

A *quadratic function field* is a quadratic extension K of $k(x)$, i.e. $K = k(x, \rho) = \{A + B\rho \mid A, B \in k(x)\}$ where $\rho^2 = D$ with $D \in k[x]$ squarefree. K is (a) *real* (quadratic function field) if $\deg D$ is even and the leading coefficient $\operatorname{sgn} D$ of D is a square in k. K is (an) *imaginary* (quadratic function field) otherwise; that is, K is imaginary if $\deg D$ is odd or $\deg D$ is even and $\operatorname{sgn} D$ is not a square in k. In the latter case, K is real quadratic over a quadratic extension of k (i.e. over $\mathbb{F}_{q^2}$), so we will henceforth exclude this case.If $g \in \mathbb{N}$ denotes the genus of K, then $\deg D = 2g + 2$ if K is real and $\deg D = 2g + 1$ if K is imaginary. While a quadratic number field $\mathbb{Q}(\sqrt{D})$ is either real ($D > 0$) or imaginary ($D < 0$), a quadratic function field K can have both a real and an imaginary representation over the same field of rational functions $k(x)$, depending only on the plane curve defining K; in fact, a real representation is always possible, but not every quadratic function field has an imaginary representation. In the real case (with a choice of ρ fixed), $\deg \rho = g + 1$ is a positive integer, so the notions of degree and absolute value naturally generalize to elements in K. For $\alpha = A + B\rho \in K$, the *conjugate* of α is $\overline{\alpha} = A - B\rho \in K$ and the *norm* of α is $N(\alpha) = \alpha\overline{\alpha} = A^2 - B^2 D$.

The algebraic closure of $k[x]$ in K is $O = k[x, \rho] = \{A + B\rho \mid A, B \in k[x]\}$. The *units* (divisors of 1) in O form a group O^*. If K is imaginary, then $O^* = k^*$, the set of nonzero constants; however, if K is real, then O^*/k^* is an infinite cyclic group. In this case, a generator of O^* is a *fundamental unit* of K. If η is a fundamental unit of positive degree (unique up to nonzero constant factors), then the integer $R = \deg \eta \geq g + 1$ is the *regulator* of K. If K is imaginary, we set $R = 1$.

Every nonzero ideal in O is a $k[x]$-module of rank 2 with a unique *standard basis* $\{SQ, S(P + \rho)\}$ where $S, Q, P \in k[x]$, $SQ \neq 0$, S and Q are monic, Q divides $D - P^2$, and $|P| < |Q|$. Henceforth, all ideals are assumed to be nonzero (so the term "ideal" will always be synonymous with "nonzero ideal") and given in this *standard representation*; write $\mathfrak{a} = S(Q, P)$. An ideal $\mathfrak{a}$ is *primitive* if $S = 1$, and a primitive ideal $\mathfrak{a} = (Q, P)$ is *reduced* if $\deg Q \leq g$, or equivalently, $|Q| < |D|^{1/2}$. The *norm* of $\mathfrak{a}$ is $N(\mathfrak{a}) = S^2 Q \in k[x]$ and the *absolute norm* is $|N(\mathfrak{a})|$. The *conjugate ideal* of an ideal $\mathfrak{a} = S(Q, P)$ is the ideal $\overline{\mathfrak{a}} = S(Q, -P)$; we have $\mathfrak{a}\overline{\mathfrak{a}} = (N(\mathfrak{a}))$ is a principal ideal with generator $N(\mathfrak{a})$. If K is real, then every nonzero principal ideal $\mathfrak{a}$ in O has a *small* generator, i.e. a generator α with $0 \leq \deg \alpha < R$. α is unique up to nonzero constant factors and is always assumed to be given in *compact representation* (see [13]).

A *fractional (O-)ideal* $\mathfrak{a}$ is a subset of K such that $G\mathfrak{a} = \{G\alpha \mid \alpha \in \mathfrak{a}\}$ is an ideal for some nonzero $G \in k[x]$; if $G = 1$ satisfies this condition, we often omit the attribute "fractional". Let $\mathcal{I}$ be the infinite Abelian group of fractional ideals under ideal multiplication with identity O, and denote by $\mathcal{H}$ the infinite subgroup of $\mathcal{I}$ of fractional principal ideals. Then the factor group $\mathcal{C} = \mathcal{I}/\mathcal{H}$ is the *ideal class group* of K; its order $h' = \#\mathcal{C}$ is finite and is the *ideal class number* of K. Two fractional ideals are *equivalent* if they belong to the same coset of $\mathcal{C}$, i.e. differ by a factor that is a principal fractional ideal. If K is imaginary, then each coset of $\mathcal{C}$ has a unique reduced representative; however, if K is real, then there can be as many as $\Omega(q^g)$ (but always finitely many) reduced representatives in each ideal class.

For K any quadratic function field, let $\mathcal{D}$ denote the group of *divisors* of K/k, $\mathcal{D}^0$ the subgroup of $\mathcal{D}$ of divisors of *degree 0*, and $\mathcal{P}$ the subgroup of $\mathcal{D}^0$ of *principal divisors*. The factor group $\mathcal{Z} = \mathcal{D}^0/\mathcal{P}$ is the *zero class group* of K; it is isomorphic to the group of k-rational points on the Jacobian of K. Its order $h = \#\mathcal{Z}$ is finite and is the *(divisor) class number* of K. We have $h = Rh'$; in fact, if K is imaginary, then $\mathcal{Z}$ is isomorphic to the ideal class group $\mathcal{C}$ of K, so $h = h'$ and the problems (DC) and (IC) defined in Section 1 are identical. From the Hasse-Weil bound (see Theorems V.1.15, p. 166, and V.2.1, p. 169, of [18]), it is easy to infer that $h = O(|D|^{1/2})$; more exactly

$$(\sqrt{q}-1)^{2g} \leq h \leq (\sqrt{q}+1)^{2g}. \tag{2.1}$$

3 Properties of Lattices and Finite Groups

In this section, we summarize some well-known results about lattices and finite Abelian groups. These ideas underly the index calculus techniques used on a variety of problems in computational number theory, such as factoring integers, extracting discrete logarithms over finite fields, and computing class groups of quadratic number fields. We will make use of them here for the purpose of verifying invariants of quadratic function fields.

Let $m, n \in \mathbb{N}$ with $m \leq n$. A matrix $\mathbf{H} = (h_{ij}) \in Mat_{m\times n}(\mathbb{Z})$ is in *Hermite Normal Form* (HNF) if $h_{ii} > 0$ for $1 \leq i \leq m$, $0 \leq h_{ij} < h_{ii}$ for $1 \leq i < j \leq m$, and $h_{ij} = 0$ otherwise. In particular, $\mathbf{H}$ has the following form:

$$H = \left(\begin{array}{cccc|ccc} h_{11} & \dots & h_{1,m-1} & h_{1m} & 0 & \dots & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & h_{m-1,m-1} & h_{m-1,m} & 0 & \dots & 0 \\ 0 & 0 & 0 & h_{mm} & 0 & \dots & 0 \end{array}\right).$$

Every matrix $\mathbf{A} = (a_{ij}) \in Mat_{m\times n}(\mathbb{Z})$ of rank m can be converted to a unique matrix in HNF by means of a sequence of unimodular column transformations. The time required to do this is polynomial in m, n, and $\log ||\mathbf{A}||$ where $||\mathbf{A}|| = \max\{|a_{ij}| \mid 1 \leq i \leq m, 1 \leq j \leq n\}$ [10].

A nonsingular square matrix $\mathbf{S} = (s_{ij}) \in Mat_{m\times m}(\mathbb{Z})$ is in *Smith Normal Form* (SNF) if $\mathbf{S} = \text{diag}(s_1, s_2, \dots, s_m)$ is a diagonal matrix with positive diagonal entries $s_1, s_2, \dots, s_m$ such that s_i divides s_{i+1} for $1 \leq i < m$. Every nonsingular matrix $\mathbf{A} \in Mat_{m\times m}(\mathbb{Z})$ can be converted to a unique matrix in SNF by means of a sequence of unimodular row and column transformations. The time required to do this is polynomial in m and $\log ||\mathbf{A}||$ [10].

A *lattice* Γ is an additive subgroup of $\mathbb{Z}^m$. Γ has finite index in $\mathbb{Z}^m$ if and only if the rank of Γ as a group is m. In this case, let $\{\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_m\}$ be a basis of Γ where $\mathbf{x}_j = (x_{1j}, x_{2j}, \dots, x_{mj}) \in \mathbb{Z}^m$ for $1 \leq j \leq m$. The *determinant* of Γ is $\det(\Gamma) = |\det(x_{ij})|$; it is independent of the basis of Γ. If Γ_1 and Γ_2 are two lattices of finite index in $\mathbb{Z}^m$ so that Γ_1 is a sublattice of Γ_2, then $\det(\Gamma_2)$ divides $\det(\Gamma_1)$.

Let $\mathcal{G}$ be a finite Abelian group of order l and let $\{g_1, g_2, \dots, g_m\}$ be a generating system for $\mathcal{G}$, i.e. every $g \in \mathcal{G}$ has a (not necessarily unique) representation $g = g_1^{e_1} g_2^{e_2} \cdots g_m^{e_m}$ with $(e_1, e_2, \dots, e_m) \in \mathbb{Z}^m$. Then the map

$$\varphi = \varphi_{\{g_1, g_2, \dots, g_m\}} : \mathbb{Z}^m \to \mathcal{G} \quad \text{via} \quad \varphi(e_1, e_2, \dots, e_m) = g_1^{e_1} g_2^{e_2} \cdots g_m^{e_m} \tag{3.2}$$

is a surjective group homomorphism whose kernel Γ is a sublattice of $\mathbb{Z}^m$. Thus, the factor group $\mathbb{Z}^m/\Gamma$ is isomorphic to $\mathcal{G}$, so $\det(\Gamma) = l$. Let $\{\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_n\}$ be a generating system of Γ where $\mathbf{x}_j = (x_{1j}, x_{2j}, \dots, x_{mj}) \in \mathbb{Z}^m$ for $1 \leq j \leq n$, and let $\mathbf{X} \in Mat_{m\times n}(\mathbb{Z})$ be the matrix whose columns are the vectors $\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_n$ (note that $m \leq n$). If $\mathbf{H} = (h_{ij}) \in Mat_{m\times n}(\mathbb{Z})$ is the matrix obtained by converting $\mathbf{X}$ into HNF, then the columns of $\mathbf{H}$ also form a generating system of Γ; in fact, the first m columns of $\mathbf{H}$ form a basis of Γ and we have

$$l = \det(\Gamma) = |\det(h_{ij})_{1\leq i,j\leq m}| = \prod_{i=1}^{m} |h_{ii}|,$$

so l can be found by converting $\mathbf{X}$ into HNF. Let $\mathbf{S} = \operatorname{diag}(s_1, s_2, \ldots s_m)$ be the SNF of the submatrix $(h_{ij}) \in Mat_{m\times m}(\mathbb{Z})$. Then $\mathbb{Z}^m/\Gamma$ (and hence $\mathcal{G}$) is isomorphic to $\mathbb{Z}/s_1\mathbb{Z} \times \mathbb{Z}/s_2\mathbb{Z} \times \cdots \times \mathbb{Z}/s_m\mathbb{Z}$. If t is the smallest index with $s_t \neq 1$, then $s_t, s_{t+1}, \ldots, s_m$ are the elementary divisors of the finite Abelian group $\mathcal{G}$, and $\mathcal{G}$ has rank $m - t + 1$. Thus, $g_1, g_2, \ldots, g_m$ is a basis of $\mathcal{G}$ if and only if $t = 1$, i.e. $s_1 \neq 1$.

4 Complexity Results

We are now ready to prove our complexity results. Rather than using the terminology of language recognition, we employ a somewhat less formal model for establishing membership in NP or co-NP of a given problem. A *prover* Peggy provides a *certificate* to a *verifier* Vic, who subsequently verifies the correctness of this certificate in time that is polynomial in the length of the inputs given by the question. We let $K = k(x, \rho)$ be a quadratic function field and $O = k[x, \rho]$ be the algebraic closure of $k[x]$ in K. Any polynomial $G \in k[x]$ is assumed to be given by a list of its coefficients and hence requires $\Omega(\log|G|)$ bits of storage; in particular, the field K, represented by q and D, has size $\Omega(\log|D|)$. The standard basis of an ideal $\mathfrak{a} = S(Q, P)$ needs $\Omega(\log|SQD|)$ bits and $\Omega(\log|D|)$ bits if $\mathfrak{a}$ is reduced. If K is real and α is a small generator of a principal ideal $\mathfrak{a}$, then the compact representation of α is polynomially bounded by the standard representation of $\mathfrak{a}$. Hence, the size of the compact representation of a small generator of a reduced principal ideal (and in particular, that of a fundamental unit η of positive degree) is polynomially bounded in $\log|D|$ (see [13]).

The following ideal computations can be carried out in polynomial time (see [7, 15, 12, 14] for the exact algorithms). All input and output ideals are assumed to be in standard representation.

1. The product of two ideals.
2. A reduced ideal $\mathfrak{red}(\mathfrak{a})$ equivalent to a given ideal $\mathfrak{a}$.
3. A reduced ideal $\mathfrak{red}(\mathfrak{a}, \mathfrak{b})$ equivalent to the product ideal $\mathfrak{ab}$, given two ideals $\mathfrak{a}$ and $\mathfrak{b}$.
4. A reduced ideal $\mathfrak{red}(\mathfrak{a}, n)$ equivalent to $\mathfrak{a}^n$, given $n \in \mathbb{N}$ and an ideal $\mathfrak{a}$.
5. The reduced principal ideal $\mathfrak{bel}(l)$ *below* l for $l \in \mathbb{N}$; that is, the unique reduced principal ideal $\mathfrak{a} = (\alpha)$ such that $\deg\alpha \leq l$ and $l - \deg\alpha$ is minimal (real case only).
6. The standard basis of a reduced principal ideal $\mathfrak{a}$, given a small generator of $\mathfrak{a}$ in compact representation (real case only).

We begin with some unconditional complexity results. We first note that the uniqueness of a reduced representative in each ideal class (or equivalently, each divisor class) in the imaginary setting immediately implies (P), (E) $\in$ P, DL $\in$ NP, and (O) $\in$ NP $\cap$ co-NP. For the last result, we observe that an ideal class $[\mathfrak{a}]$ has order $l \in \mathbb{N}$ if and only if $\mathfrak{red}(\mathfrak{a}, l) = O$ and $\mathfrak{red}(\mathfrak{a}, l/p) \neq O$ for each prime divisor p of l. For $l = 1$, the verification is simply a principality test for $\mathfrak{red}(\mathfrak{a})$. If $l > 1$, Peggy provides Vic with the prime factorization of l and a certificate of primality for each prime divisor of l. An analogous technique can be turned into a test for the regulator R of a real quadratic function field K:

Lemma 4.1 *Let K be real and let $\tilde{R} \in \mathbb{Z}$, $\tilde{R} \geq 2$. Then $\tilde{R} = R$ if and only if $\tilde{R}$ is a multiple of R and $\mathfrak{bel}(\tilde{R}/p) \neq O$ for every prime divisor p of $\tilde{R}$ with $\tilde{R}/p > g$.*

Proof: If $\tilde{R} = R$, then clearly R divides $\tilde{R}$. Let p be a prime divisor of $\tilde{R}$ as in the Lemma. Then $\mathfrak{bel}(\tilde{R}/p) \neq O$ follows from the fact that there exists a nontrivial reduced principal ideal with a small generator of degree $g + 1 \leq \tilde{R}/p < R$. Conversely, assume $\tilde{R} = nR$ with $n \in \mathbb{N}$ and $\mathfrak{bel}(\tilde{R}/p) \neq O$ for every prime divisor p of $\tilde{R}$ with $\tilde{R}/p > g$. Suppose $n \neq 1$ and let p be a prime divisor of n. Then R divides $\tilde{R}/p$, so $\mathfrak{bel}(\tilde{R}/p) = O$, implying $\tilde{R}/p \leq g$. But then $g < R \leq Rn/p = \tilde{R}/p \leq g$, a contradiction. ◇

Corollary 4.2 *If K is real, then (R) $\in$ NP $\cap$ co-NP.*

Proof: Vic computes the regulator R of K as follows. Peggy provides a fundamental unit η of positive degree in compact representation and the unique prime factorization of $\tilde{R} = \deg \eta$ with the appropriate verification information. Vic verifies this prime factorization and checks that the standard representation of the ideal (η) is $(\eta) = O = (1, 0)$; this proves that η is a unit, so R divides $\tilde{R}$. By the previous Lemma, $\tilde{R} = R$ if and only if $\mathfrak{bel}(\tilde{R}/p) \neq O$ for each prime p dividing $\tilde{R}$ with $\tilde{R}/p > g$. ◇

For our remaining complexity results, we require the following assumption about the ideal class group $\mathcal{C}$ of K:

(A) A generating system of polynomial size for $\mathcal{C}$ is known.

(2.1) implies that the rank of $\mathcal{C}$ is $O(\log |D|)$, so since each ideal class has a reduced representative, such a generating system always exists, but there is no easy way to explicitly find one or even verify a given generating system as such. There is however an infinite number of quadratic function fields for which (A) holds:

Lemma 4.3 *Let*

$$d = \left\lceil \frac{2\log(4g-2)}{\log q} \right\rceil .$$

Then the set $\mathcal{F}$ consisting of the classes of nonprincipal prime ideals whose absolute norm is at most q^d form a generating system of $\mathcal{C}$. Furthermore, $\#\mathcal{F} < 4dq^d$.

Proof: Follows from Corollary 1 of [11] and Theorem 5.4.3 and Lemma 6.2.3 of [16]. ◇

Corollary 4.4 *If q is bounded by a polynomial in g, then assumption (A) holds for K.*

Proof: Let $\mathcal{F}$ and d be as in the previous Lemma. Since $d < (2\log(4g-2)/\log q) + 1$, we have $q^d < (4g-2)^2 q$ which is polynomially bounded in g. Hence, $\#\mathcal{F}$ is polynomial in g under these bounds. By [3], each nonprincipal prime ideal $\mathfrak{p}$ of K has a standard representation $\mathfrak{p} = (Q, P)$ where Q is irreducible and $P^2 \equiv D \pmod{Q}$. Hence for each $\mathfrak{p} \in \mathcal{F}$, we have $|P| < |Q| = |N(\mathfrak{p})| \leq q^d$. ◇

Proposition 4.5 *Under assumption (A), (G) $\in$ NP.*

Proof: Let $[\mathfrak{a}_1], [\mathfrak{a}_2], \ldots, [\mathfrak{a}_m]$ be a set of ideal classes. Vic wishes to verify that these classes generate $\mathcal{C}$. Let $[\mathfrak{b}_1], [\mathfrak{b}_2], \ldots, [\mathfrak{b}_n]$ be a known generating system of $\mathcal{C}$ of polynomial size. Peggy provides a matrix $\mathbf{X} = (x_{ij}) \in Mat_{m \times n}(\mathbb{Z})$ where

$$[\mathfrak{b}_j] = [\mathfrak{a}_1]^{x_{1j}} [\mathfrak{a}_2]^{x_{2j}} \cdots [\mathfrak{a}_m]^{x_{mj}} \text{ for } j = 1, 2, \ldots, n \tag{4.3}$$

and $0 \leq x_{ij} < h'$ for $1 \leq i \leq m$ and $1 \leq j \leq n$. By (2.1), the size of $\mathbf{X}$ is $O(mn \log |D|)$. For each $j \in \{1, 2, \ldots, n\}$, Vic computes the following reduced ideals in the order given:

$$\begin{aligned} \mathfrak{r}_{ij} &= \mathfrak{red}(\mathfrak{a}_i, x_{ij}) \quad \text{for } i = 1, 2, \ldots, m, \\ \mathfrak{s}_{1j} &= \mathfrak{r}_{1j}, \quad \mathfrak{s}_{ij} = \mathfrak{red}(\mathfrak{s}_{i-1,j} \mathfrak{r}_{ij}) \quad \text{for } i = 2, 3, \ldots, m, \\ \mathfrak{t}_j &= \mathfrak{red}(\mathfrak{s}_{mj} \overline{\mathfrak{b}_j}). \end{aligned}$$

Note that for $j = 1, 2, \ldots, n$, $\mathfrak{s}_{mj}$ is a reduced ideal equivalent to $\mathfrak{a}_1^{x_{1j}} \mathfrak{a}_2^{x_{2j}} \cdots \mathfrak{a}_m^{x_{mj}}$, so (4.3) holds if and only if $\mathfrak{t}_j$ is principal. If K is imaginary, Vic verifies that each $\mathfrak{t}_j = O$; if K is real, then Peggy provides a small generator θ_j for each $\mathfrak{t}_j$. By computing the standard representations (Q_j, P_j) of each (θ_j), Vic can easily check whether $\mathfrak{t}_j = (Q_j, P_j)$ for $j = 1, 2, \ldots, n$, thereby verifying (4.3). ◇

Several of our verification procedures require computations similar to the one in the previous proposition; in particular, Vic oftentimes needs to establish a reduced ideal as being principal. If K is real, we always assume that Peggy provides a small generator of the ideal in question.

Proposition 4.6 *Under assumption (A), (IC) $\in$ NP $\cap$ co-NP.*

Proof: Vic computes the ideal class number h' of K as follows. Let $\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_m$ be a polynomial size set of ideals for which it is known (or has been verified) that their classes generate $\mathcal{C}$. Peggy provides a matrix $\mathbf{X} = (x_{ij}) \in Mat_{m\times n}(\mathbb{Z})$ whose columns generate the kernel Γ of the map $\varphi : \mathbb{Z}^m \to \mathcal{C}$ of (3.2) with respect to the given generating system. Here, $0 \leq x_{ij} < h'$ $(1 \leq i \leq m, 1 \leq j \leq n)$ as before. Then $\mathfrak{a}_1^{x_{1j}}\mathfrak{a}_2^{x_{2j}} \cdots \mathfrak{a}_m^{x_{mj}}$ is principal for $j = 1, 2, \ldots, n$. Vic computes the ideals $\mathfrak{r}_{ij}$ and $\mathfrak{s}_{ij}$ $(1 \leq i \leq m, 1 \leq j \leq n)$ as in the previous proposition and checks that $\mathfrak{s}_{mj}$ is principal for $j = 1, 2, \ldots, n$.

The principality of the ideals $\mathfrak{s}_{m1}, \mathfrak{s}_{m2}, \ldots, \mathfrak{s}_{mn}$ proves to Vic that the columns of $\mathbf{X}$ lie in fact in the kernel Γ of φ, so they generate a sublattice Γ' of Γ. Let $\mathbf{H} = (h_{ij}) \in Mat_{m\times n}(\mathbb{Z})$ be the matrix obtained by converting $\mathbf{X}$ to HNF. Then Vic knows that $\hat{h'} = \det(\Gamma') = |h_{11}h_{22}\cdots h_{mm}|$ is a multiple of h'.

If K is real, Peggy provides the regulator R of K, together with a verification certificate. Vic verifies the value of the regulator and, for both the real and the imaginary setting, computes the multiple $\hat{h} = R\hat{h'}$ of h ($\hat{h} = \hat{h'}$ if K is imaginary) as well as a real number t such that $t < h < 2t$. A suitable value of t is given in Theorem 6.2.1 of [16] and can be computed in time polynomial in $\log|D|$. Then $\hat{h} = h$ if and only if $t < \hat{h} < 2t$. This is the case if and only if $\hat{h'} = h'$ (which in turn is the case if and only if the vectors $\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_n$ generate all of Γ). $\diamond$

Corollary 4.7 *Under assumption (A), (DC) $\in$ NP $\cap$ co-NP.*

Proof: This is clear in the imaginary case. In the real case, simply verify R and h', then $h = Rh'$. $\diamond$

Proposition 4.8 *Under assumption (A), (B) $\in$ NP.*

Proof: Let $\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_m$ be a set of ideals. Vic wishes to find out whether the classes containing these ideals form a basis of $\mathcal{C}$. Peggy provides Vic with information to verify that the classes of $\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_m$ generate $\mathcal{C}$. She also supplies the matrix $\mathbf{X}$ of the proof of Proposition 4.6. Vic proceeds as in the proof of that proposition, i.e. he computes the matrix $\mathbf{H}$ and the ideal class number h'. Finally, he determines the SNF $S = \mathrm{diag}(s_1, s_2, \ldots, s_m)$ of the submatrix $(h_{ij})_{1\leq i,j\leq m}$ of $\mathbf{H}$. Then the classes containing $\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_m$ form a basis of $\mathcal{C}$ if and only if $s_1 \neq 1$. $\diamond$

Proposition 4.9 *If K is real, then under assumption (A), (O) $\in$ NP $\cap$ co-NP.*

Proof: Let $\mathfrak{a}$ be an ideal. Vic determines the order of the class $[\mathfrak{a}]$ in $\mathcal{C}$ as follows. Peggy provides a polynomial size set of ideals $\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_m$ whose classes form a basis of $\mathcal{C}$. She also gives the order h_i of the class of $\mathfrak{a}_i$ for $1 \leq i \leq m$ and the ideal class number h'. Vic can verify the orders h_i by checking that $h_i > 1$, $\mathfrak{red}(\mathfrak{a}_i, h_i)$ is principal $(i = 1, 2, \ldots, m)$, and $h_1h_2\cdots h_m = h'$. Peggy now supplies a vector $(e_1, e_2, \ldots, e_m)$ such that the product $\mathfrak{a}_1^{e_1}\mathfrak{a}_2^{e_2}\cdots\mathfrak{a}_m^{e_m}$ is equivalent to $\mathfrak{a}$; Vic checks this by computing $\mathfrak{r}_i = \mathfrak{red}(\mathfrak{a}_i, e_i)$ $\mathfrak{s}_1 = \mathfrak{r}_1$, $\mathfrak{s}_i = \mathfrak{red}(\mathfrak{s}_{i-1}\mathfrak{r}_i)$ $(2 \leq i \leq m)$, and verifying that $\mathfrak{red}(\mathfrak{s}_m\overline{\mathfrak{a}})$ is principal. Then the order of $[\mathfrak{a}]$ in $\mathcal{C}$ is

$$\mathrm{lcm}\left(\frac{h_1}{\gcd(h_1, e_1)}, \frac{h_2}{\gcd(h_2, e_2)}, \ldots, \frac{h_m}{\gcd(h_m, e_m)}\right).$$

$\diamond$

Corollary 4.10 *If K is real, then under assumption (A), (P) $\in$ co-NP and (E) $\in$ co-NP.*

Proposition 4.11 *Under assumption (A), (B) $\in$ co-NP.*

Proof: Suppose that Vic wishes to verify that the classes represented by the ideals $\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_m$ do not form a basis of $\mathcal{C}$. If these ideal classes are dependent, Peggy provides a vector $(e_1, e_2, \ldots, e_m)$ such that $\mathfrak{a}_1^{e_1}\mathfrak{a}_2^{e_2}\cdots\mathfrak{a}_m^{e_m}$ is principal. Suppose now that the ideal classes are independent. Then they generate a subgroup of $\mathcal{C}$. Peggy provides the value of h' and for $i = 1, 2, \ldots, m$ the order h_i of the class of $\mathfrak{a}_i$, together with certificates to verify the correctness of these values. Then the ideal classes in question do not form a basis if and only if the product $h_1h_2\cdots h_m$ is a proper divisor of h'. $\diamond$

Proposition 4.12 *Under assumption (A), (G) $\in$ co-NP.*

Proof: Let $\mathfrak{b}_1, \mathfrak{b}_2, \ldots, \mathfrak{b}_n$ be ideals. Vic wants to ensure that the classes represented by these ideals do not generate the ideal class group $\mathcal{C}$. Peggy provides a polynomial size set of ideals $\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_m$ whose classes form a basis of $\mathcal{C}$. She also gives the order h_i of $[\mathfrak{a}_i]$ for $i = 1, 2, \ldots, m$ and a matrix $\mathbf{X} = (x_{ij}) \in Mat_{m\times n}(\mathbb{Z})$ such that $[\mathfrak{b}_j] = [\mathfrak{a}_1]^{x_{1j}}[\mathfrak{a}_2]^{x_{2j}}\cdots[\mathfrak{a}_m]^{x_{mj}}$ for $1 \le j \le n$. Now there must exist an index l (which Peggy provides) such that the class of $\mathfrak{a}_l$ is not contained in the subgroup generated by the classes of the $\mathfrak{b}_j$ for $1 \le j \le n$. Consider the system of linear diophantine equations

$$\sum_{j=1}^{n} x_{ij}y_j + h_i y_{n+i} = \delta_{il} \quad (1 \le i \le m) \tag{4.4}$$

in the unknowns $y_1, \ldots, y_n, y_{n+1}, \ldots, y_{n+m}$ where $\delta_{il} = 1$ if $i = l$ and 0 otherwise. (4.4) has an integer solution if and only if

$$\sum_{j=1}^{n} x_{ij}y_j \equiv \delta_{il} \pmod{h_i} \quad \text{for } i = 1, 2, \ldots, m,$$

which is the case if and only if

$$[\mathfrak{a}_l] = \prod_{i=1}^{m}[\mathfrak{a}_i]^{\delta_{il}} = \prod_{i=1}^{m}[\mathfrak{a}_i]^{\sum_{j=1}^{n} x_{ij}y_j} = \prod_{j=1}^{n}\prod_{i=1}^{m}[\mathfrak{a}_i]^{x_{ij}y_j} = \prod_{j=1}^{n}[\mathfrak{b}_j]^{y_j},$$

contradicting the fact that the class of $\mathfrak{a}_l$ is not a combination of the classes of $\mathfrak{b}_1, \mathfrak{b}_2, \ldots, \mathfrak{b}_n$. So Vic simply needs to verify that (4.4) has no solutions. This can be done in polynomial time using the methods of [8] or [10]. $\diamond$

Finally, to show that DL $\in$ co-NP, we make use of the following elementary number theoretic lemma.

Lemma 4.13 *Let $a, b \in \mathbb{Z}$ and $m, n \in \mathbb{N}$. Then the system of linear congruences*

$$\begin{aligned} x &\equiv a \ (mod\ m) \\ x &\equiv b \ (mod\ n) \end{aligned} \tag{4.5}$$

has a solution if and only if $d = \gcd(m, n)$ divides $a - b$. In this case, if z is a solution of (4.5), then all other solutions of (4.5) are given by the congruence class $z + lcm(m, n)\mathbb{Z}$.

Proof: If z is a solution of (4.5), then $z = a + sm = b + tn$ for some $s, t \in \mathbb{Z}$, so d divides $tn - sm = a - b$. Clearly, $z + l\cdot\mathrm{lcm}(m, n)$ is a solution of (4.5) for any $l \in \mathbb{Z}$. If $\tilde{z}$ is another solution of (4.5), then $z \equiv \tilde{z} \pmod{m}$ and $z \equiv \tilde{z} \pmod{n}$, so $\mathrm{lcm}(m, n)$ divides $z - \tilde{z}$.

Conversely, suppose d divides $a - b$, say $a - b = ud$ with $u \in \mathbb{Z}$. Let $v, w \in \mathbb{Z}$ with $d = vm + wn$. Set $z = a - uvm$, then $z \equiv a \pmod{m}$ and $z \equiv a - ud + uwn \equiv b - uwn \equiv b \pmod{n}$. $\diamond$

Proposition 4.14 *Under Assumption (A), (DL) $\in$ co-NP.*

Proof: Let $\mathfrak{a}$, $\mathfrak{b}$ be ideals. The question is whether there exists $l \in \mathbb{N}$ so that $\mathfrak{a}^l$ is equivalent to $\mathfrak{b}$. Peggy provides a polynomial size basis $[\mathfrak{a}_1], [\mathfrak{a}_2], \ldots, [\mathfrak{a}_m]$ of $\mathcal{C}$, together with the orders h_i of $[\mathfrak{a}_i]$ $(1 \leq i \leq m)$ and vectors $(a_1, a_2, \ldots, a_m)$ and $(b_1, b_2, \ldots, b_m)$ $(0 \leq a_i, b_i < h_i$ for $i = 1, 2, \ldots, m)$ such that $[\mathfrak{a}] = [\mathfrak{a}_1]^{a_1}[\mathfrak{a}_2]^{a_2} \ldots [\mathfrak{a}_m]^{a_m}$ and $[\mathfrak{b}] = [\mathfrak{a}_1]^{b_1}[\mathfrak{a}_2]^{b_2} \ldots [\mathfrak{a}_m]^{b_m}$. Now $[\mathfrak{a}]^l = [\mathfrak{b}]$ for some $l \in \mathbb{Z}$ if and only if $\mathfrak{a}_1^{la_1-b_1}\mathfrak{a}_2^{la_2-b_2} \cdots \mathfrak{a}_m^{la_m-b_m}$ is principal, or equivalently, $la_i \equiv b_i \pmod{h_i}$ for $i = 1, 2, \ldots, m$. A necessary condition for this system of linear congruences to have a solution l is that $d_i = \gcd(a_i, h_i)$ divides b_i for $i = 1, 2, \ldots, m$, so failure of this condition for some $i \in \{1, 2, \ldots, m\}$ finishes the verification. Suppose that d_i divides b_i for all i and set $a_i' = a_i/d_i$, $b_i' = b_i/d_i$, and $h_i' = h_i/d_i$ $(1 \leq i \leq m)$. Also, define integers c_i via $a_i'c_i \equiv b_i' \pmod{h_i'}$. It then suffices to show that the system of linear congruences

$$x \equiv c_i \pmod{h_i'} \quad (1 \leq i \leq m) \tag{4.6}$$

has no solution. By Lemma 4.13, (4.6) has a solution if and only if for all $j \in \{2, 3, \ldots, m\}$ the following holds. Suppose inductively that l_{j-1} is a solution to the first $j-1$ congruences of (4.6). Then by Lemma 4.13, the first j congruences of (4.6) have a solution l_j if and only if $\gcd(\operatorname{lcm}(h_1', h_2', \ldots, h_{j-1}'), h_j')$ divides $l_{j-1} - c_j$. So an index $j \in \{2, 3, \ldots, m\}$ such that this divisibility condition is not satisfied proves the nonexistence of l. $\diamond$

We summarize our results in the two tables below.

Unconditional Complexity Results

Problem	*Real Fields*	*Imaginary Fields*
(P)	NP	P
(E)	NP	P
(DL)	NP	NP
(O)		NP ∩ co-NP
(R)	NP ∩ co-NP	—

Complexity Results Assuming (A)

Problem	*Real Fields*	*Imaginary Fields*
(IC)	NP ∩ co-NP	NP ∩ co-NP
(DC)	NP ∩ co-NP	NP ∩ co-NP
(G)	NP ∩ co-NP	NP ∩ co-NP
(B)	NP ∩ co-NP	NP ∩ co-NP
(P)	NP ∩ co-NP	P
(E)	NP ∩ co-NP	P
(DL)	NP ∩ co-NP	NP ∩ co-NP
(O)	NP ∩ co-NP	NP ∩ co-NP

Acknowledgement. The author wishes to thank an anonymous referee for his or her helpful suggestions, including pointing out an error (and offering a correction) in the proof of Lemma 4.1 as well as providing a stronger version of Corollary 4.4.

References

[1] L. M. Adleman, J. DeMarrais & M. D. Huang, A subexponential algorithm for discrete logarithms over the rational subgroup of the Jacobians of large genus hyperelliptic curves over finite fields. *First International Symposium on Algorithmic Number Theory ANTS-I* (L. M. Adleman & M.-D. Huang, eds.), *Lect. Notes Comp. Sci.* **877**, Springer, Berlin 1994, 28–40.

[2] L. M. Adleman & M. D. Huang, Counting rational points on curves and Abelian varieties over finite fields. *Second International Symposium on Algorithmic Number Theory ANTS-II* (H. Cohen, ed.), *Lect. Notes Comp. Sci.* **1122**, Springer, Berlin 1996, 1–16.

[3] E. Artin, Quadratische Körper im Gebiete der höheren Kongruenzen I, II. *Math. Zeitschr.* **19** (1924), 153–206.

[4] E. Bach, Explicit bounds for primality testing and related problems, *Math. Comp.* **55** (1990), 355–380.

[5] J. A. Buchmann & H. C. Williams, On the existence of a short proof for the value of the class number and regulator of a real quadratic field. *Number Theory and Applications* (R. A. Mollin, ed.), *NATO ASI Series C* **265**, Kluwer, Dordrecht (The Netherlands) 1989, 327–345.

[6] J. A. Buchmann & H. C. Williams, Some remarks concerning the complexity of computing class groups of quadratic fields. *J. Complexity* **7** (1991), 311–315.

[7] D. G. Cantor, Computing in the Jacobian of a hyperelliptic curve. *Math. Comp.* **48** (1987), 95–101.

[8] M. A. Frumkin, Polynomial time algorithms in the theory of linear diophantine equations. *Fundamentals of Computation Theory* (M. Karpinski, ed.), *Lect. Notes Comp. Sci.* **56**, Springer, New York 1977, 386–392.

[9] J. L. Hafner & K. S. McCurley, A rigorous subexponential algorithm for computation of class groups. *J. Amer. Math. Soc.* **2** (1989), 837–849.

[10] R. Kannan & A. Bachem, Polynomial algorithms for computing the Smith and Hermite normal forms of an integer matrix. *SIAM J. Computing* **8** (1979), 499–507.

[11] V. Müller, A. Stein & C. Thiel, Computing discrete logarithms in real quadratic congruence function fields of large genus. *Math. Comp.* **68** (1999), 807-822.

[12] S. Paulus & A. Stein, Comparing real and imaginary arithmetics for divisor class groups of hyperelliptic curves. *Third International Symposium on Algorithmic Number Theory ANTS-III* (J. P. Buhler, ed.), *Lect. Notes Comp. Sci.* **1423**, Springer, Berlin 1998, 576–591.

[13] R. Scheidler, Compact representation in real quadratic congruence function fields. *Second International Symposium on Algorithmic Number Theory ANTS-II* (H. Cohen, ed.), *Lect. Notes Comp. Sci.* **1122**, Springer, Berlin 1996, 323–336.

[14] R. Scheidler, A. Stein & H. C. Williams, Key-exchange in real quadratic congruence function fields. *Designs, Codes and Cryptography* **7** (1996), 153–174.

[15] A. Stein, *Baby step-Giant step-Verfahren in reell-quadratischen Kongruenzfunktionenkörpern mit Charakteristik ungleich 2.* Diplomarbeit, Universität des Saarlandes, Saarbrücken (Germany), 1992.

[16] A. Stein, *Algorithmen in reell-quadratischen Kongruenzfunktionenkörpern.* Doctoral Dissertation, Universität des Saarlandes, Saarbrücken (Germany), 1996.

[17] A. Stein & H. C. Williams, Some methods for evaluating the regulator of a real quadratic function field. *Exp. Math.* **8** (1999), 119-133

[18] H. Stichtenoth, *Algebraic Function Fields and Codes.* Springer, Berlin 1993.