# Some Methods for Evaluating the Regulator of a Real Quadratic Function Field

Andreas Stein and Hugh C. Williams

**CONTENTS**

**1. Introduction**
**2. The Baby Step Method**
**3. The Baby Step – Giant Step Method**
**4. The $O(|D|^{1/5})$-Method**
**5. Computations**
**Acknowledgements**
**References**

We develop methods for the rapid computation of the regulator of a real quadratic congruence function field $K = k(x)(\sqrt{D})$. By extending Shanks' infrastructure ideas in real quadratic number fields to real quadratic congruence function fields we obtain a baby step – giant step method for evaluating the regulator of K in $O(|D|^{1/4})$ polynomial operations. We also show the existence of an effective algorithm which computes the regulator unconditionally in $O(|D|^{1/5})$ polynomial operations. By implementing both methods on a computer, we found that the $O(|D|^{1/5})$-algorithm tends to be far better than the baby step – giant step algorithm in those cases where the regulator exceeds $10^8$.

## 1. INTRODUCTION

Let $k = \mathbb{F}_q$ be a finite field of odd characteristic with $q$ elements and let $K = k(x)(\sqrt{D})$, where $D$ is a monic, squarefree polynomial of even degree. Such a field is known as a *real quadratic congruence function field* (of odd characteristic). If $\alpha = u + v\sqrt{D} \in K$ with $u, v \in k(x)$, then the conjugate of $\alpha$ is given by $\bar{\alpha} = u - v\sqrt{D}$. The *norm* of $\alpha$ is defined as $N(\alpha) = \alpha\bar{\alpha} = u^2 - v^2 D$, giving a rational function.

The *ring of integers of* $K$ is $\mathcal{O}_K = k[x][\sqrt{D}]$. Let $\mathcal{E} = \mathcal{O}_K^*$ be the *group of units* in $\mathcal{O}_K$. We know that $\mathcal{E} = k^* \times \langle\varepsilon\rangle$ where $\varepsilon \in K$ is a *fundamental unit.* In this case, the decomposition of the infinite place $\infty$ of $k(x)$ is $\infty = \infty_1 \cdot \infty_2$ , where $\infty_1$ and $\infty_2$ are the infinite places of $K/k$ with respect to $\mathcal{O}_K$. Denoting by $v_1$ and $v_2$ the corresponding normalized valuations of $K$, we define the natural number

$$R := |v_1(\varepsilon)| = |v_2(\varepsilon)| \geq 1$$

as the *regulator of* $K/k$ *with respect to* $\mathcal{O}_K$. A result of F. K. Schmidt [1931] shows its connection

Williams was supported by NSERC of Canada, Grant #A7649.

Mathematics Subject Classification (1991): Primary 11R58, 11Y65

with two further invariants, namely the *ideal class number* $h'$ and the *divisor class number* $h$,

$$h = Rh'.$$

The regulator is not only an important invariant, it is also of cryptographic relevance. In [Scheidler et al. 1996], a secure key-exchange protocol was developed by making use of the arithmetic in real quadratic function fields. Computation of the regulator is itself an instance of computing a discrete logarithm as defined in that same article; furthermore, the size of the regulator also provides a measure for the key space.

The purpose of this paper is to show how $R$ can be efficiently computed by adapting the infrastructure techniques of Shanks [1972], originally applied to real quadratic number fields, to real quadratic function fields. In order to do this we must first briefly discuss the continued fraction expansion of elements of $K$. This algorithm goes back to Artin [1924a]. We then modify the techniques of [Williams and Wunderlich 1987; Stephens and Williams 1988a; 1988b] in order to apply Shanks's infrastructure ideas to $K$. These results, discussed in much greater detail in [Stein and Zimmer 1991; [1992]], provide us with algorithms that compute $R$ in $O(q^{(1/4)\deg D})$ polynomial operations. We then show how the ideas of Lenstra [1982] and Schoof [1982] can be applied to the problem of determining $R$. From these considerations we produce an algorithm for calculating $R$ that executes unconditionally in $O(q^{(1/5)\deg D})$ polynomial operations. Finally, we implemented the algorithms and compared their running times.

## 2. THE BABY STEP METHOD

Let $L := k(x)_\infty$ be the completion of $k(x)$ with respect to $\infty$. Then $L$ is the field of power series in the variable $1/x$, and the completions of $K$ with respect to $\infty_1$ and $\infty_2$ are isomorphic to $L$:

$$K_{\infty_1} \cong K_{\infty_2} \cong k(x)_\infty = k((1/x)).$$

Also, $K$ is a subfield of $k((1/x))$. We then only have to fix one of the two places. Let $\infty_1$ be the place which corresponds to the branch where $\sqrt{1} = 1$. Then we define the continued fraction expansion in $K$ via Laurent series at $\infty_1$ in the variable $1/x$.

### 2A. Continued Fractions

In $L = k((1/x))$ we define, for a nonzero element $\alpha = \sum_{i=-\infty}^{l} c_i x^i$ with $c_l \neq 0$:

$$\left.\begin{aligned} \deg\alpha = l, \qquad & |\alpha| = q^l, \\ \operatorname{sgn}\alpha = c_l, \qquad & \lfloor\alpha\rfloor = \sum_{i=0}^{l} c_i x^i. \end{aligned}\right\} \tag{2–1}$$

If $l$ is negative we have $\lfloor\alpha\rfloor = 0$. For completeness, we set $\deg 0 = -\infty$ and $|0| = 0$. We now introduce continued fraction expansions on $L$ in the sense of Artin. Many properties of these continued fractions can be found in [Artin 1924a; Weis and Zimmer 1991]; many others can easily be established by analogy to results given in [Perron 1913; Williams and Wunderlich 1987]. (See also [Stephens and Williams 1988a; 1988b].) For an element $\alpha \in L \setminus k(x)$, we put $\alpha_0 := \alpha$, $a_0 := \lfloor\alpha_0\rfloor$, and

$$\alpha_{i+1} = \frac{1}{(\alpha_i - a_i)}, \qquad a_{i+1} = \lfloor\alpha_{i+1}\rfloor, \tag{2–2}$$

for $i \in \mathbb{N}_0$. (Here and in the sequel, $\mathbb{N}$ and $\mathbb{N}_0$ denote the positive and nonnegative integers, respectively.) As usual we define

$$\theta_1 := 1, \qquad \theta_{i+1} := \prod_{j=1}^{i} \frac{1}{\alpha_j} \quad \text{for } i \in \mathbb{N}. \tag{2–3}$$

We note that $|\alpha_i| = |a_i| \geq q > 1$ for $i \in \mathbb{N}$. In contrast to the case of real quadratic number fields, we have to distinguish two forms of periodic behavior. Let $\alpha \in L$. We say that the continued fraction expansion of $\alpha$ is *quasiperiodic* if there are integers $\nu > \nu_0 \geq 0$ and a constant $c \in k^*$ such that

$$\alpha_\nu = c\alpha_{\nu_0}. \tag{2–4}$$

The smallest positive integer $\nu - \nu_0$ for which (2–4) holds is called the *quasiperiod* of the continued fraction expansion of $\alpha$. The expansion of $\alpha$ is called *periodic* if (2–4) holds with $c = 1$. The smallest positive integer $\nu - \nu_0$ for which (2–4) holds with $c = 1$ is called the *period* of the continued fraction expansion of $\alpha$. In the periodic case, the quasiperiod divides the period, and they both start at the same index $\nu_0$.

### 2B. Reduction

We consider the continued fraction expansion of a *real quadratic irrationality* of the form

$$\alpha = (P + \sqrt{D})/Q,$$

for $\alpha \in L \backslash k(x)$, where $P, Q \in k[x]$, $Q \neq 0$, $Q$ divides $(D - P^2)$. In this situation, we put $Q_0 = Q$, $P_0 = P$, $\alpha_0 = \alpha$, $Q_{-1} = (D - P^2)/Q$, and $d = \lfloor \sqrt{D} \rfloor$. We iterate

$$P_{i+1} = a_i Q_i - P_i; Q_{i+1} = (D - P_{i+1}^2)/Q_i, \qquad (2\text{–}5)$$

for $i \in \mathbb{N}_0$. Then $0 \neq Q_i, P_i \in k[x]$, $Q_i | (D - P_i^2)$, and

$$\alpha_i = (P_i + \sqrt{D})/Q_i \qquad \text{for } i \in \mathbb{N}_0. \qquad (2\text{–}6)$$

Defining $r_i \in k[x]$ to be the remainder on division of $P_i + d$ by $Q_i$, we obtain

$$\left.\begin{aligned} P_{i+1} &= d - r_i && \text{for } i \in \mathbb{N}_0, \\ Q_{i+1} &= Q_{i-1} + a_i(r_i - r_{i-1}) && \text{for } i \in \mathbb{N}, \\ a_i &= (P_i + d) \operatorname{div} Q_i && \text{for } i \in \mathbb{N}_0, \\ r_i &= (P_i + d) \bmod Q_i && \text{for } i \in \mathbb{N}_0. \end{aligned}\right\} \quad (2\text{–}7)$$

We notice that $\deg r_i < \deg Q_i$ for $i \geq 0$. Finally,

$$\mathrm{N}(\theta_{i+1}) = \theta_{i+1}\bar{\theta}_{i+1} = (-1)^i Q_i / Q_0 \qquad (2\text{–}8)$$

for $i \in \mathbb{N}_0$,

A real quadratic irrationality is said to be *reduced* if $|\bar{\alpha}| < 1 < |\alpha|$, or equivalently, $|P - \sqrt{D}| < |Q| < |P + \sqrt{D}|$. Artin [1924a, p. 193] showed that if some $\alpha_i$ is reduced for $i \in \mathbb{N}_0$, then so are all $\alpha_j$, for $j \geq i$. From the properties of a reduced real quadratic irrationality [Artin 1924a, p. 194] we obtain the following result.

**Proposition 2.1.** *If, in the continued fraction expansion of a real quadratic irrationality $\alpha$, some $\alpha_{i_0}$ is reduced for $i_0 \geq 0$, then we have for all $i \geq i_0$:*

(a) $|P_i| = |P_i + \sqrt{D}| = |\sqrt{D}| = |d|$.

(b) $\operatorname{sgn} P_i = \operatorname{sgn} \sqrt{D}$. *Indeed, the two highest coefficients are equal.*

(c) $|a_i Q_i| = |\sqrt{D}|$. *In particular,* $1 < |a_i| \leq |\sqrt{D}|$ *and* $1 \leq |Q_i| < |\sqrt{D}|$.

It is well-known that the continued fraction algorithm can be interpreted as a reduction process. In fact, we can prove the following result.

**Theorem 2.2.** *Let $\alpha$ be a real quadratic irrationality. Then the $\alpha_i$'s are reduced for*

$$i > \max\left\{0, \tfrac{1}{2}\deg Q_0 - \tfrac{1}{4}\deg D + 1\right\}.$$

The bounds in Proposition 2.1 for the polynomials $P_i$ and $Q_i$ lead to the periodicity of the continued fraction expansion of real quadratic irrationalities in the case of a finite field $k$. This had already been proved in [Artin 1924a].

### 2C. Symmetries

The continued fraction expansion of $\alpha = \sqrt{D}$ is periodic with period $n$ and quasiperiodic with quasiperiod $m$. We easily see that $\alpha$ is not reduced; but $\alpha_1$ is reduced, and, therefore, so is $\alpha_i$ for any $i \geq 1$. Results concerning periodicity can be deduced as in [Perron 1913]. Artin [1924a, p. 195–197] showed that $\mathcal{E} = k^* \times \langle \bar{\theta}_{m+1} \rangle$, and the regulator $R$ of $K$ with respect to $\mathcal{O}_K$ is then

$$R = \deg \bar{\theta}_{m+1}. \qquad (2\text{–}9)$$

We also know that, for $s \in \mathbb{N}_0$, we have $Q_s \in k^*$ if and only if $s = \lambda m$ with $\lambda \geq 0$. Furthermore,

$$N(\bar{\theta}_{\lambda m+1}) \in k^* \quad \text{for } \lambda \geq 1. \qquad (2\text{–}10)$$

As in the case of a real quadratic number field, there exist symmetries with respect to the period and to the quasiperiod.

**Theorem 2.3.** *With $c \in k^*$ chosen such that $\alpha_{1+m} = c\alpha_1$, we have:*

$$\begin{aligned} P_{i+1} &= P_{m-i} && \textit{for } i = 0, \ldots, m-1, \\ Q_i &= c^{(-1)^{i-1}} Q_{m-i} && \textit{for } i = 0, \ldots, m, \\ -\frac{1}{\bar{\alpha}_{m-i}} &= c^{(-1)^i} \alpha_{i+1} && \textit{for } i = 0, \ldots, m-1. \end{aligned}$$

Using proof techniques similar to those employed in the real quadratic number field case, we can also obtain duplication formulas with respect to the quasiperiod. For computing the regulator of $K$, we compute the continued fraction expansion of $\alpha = \sqrt{D}$ until we reach half of the quasiperiod. We need to recursively calculate the quantities $a_i$, $r_i$, $P_i$, $Q_i$, where we use the optimized formulas in (2–7). This iterative process is known as the *baby-step method.*

## 3. THE BABY STEP – GIANT STEP METHOD

### 3A. Ideals and Continued Fractions

We summarize properties of integral ideals and introduce their continued fraction expansion. The corresponding proofs can be found in [Artin 1924a]. Any nonzero subset $\mathfrak{a}$ of $\mathcal{O}_K$ is an integral ideal if and only if there exist $S, P, Q \in k[x]$ with $Q \mid (D - P^2)$ such that $\mathfrak{a} = SQ\mathbb{F}_q[x] + (SP + S\sqrt{D})\mathbb{F}_q[x]$. In this case, we call $\{SQ,\ SP+S\sqrt{D}\}$ a $k[x]$-*basis of* $\mathfrak{a}$, and we write $\mathfrak{a} = [SQ,\ SP + S\sqrt{D}]$. If an integral ideal $\mathfrak{a}$ is given with such a $k[x]$-base, we define the *norm* of $\mathfrak{a}$ by

$$N(\mathfrak{a}) = \frac{QS^2}{\operatorname{sgn}(QS^2)} \in k[x]. \tag{3–1}$$

Note that $\operatorname{sgn} N(\mathfrak{a}) = 1$. We say that an integral $\mathcal{O}_K$-ideal $\mathfrak{a}$ is *primitive*, if $S$ can be chosen to be 1, that is, if $\mathfrak{a} = \bigl[Q,\ P + \sqrt{D}\bigr]$ with $Q \mid (D - P^2)$. A $k[x]$-base of an integral ideal $\mathfrak{a}$ can be chosen to be in *adapted* form, meaning that

$$\mathfrak{a} = \bigl[T,\ R + S\sqrt{D}\bigr] \quad \text{for some } T, R, S \in k[x] \tag{3–2}$$

with $\deg R < \deg T$. The polynomials $T, R, S$ are unique up to constant factors. For any $\mathcal{O}_K$-ideal $\mathfrak{a}$, the $\mathcal{O}_K$-ideal $\bar{\mathfrak{a}} := \{\bar{\alpha}; \alpha \in \mathfrak{a}\}$ is called the *conjugate ideal* of $\mathfrak{a}$. If $\mathfrak{a} = (\alpha) = \alpha\mathcal{O}_K$ with $\alpha \in K$, we call $\mathfrak{a}$ a *principal* $\mathcal{O}_K$*-ideal*. We say that two integral $\mathcal{O}_K$-ideals $\mathfrak{a}$ and $\mathfrak{b}$ are *equivalent*, written $\mathfrak{a} \sim \mathfrak{b}$, if there exist some nonzero elements $\alpha, \beta \in \mathcal{O}_K$ such that $(\alpha)\mathfrak{a} = (\beta)\mathfrak{b}$.

Let $\mathfrak{a}_i = [Q_i,\ P_i + \sqrt{D}]$, for $i = 1, 2$, be primitive $\mathcal{O}_K$-ideals given with adapted bases. By using essentially the same ideas as Gauss, as in [Shanks 1971], [Lenstra 1982] or [Stephens and Williams 1988a], we can compute the product of $\mathfrak{a}_1$ and $\mathfrak{a}_2$, i.e. a primitive $\mathcal{O}_K$-ideal $\mathfrak{c}$ and a polynomial $S \in k[x]$ such that $\mathfrak{a}_1\mathfrak{a}_2 = (S)\mathfrak{c}$. This can be done in $O(\deg D)$ polynomial operations. (We use this expression to mean one of the basic arithmetic operations of addition, subtraction, multiplication, division with remainder, degree comparison, or assignment in $k[x]$.)

An integral $\mathcal{O}_K$-ideal $\mathfrak{a}$ is called a *reduced* $\mathcal{O}_K$*-ideal* if $\mathfrak{a}$ is primitive and if there exists a $\mathbb{F}_q[x]$-basis of the form $\{Q,\ P + \sqrt{D}\}$ with polynomials $Q, P \in \mathbb{F}_q[x]$ such that $Q \mid (D - P^2)$ and $|P - \sqrt{D}| < |Q| < |P + \sqrt{D}|$, or equivalently, if $(P + \sqrt{D})/Q$ is a reduced real quadratic irrationality.

**Theorem 3.1.** *A primitive* $\mathcal{O}_K$*-ideal* $\mathfrak{a}$ *is reduced if and only if* $|N(\mathfrak{a})| < |\sqrt{D}|$.

Let $\mathfrak{a}$ be any primitive $\mathcal{O}_K$-ideal, and let $Q,\ P \in \mathbb{F}_q[x]$ with $Q \mid (D - P^2)$ be such that $\mathfrak{a} = [Q,\ P + \sqrt{D}]$. If we set $\alpha := (P + \sqrt{D})/Q$, then $\alpha$ is a real quadratic irrationality, and we can carry through the continued fraction expansion of $\alpha$. With $Q_i, P_i \in \mathbb{F}_q[x]$ defined as in (2–5), we let $\mathfrak{a}_1 := \mathfrak{a}$, $Q_0 := Q$, $P_0 := P$, and for $i \in \mathbb{N}$, we let

$$\mathfrak{a}_i := \bigl[Q_{i-1},\ P_{i-1} + \sqrt{D}\bigr]. \tag{3–3}$$

For $i \in \mathbb{N}$ we know from (2–6) that

$$\alpha_{i-1} = (P_{i-1} + \sqrt{D})/Q_{i-1},$$

where $P_{i-1}, Q_{i-1} \in \mathbb{F}_q[x]$, $Q_{i-1} \neq 0$, and $Q_{i-1}$ divides $(D - P_{i-1}^2)$. We deduce that each $\mathfrak{a}_i$ is a primitive integral $\mathcal{O}_K$-ideal. Most of the following results correspond to those for real quadratic number fields (see [Williams and Wunderlich 1987], for example). However, we shall prove them using the terminology of integral ideals. It is easy to prove (see [Stein 1992]) that $Q_0\theta_i, Q_0\bar{\theta}_i \in \mathcal{O}_K$ for $i \in \mathbb{N}$, and that

$$(Q_0\theta_i)\,\mathfrak{a}_i = (Q_{i-1})\,\mathfrak{a}_1. \tag{3–4}$$

First note that if $\alpha_i = (P_i + \sqrt{D})/Q_i$ is reduced for an index $i \in \mathbb{N}_0$, then the ideal $\mathfrak{a}_{i+1}$ is reduced, because the reduced $\mathbb{F}_q[x]$-base for $\mathfrak{a}_{i+1}$ is given by $\{Q_i,\ P_i + \sqrt{D}\}$. From 2.2 we then immediately derive the following theorem.

**Theorem 3.2.** *If* $\mathfrak{a} = \mathfrak{a}_1 = [Q_0,\ P_0 + \sqrt{D}]$ *is any primitive* $\mathcal{O}_K$*-ideal, then* $\mathfrak{a}_i$ *is reduced for*

$$i > I_0 := \max\bigl\{1,\ \tfrac{1}{2}\deg Q_0 - \tfrac{1}{4}\deg D + 2\bigr\}.$$

Conversely, if $\mathfrak{a}_i$ is reduced, the basis representation in (3–3) need not be the reduced one. This means that $\alpha_{i-1}$ is not necessarily reduced.

**Lemma 3.3.** *Let* $\alpha$ *be a real quadratic irrationality, and let* $i \in \mathbb{N}$. *Then* $\alpha_i$ *is reduced if and only if* $|Q_{i-1}| < |\sqrt{D}\,|$.

This means that if $\mathfrak{a}_i$ is reduced for an $i \in \mathbb{N}$, then $\alpha_i$ is reduced, since, by Theorem 3.1, $|N(\mathfrak{a}_i)| = |Q_{i-1}| < |\sqrt{D}\,|$.

**Lemma 3.4.** *If, in the continued fraction expansion of $\alpha := (P + \sqrt{D})/Q$, there exists a minimal $l \in \mathbb{N}$ such that $|Q_{l-1}| < |\sqrt{D}|$, then $\mathfrak{a}_l$ is reduced, and*

$$\left|\bar{\theta}_l\right| \leq 1, \quad |\theta_l| \geq \frac{|Q_{l-1}|}{|Q_0|}.$$

Now we will see that the continued fraction algorithm applied to a reduced ideal produces all equivalent, reduced ideals.

**Theorem 3.5.** *Let $\mathfrak{a} = \mathfrak{a}_1$ and $\mathfrak{b}$ be two equivalent reduced integral $\mathcal{O}_K$-ideals. Then there exists $\gamma \in \mathfrak{a}$ such that*

$$(\gamma)\mathfrak{b} = (N(\mathfrak{b}))\,\mathfrak{a},$$

*where $0 < |\gamma| \leq |N(\mathfrak{a})|$. Then there exists some $\nu \in \mathbb{N}$ and $c \in \mathbb{F}_q^*$ such that $\mathfrak{b} = \mathfrak{a}_\nu$ and $\gamma = cN(\mathfrak{a})\theta_\nu$.*

The theorem corresponds to [Williams and Wunderlich 1987, Theorem 4.5], and a complete proof for the case of a real quadratic congruence function field is given in [Stein 1992]. The existence of such a $\gamma \in \mathfrak{a}$ can be guaranteed in the same way as in [Williams and Wunderlich 1987, Lemma 3.1].

### 3B. Distance and Giant Steps

Let $\mathfrak{a} = \mathfrak{a}_1$ and $\mathfrak{b}$ be two equivalent, reduced, integral $\mathcal{O}_K$-ideals. By Theorem 3.5, there exists some $\nu \in \mathbb{N}$ such that $\mathfrak{b} = \mathfrak{a}_\nu$, and by (3–4), we have $(N(\mathfrak{a})\theta_\nu)\mathfrak{a}_\nu = (N(\mathfrak{a}_\nu))\mathfrak{a}$. Then we define the *distance from $\mathfrak{a}$ to $\mathfrak{b}$* as

$$\delta(\mathfrak{b}, \mathfrak{a}) = \delta(\mathfrak{a}_\nu, \mathfrak{a}) := \deg \bar{\theta}_\nu. \tag{3–5}$$

We always put $\delta_\nu := \delta(\mathfrak{a}_\nu, \mathfrak{a})$.

**Remark 3.6.** Distance is only defined between equivalent, reduced ideals. From (2–3) and because $\alpha_i$ is reduced for $i \geq 1$, we deduce that the distance function $\delta_i$ is strictly increasing in $i$, i.e. $\delta_{i+1} > \delta_i$. Since the values of the distance function are integers, we have $\delta_{t+i} \geq \delta_t + i$. Thus, if $\delta_i = \delta_j$, we conclude that $\mathfrak{a}_i = \mathfrak{a}_j$. Especially, if there are $\nu, j, l \in \mathbb{N}$ such that $\delta_j \leq \delta_\nu \leq \delta_l$, then $\mathfrak{a}_\nu \in \{\mathfrak{a}_i; j \leq i \leq l\}$ , and $\delta_i = 0$ if and only if $\mathfrak{a}_i = \mathfrak{a}$. Conversely, if $\mathfrak{a}_i = \mathfrak{a}_j$ then $\delta_i = \delta_j + lR$ where $R$ is the regulator of $K$. In this case we deduce from (3–4) that $\bar{\theta}_i$ and $\bar{\theta}_j$ differ only by a unit.

Furthermore, by (2–8), (2–3) and Proposition 2.1(c), we see that

$$\delta_i = \tfrac{1}{2}\deg D - \deg Q_0 + \sum_{j=1}^{i-2} \deg a_j \qquad \text{for } i \in \mathbb{N},\ i \geq 2. \tag{3–6}$$

In the sequel, we let $\mathfrak{a} = \mathfrak{a}_1 = (1) = \mathcal{O}_K = [1, \sqrt{D}]$. With reference to (3–3), we have $\alpha_0 = \alpha = \sqrt{D}$. Clearly, $\mathfrak{a}$ is reduced, because $|N(\mathfrak{a})| = 1 < |\sqrt{D}|$. Also $\mathfrak{a}_{i+1} = (\bar{\theta}_{i+1})$ are reduced principal ideals for $i \in \mathbb{N}_0$, where $\bar{\theta}_{i+1} \in \mathcal{O}_K$. Then $\delta_i := \delta(\mathfrak{a}_i, \mathfrak{a})$ is defined for all $i \in \mathbb{N}$. Note that, by (3–6) and Proposition 2.1(c),

$$\tfrac{1}{2}\deg D + i - 2 \;\leq\; \delta_i \;\leq\; (i-1)\cdot \tfrac{1}{2}\deg D \qquad \text{for } i \in \mathbb{N},\ i \geq 2. \tag{3–7}$$

Let $\mathfrak{b}$ be an arbitrary reduced $\mathcal{O}_K$-ideal. We develop the continued fraction expansion of $\mathfrak{b}$ as in (3–3) and denote by $P_i'$, $Q_i'$, $\theta_i'$ and $\delta_i' := \delta(\mathfrak{b}_i, \mathfrak{b})$ the quantities appearing in the continued fraction expansion applied to $\mathfrak{b}$. For any $s, t \in \mathbb{N}$, we find a polynomial $S \in \mathbb{F}_q[x]$ and a primitive $\mathcal{O}_K$-ideal $\mathfrak{c}$ such that $\mathfrak{a}_s\mathfrak{b}_t = (S)\mathfrak{c}$. We apply the continued fraction algorithm to $\mathfrak{c} = \mathfrak{c}_1$. By Theorem 3.2, it is guaranteed that, after a finite number of steps, we will obtain a reduced ideal equivalent to $\mathfrak{c}$. We denote by $P_i''$, $Q_i''$ and $\theta_i''$ the quantities appearing in the continued fraction expansion applied to $\mathfrak{c}$. In view of Lemma 3.4, let $l \in \mathbb{N}$ minimal such that $|Q_{l-1}''| < |\sqrt{D}|$; hence, $\mathfrak{c}_l$ is reduced. Summarizing, we get the following chain of equivalent ideals

$$\mathfrak{c}_l \sim \mathfrak{c} \sim (S)\mathfrak{c} = \mathfrak{a}_s\mathfrak{b}_t = (\bar{\theta}_s)\mathfrak{b}_t \sim \mathfrak{b}_t \sim \mathfrak{b}.$$

Thus, $\mathfrak{c}_l$ and $\mathfrak{b}$ are equivalent. Since they both are reduced, by Theorem 3.5 there must exist some $\nu \in \mathbb{N}$ such that $\mathfrak{c}_l = \mathfrak{b}_\nu$. We derive a result that can be proven analogously to [Williams and Wunderlich 1987, Theorem 5.2].

**Theorem 3.7.** *In the situation above there exists some $C \in \mathbb{F}_q^*$ such that*

$$\theta_\nu' = C\theta_s\theta_t'\frac{\theta_l''}{S} \quad \textit{and} \quad \delta_\nu' = \delta_t' + \delta_s + f,$$

*where $f := \deg\overline{\theta_l''} - \deg S \in \mathbb{Z}$ and $-\deg D + 2 \leq f \leq 0$.*

Note that the quantities $s, t$ can be arbitrarily large here, but $l$ is bounded by a fixed small quantity which depends on $D$. Furthermore, the integer $f$, the “error”, is bounded and is always less than 0. In general, $f$ is small compared to $\delta_s$ or $\delta'_t$. The result is of special interest for large $s, t$. As in the number field case, we expect the distance function to be roughly linear. Therefore, we really have *giant steps*. In the situation of the theorem we define a new operation called *giant step* by

$$\mathfrak{a}_s * \mathfrak{b}_t := (\mathfrak{b}_\nu, f) = (\mathfrak{c}_l, f)\,. \tag{3–8}$$

Consequently, a giant step is a composition of two operations, namely computation of the product of two primitive $\mathcal{O}_K$-ideals and reduction of the primitive part of the product using the continued fraction algorithm. Let $m$ be the quasiperiod of the continued fraction expansion of $\alpha = \sqrt{D}$. From (2–10), we deduce that $\mathfrak{a}_{m+1} = \mathfrak{a}_1 = \mathfrak{a} = \mathcal{O}_K$, and from (2–9), we see that $R = \delta_{m+1}$, where $R$ is the regulator of $K$. We easily derive that $\mathfrak{a}_{\lambda m+i+1} = \mathfrak{a}_{i+1}$ and $\delta_{\lambda m+i+1} = \lambda R + \delta_{i+1}$ for $i \in \mathbb{N}$. Furthermore, by Remark 3.6 and (3–6) with $t := 2$ and $i = t + (i-2)$, we have $\delta_i \geq \frac{1}{2}\deg D + i - 2$ for $i \in \mathbb{N}$, $i \geq 2$. Next, we consider the effects of symmetries in the case $\alpha = \sqrt{D}$. For $\mathfrak{a}_i$ defined in (3–3), we have $\bar{\mathfrak{a}}_i = [Q_{i-1},\, P_i + \sqrt{D}]$. Theorem 2.3 then yields

$$\bar{\mathfrak{a}}_i = \mathfrak{a}_{m-i+2} \quad \text{for } 1 \leq i \leq m+1. \tag{3–9}$$

If we set $\tilde{\delta}_i := \delta(\bar{\mathfrak{a}}_i, \mathfrak{a}) = \delta_{m-i+2}$, we get

$$R = \tilde{\delta}_i + \delta_i - \deg Q_{i-1} \quad \text{for } 1 \leq i \leq m+1. \tag{3–10}$$

We see that the conjugate ideals are exactly those which occur before the quasiperiod is reached.

### 3C. The Algorithm

The idea of the optimized baby step – giant step algorithm is to create a stock of principal, reduced ideals up to an index $s+T$ where $T \geq \frac{1}{4}\deg D$, and $s$, as we shall show, should be of order $q^{(1/4)\deg D}$. By using giant steps we jump to principal ideals in the same chain lying at a distance of about $2\delta_s$ away from each other. Because of the quasiperiodicity of the continued fraction expansion of $\alpha = \sqrt{D}$, we must reach one of the stored ideals. We only have to make sure that the step size is not greater than the length of the initial interval. The correctness of the algorithm is similar to that in [Stephens and Williams 1988b, p. 814–815] and is fully described in [Stein 1992, p. 144 ff.].

**Algorithm 3.8 (Regulator1).**

```
Input: $k = \mathbb{F}_q$ and $D \in k[x]$ monic, squarefree of even degree.
Output: $R$, the regulator of $k(x)(\sqrt{D})$.

1. Put $s \leftarrow \lfloor q^{(1/4)\deg D} \rfloor$ and $T \leftarrow \lfloor \frac{1}{4}\deg D + 1 \rfloor$.
2. By carrying out the continued fraction expansion of $\alpha = \sqrt{D}$, compute $\mathfrak{a}_i$ and $\delta_i$ up to the least $\delta_n$
   such that $\delta_n > \delta_{s+T}$, starting with $\mathfrak{a}_1 = (1) = \mathcal{O}_K$. Store and sort them on some coefficients of
   $N(\mathfrak{a}_i)$ in the form
       $(\mathfrak{a}_i, \delta_i) = (N(\mathfrak{a}_i), P_{i-1}, \delta_i)\,.$
   If $P_\nu = P_{\nu+1}$ for a minimal $1 \leq \nu < n$, set
       $R \leftarrow 2\delta_{\nu+1} - \deg Q_\nu;$   return.
   If $Q_\mu/\operatorname{sgn} Q_\mu = Q_{\mu+1}/\operatorname{sgn} Q_{\mu+1}$ for a minimal $1 \leq \mu < n$, set
       $R \leftarrow 2\delta_{\mu+1} - \deg Q_\mu + \deg a_{\mu+1};$   return.
3. Set $(\mathfrak{b}_1, f_1) \leftarrow \mathfrak{a}_s * \mathfrak{a}_s$; $\delta'_1 \leftarrow 2\delta_s + f_1$; $j \leftarrow 1$.
4. While $\bigl(\mathfrak{b}_j \notin \{\mathfrak{a}_1, \mathfrak{a}_2, \dots, \mathfrak{a}_n\} \cup \{\bar{\mathfrak{a}}_1, \bar{\mathfrak{a}}_2, \dots, \bar{\mathfrak{a}}_n\}\bigr)$ do:
     $(\mathfrak{b}_{j+1}, f_{j+1}) \leftarrow \mathfrak{b}_1 * \mathfrak{b}_j$; $\delta'_{j+1} \leftarrow \delta'_1 + \delta'_j + f_{j+1}$;
     $j \leftarrow j + 1$.
5. We have $\mathfrak{b}_j \in \{\mathfrak{a}_1, \mathfrak{a}_2, \dots, \mathfrak{a}_n\} \cup \{\bar{\mathfrak{a}}_1, \bar{\mathfrak{a}}_2, \dots, \bar{\mathfrak{a}}_n\}$.
   If $\mathfrak{b}_j = \mathfrak{a}_i \in \{\mathfrak{a}_1, \dots, \mathfrak{a}_n\}$ set $R \leftarrow \delta'_j - \delta_i$; return.
   If $\mathfrak{b}_j = \bar{\mathfrak{a}}_l \in \{\bar{\mathfrak{a}}_1, \dots, \bar{\mathfrak{a}}_n\}$ set
       $R \leftarrow \delta'_j + \delta_l - \deg Q_{l-1};$   return.
```

Note that after step 2 the objects have been sorted, so that in the while-loop of step 4 the searching is being performed on sorted objects. For instance, if $q$ is large, this can be done by hashing with respect to one fixed coefficient of $N(\mathfrak{a}_i)$. The baby step – giant step techniques of Algorithm 3.8 for computing the regulator $R$ of a real quadratic congruence function field $K$, have a complexity of

$$O\bigl(q^{(1/4)\deg D}\bigr) \tag{3–11}$$

polynomial operations. This is based on the following observations. We denote by $g$ the genus and by $h$ the divisor class number of $K$. Let

$$\zeta_0(s) = \bigl(1 - q^{-s+1}\bigr)^{-1}\bigl(1 - q^{-s}\bigr)^{-1}$$

and let $\zeta(s)$ be the zeta function for $K$. Then it is well known (see [Eichler 1966, pp. 299–306], for example) that

$$\frac{\zeta(s)}{\zeta_0(s)} = L(q^{-s}) = \prod_{i=1}^{2g}\Bigl(1-\frac{\omega_i}{q^s}\Bigr),$$

where $g = \frac{1}{2}\deg D - 1$ (see [Deuring 1973]) and $|\omega_i| = q^{1/2}$ for $i = 1, 2, \dots, 2g$. Furthermore,

$$h = L(1) = q^g L(1/q); \tag{3–12}$$

thus,

$$\bigl(\sqrt{q}-1\bigr)^{2g} \le h \le \bigl(\sqrt{q}+1\bigr)^{2g}. \tag{3–13}$$

Therefore, we may assume that $h = O(q^{(1/2)\deg D})$. On the other hand, we know that $h = Rh'$, where $h'$ is the ideal class number; thus $R = O(q^{(1/2)\deg D})$. We know that the distance function is strictly increasing. By (3–7), we may then assume that $m = O(R) = O(q^{(1/2)\deg D})$, since $R = \delta_{m+1}$. Furthermore, $m \approx sz$, where $s$ is the number of baby steps and $z$ the number of giant steps. We see that an optimal choice for them should be

$$s \approx O(q^{(1/4)\deg D}) \quad\text{and}\quad z \approx O(q^{(1/4)\deg D}).$$

In the continued fraction expansion, the only operations which are necessary depend on polynomial arithmetic in finite fields. We know from Proposition 2.1 that the polynomials occurring are bounded in their degrees by $\frac{1}{2}\deg D$. The same argument holds for the quantities that appear in the ideal product, and by Theorem 3.2 the number of steps to reduce a primitive ideal is $O(\deg D)$. Thus, the complexity of a giant step and a baby step is polynomial in $\log(q)$ and $\deg D$. Asymptotically, those factors are included in

$$O(q^{(1/4)\deg D})$$

polynomial operations. Thus, the total complexity determining $R$ by our algorithms is

$$O\,(s+z) = O\bigl(q^{\frac{1}{4}\deg D}\bigr)$$

polynomial operations. The iterative algorithms of Section 2C have a complexity of $O(q^{(1/2)\deg D})$ polynomial operations, because the iterations in the continued fraction expansion have to be carried out up to the quasiperiod $m$ or $m/2$.

## 4. THE O(|D|$^{1/5}$)-METHOD

In this section we will use the basic ideas of Lenstra [1982] and Schoof [1982] to show how to compute $R$ in $O(q^{(1/5)\deg D}) = O(|D|^{1/5})$ polynomial operations over $k$ if $\deg D \ge 8$. For $\deg D = 4$ or $6$, we actually obtain faster methods. We first point out that if $R \le G$ for some $G \in \mathbb{Z}$, we can determine it in $O(s+G/s)$ polynomial operations by using an algorithm like Algorithm 3.8 with a step size $s$. Thus, we will now assume that such an algorithm has been executed and that no regulator has been found for an upper bound $z$ on the search parameter $j$ which guarantees that $R > G$. Such a bound is given by

$$z = \frac{G+\delta_{T+s}}{2(\delta_s - \deg D + 2)} = O((G+s)/s).$$

For instance, if one performs $s = \lfloor\sqrt{G}\rfloor$ baby steps and $z = O(\sqrt{G})$ giant steps, then one can determine whether $R \le G$ in $O(\sqrt{G})$ polynomial operations.

We now divide the problem of determining $R$ into two parts. In the first part we find an estimate $E$ of $h$; in the next part we use the estimate to produce an integer $h^*R$ which is divisible by $R$ and then determine $h^*$. Unlike the situation of a real quadratic number field as dealt with in [Lenstra 1982] and [Schoof 1982], we do have the Riemann Hypothesis here; thus, it will turn out that our algorithm for determining $R$ is of unconditional complexity $O(q^{(2/5)g})$. Furthermore, we shall attempt to present an algorithm which is computationally efficient.

### 4A. An Estimate for h

Let $P$ represent any prime polynomial in $k[x]$ and define $\chi(P) \in \{-1, +1, 0\}$ by Artin's [1924a] symbol $\bigl[\frac{D}{P}\bigr]$. We have

$$L(q^{-s}) = \bigl(1-q^{-s}\bigr)^{-1}\prod_P\left(1-\frac{\chi(P)}{|P|^s}\right)^{-1}. \tag{4–1}$$

Define (see [Reichardt 1936])

$$n_\nu = \#\{\,P : |P| = q^\nu\,\} = \tfrac{1}{\nu}\sum_{k\,|\,\nu}(q^k+1)\,\mu(\nu/k),$$

where $\mu$ denotes the Möbius function, and

$$N_\nu = \#\{\,\wp : \wp \text{ prime ideal of } K,\ |N(\wp)| = q^\nu\,\}.$$

From the results in [Artin 1924a] on how $P$ splits in $K$, we know that when $\nu$ is odd

$$N_\nu = 2\sum_{\substack{\chi(P)=1\\ |P|=q^\nu}} 1 + \sum_{\substack{\chi(P)=0\\ |P|=q^\nu}} 1 = \sum_{|P|=q^\nu}(\chi(P)+1),$$

and when $\nu$ is even

$$N_\nu = \sum_{\substack{\chi(P)=-1\\ |P|=q^{\nu/2}}} 1 + \sum_{|P|=q^\nu}(\chi(P)+1).$$

From [Artin 1924b] we have

$$\sum_{k\,|\,\nu} k\,N_k = q^\nu - 1 - s_\nu,$$

where

$$s_\nu = \sum_{i=1}^{2g}\omega_i^\nu.$$

It follows by Möbius inversion that if $\nu > 1$, then

$$\nu(N_\nu - n_\nu) = -\sum_{k\,|\,\nu} s_k\,\mu(\nu/k);$$

thus,

$$\nu\,|N_\nu - n_\nu| \le 2g\sum_{k|\nu} q^{k/2}.$$

Hence, for all $\nu \ge 1$, we get

$$\nu\left|\sum_{\substack{P\\ |P|=q^\nu}}\chi(P)\right| \le (2g+2)\,d(\nu)\,q^{\nu/2}. \qquad \text{(4–2)}$$

Here $d(n)$ denotes the number of divisors of $n$. Now consider

$$\begin{aligned} B(w,D) &= \log \prod_{\substack{P\\ |P|>q^w}} \left(1-\frac{\chi(P)}{|P|}\right)^{-1} \\ &= -\sum_{n=w+1}^{\infty} \frac{1}{nq^n}\sum_{\substack{\nu\,|\,n\\ \nu>w}} \nu\, S_\nu(n/\nu), \end{aligned}$$

where

$$S_k(j) = \sum_{|P|=q^k}\chi(P)^j.$$

Notice that if $2\,|\,j$, then $0 \le S_k(j) \le n_k$; and if $2\nmid j$, then $k\,|S_k(j)| \le (2g+2)\,d(k)\,q^{k/2}$ by (4–2). It follows that

$$\left|\sum_{\substack{\nu\,|\,n\\ \nu>w}}\nu S_\nu(n/\nu)\right| \le q^{n/2} + (2g+2)\sum_{\substack{\nu\,|\,n\\ n/\nu\ \text{odd}}} q^{\nu/2}\,d(\nu).$$

Clearly,

$$\sum_{\substack{\nu\,|\,n\\ n/\nu\ \text{odd}}} q^{\nu/2}\,d(\nu) \le n\,q^{n/2}$$

for $n \le 4$. Also, if $n \ge 5$, it is easy to show that $n/d(n) \ge 3/2$; hence,

$$\begin{aligned} \sum_{\substack{\nu\,|\,n\\ n/\nu\ \text{odd}}} q^{\nu/2}\,d(\nu) &\le d(n) \sum_{\substack{\nu\,|\,n\\ n/\nu\ \text{odd}}} q^{\nu/2} \\ &< d(n)\left(q^{n/2} + \frac{(q^{(n/6)+(1/2)}-1)}{(q^{1/2}-1)}\right) \\ &< \tfrac{3}{2}\,d(n)\,q^{n/2} \le n\,q^{n/2}. \end{aligned}$$

Hence,

$$\left|\sum_{\substack{\nu\,|\,n\\ \nu>w}}\nu\, S_\nu(n/\nu)\right| < (2g+2)\,n\,q^{n/2} + q^{n/2}$$

and

$$\bigl|B(w,D)\bigr| < (2g+3)\sum_{n=w+1}^{\infty} q^{-n/2} = \frac{(2g+3)\,q^{-w/2}}{q^{1/2}-1}. \qquad \text{(4–3)}$$

If we put

$$\psi(w,D) = \frac{(2g+3)\ q^{-w/2}}{(q^{1/2}-1)}, \qquad \text{(4–4)}$$

it follows that

$$\begin{aligned} &\left|1-\prod_{|P|>q^w}\left(1-\frac{\chi(P)}{|P|}\right)^{-1}\right| \\ &\qquad < \max\{\,e^{\psi(w,D)}-1,\ 1-e^{-\psi(w,D)}\,\} \\ &\qquad = e^{\psi(w,D)}-1. \end{aligned} \qquad \text{(4–5)}$$

By our earlier results,

$$h = q^g\,L(1/q) = q^g\left(1-q^{-1}\right)^{-1}\prod_{P}\left(1-\frac{\chi(P)}{|P|}\right)^{-1}.$$

We set

$$E'(w,D) = q^g\,(1-q^{-1})^{-1}\prod_{|P|\le q^w}\left(1-\frac{\chi(P)}{|P|}\right)^{-1}, \qquad \text{(4–6)}$$

and let our estimate of $h$ be defined by

$$E(w,D) = \operatorname{rnd}(E'(w,D)), \qquad \text{(4–7)}$$

where $\operatorname{rnd}(y)$ denotes the nearest integer to $y$. Then

$$|h - E(w,D)| < E'(w,D)(e^{\psi(w,D)}-1) + \tfrac{1}{2}$$

by (4–5). Putting

$$L(w,D)=\left\lceil \sqrt{E'(w,D)(e^{\psi(w,D)}-1)+\tfrac{1}{2}}\,\right\rceil, \qquad (4\text{–}8)$$

we get

$$|h-E(w,D)|<L^2(w,D). \qquad (4\text{–}9)$$

We also need to show that $E(w,D)$ can not become too large.

**Theorem 4.1.** *There exist positive constants $c, c^*$ such that*

$$c^*\,\frac{1}{w}\,q^g<E(w,D)<c\,wq^g.$$

*Proof.* Put

$$M(w,D)=\prod_{|P|\le q^w}\left(1-\frac{\chi(P)}{|P|}\right)^{-1},$$

$$M(w)=\prod_{|P|\le q^w}\left(1-\frac{1}{|P|}\right)^{-1},$$

$$M^*(w)=\prod_{|P|\le q^w}\left(1+\frac{1}{|P|}\right)^{-1}.$$

It suffices to show that $M(w)=O(w)$ and $M^*(w)=\Omega(1/w)$. We have

$$M(w)=\prod_{\nu=1}^{w}\left(1-\frac{1}{q^\nu}\right)^{-n_\nu}$$

and

$$n_\nu=\frac{q^\nu}{\nu}+t_\nu,$$

where

$$|t_\nu|\le\sum_{i=0}^{\lfloor\nu/2\rfloor}\frac{q^i}{\nu}<\frac{3q^{\nu/2}}{2\nu}.$$

Since

$$\left(1-\frac{1}{q^\nu}\right)^{-1}=1+\frac{1}{q^\nu-1}<\exp\left(\frac{1}{q^\nu-1}\right),$$

we get

$$\log M(w)\le\sum_{\nu=1}^{w}\frac{n_\nu}{q^\nu-1}\le\sum_{\nu=1}^{w}\frac{1}{\nu}+T,$$

where

$$|T|<\frac{3}{2}\sum_{\nu=1}^{\infty}\frac{1}{\nu\,(q^{\nu/2}-1)}.$$

It follows that

$$\log M(w)=\log w+O(1);$$

hence,

$$M(w)=O(w).$$

Similarly, one can show that $M^*(w)=\Omega(1/w)$. □

**Corollary 4.2.** *If*

$$\psi(w,D)=\frac{(2g+3)\,q^{-w/2}}{q^{1/2}-1}<1,$$

*there exist positive constants $C, C^*$ such that*

$$C^*\,\frac{1}{\sqrt{w}}\,\sqrt{g}\,q^{(g/2)-(w+1/4)}<L(w,D)$$
$$<C\,\sqrt{w}\,\sqrt{g}\,q^{(g/2)-(w+1/4)}.$$

*Proof.* Note that $0<y\le a/b<1$ implies

$$e^y-1<\frac{2b-a}{2(b-a)}\,y.$$

Thus, if $\psi(w,D)<1$, there exist $a,b\ge 0$ such that $\psi(w,D)\le a/b<1$. From this we derive that

$$e^{\psi(w,D)}-1<\frac{2b-a}{2(b-a)}\,\psi(w,D).$$

Also, $e^{\psi(w,D)}-1>\psi(w,D)$. The result then follows from (4–4), (4–8), and Theorem 4.1. □

### 4B. Computation of R

Let $y$ be any nonnegative integer and define the principal ideal $\mathfrak{a}(y)$ by $\mathfrak{a}(y)=\mathfrak{a}_k$, where

$$\delta(\mathfrak{a}_k,\mathfrak{a}_1)\le y,\quad \delta(\mathfrak{a}_{k+1},\mathfrak{a}_1)>y.$$

Since $\delta(\mathfrak{a}_{j+1},\mathfrak{a}_j)\ge 1$, we see that $\mathfrak{a}(y)$ is well defined. We also note that $\mathfrak{a}(y)$ can be computed in $O(\deg D\log y)$ baby steps and giant steps. This can be easily: let

$$y=2^kb_0+2^{k-1}b_1+\cdots+b_k,$$

where $b_0=1$ and $b_i=0$ or $1$ for $1\le i\le k$, be the binary representation of $y$. That is, if $s_0=1$ and $s_{n+1}=2s_n+b_{n+1}$ for $n=0,1,2,\dots k+1$, then $s_k=y$ and $k=\lceil\log_2 y\rceil$. For a given $n$, let $\mathfrak{a}_m=\mathfrak{a}(s_n)$ and let $\mathfrak{a}_r=\mathfrak{a}_m*\mathfrak{a}_m$; then

$$\delta(\mathfrak{a}_r,\mathfrak{a}_1)=2\delta(\mathfrak{a}_m,\mathfrak{a}_1)+f,$$

where $-\deg D+2\le f\le 0$. Also, $\delta(\mathfrak{a}_{m+1},\mathfrak{a}_m)\le\frac{1}{2}\deg D$; thus,

$$2s_n-2\deg D+2\le\delta(\mathfrak{a}_r,\mathfrak{a}_1)\le 2s_n.$$

It follows that, given $\mathfrak{a}(s_n)$ and $\delta(\mathfrak{a}(s_n),\mathfrak{a}_1)$, we need only perform one giant step and at most $2\deg D$

baby steps, starting at $\mathfrak{a}_r$, in order to find $\delta(\mathfrak{a}_t, \mathfrak{a}_1)$ and $\mathfrak{a}_t$ $(= \mathfrak{a}(s_{n+1}))$ such that

$$\delta(\mathfrak{a}_t, \mathfrak{a}_1) \le 2s_n + b_{n+1} = s_{n+1}, \quad \delta(\mathfrak{a}_{t+1}, \mathfrak{a}_1) > s_{n+1}.$$

We will also require the following simple observation, which we state here as a lemma.

**Lemma 4.3.** *Let $T, F \in \mathbb{Z}$ and $0 \le T \le F$. If $\mathfrak{a}$ and $\mathfrak{b}$ are reduced principal ideals such that*

$$\delta(\mathfrak{a}, \mathfrak{a}_1) \equiv \delta(\mathfrak{b}, \mathfrak{a}_1) + T \pmod{R},$$

*then $\mathfrak{a} = \mathfrak{b}_i$, where $\mathfrak{b}_1 = \mathfrak{b}$. Furthermore, $1 \le i \le n$ for any $n$ such that $\delta(\mathfrak{b}_n, \mathfrak{b}_1) \ge F$.*

*Proof.* Since $\mathfrak{a}$ and $\mathfrak{b}$ are reduced and principal, we know by Theorem 3.5 and some of our later observations that we may assume $\mathfrak{a} = \mathfrak{a}_r$, $\mathfrak{b} = \mathfrak{a}_s$ with $1 \le r, s \le m$, where $m$ is the quasi period of the continued fraction expansion of $\alpha = \sqrt{D}$. If $r < s$, replace $r$ by $r + m \ge s$. We now have $r \ge s$ and

$$\begin{aligned}\delta(\mathfrak{a}_r, \mathfrak{a}_1) &= \delta(\mathfrak{a}_s, \mathfrak{a}_1) + T \le \delta(\mathfrak{a}_s, \mathfrak{a}_1) + F \\ &\le \delta(\mathfrak{a}_s, \mathfrak{a}_1) + \delta(\mathfrak{a}_{n+s-1}, \mathfrak{a}_s) \\ &= \delta(\mathfrak{a}_{n+s-1}, \mathfrak{a}_1).\end{aligned}$$

It follows that $r \le s + n - 1$. If we put $r = s + i - 1$, then $i \ge 1$ and $i \le n$; also, $\mathfrak{a}_r = \mathfrak{b}_i$. □

First note that for $\deg D \le 6$, i.e. $g = 1$ or 2, we obtain a better approximation of $h$ by making use of (3–13). In this case, the approximation of $h$ is given immediately without further computations. Also, it will turn out for $g \ge 3$ that the optimal choice for $w$ is $w = (2g - 1)/5$. For the approximation of $h$, we need $w \in \mathbb{N}$, and therefore set there $w = \operatorname{rnd}((n - 3)/5)$, where $n = \deg D = 2g + 2$. Then $w = \lfloor n/5 \rfloor - 1$, if $n \equiv 0 \pmod{10}$, and $w = \lfloor n/5 \rfloor$, otherwise. We also assume that $q$ is sufficiently large that $\psi(w, D) < 1$.

**Algorithm 4.4 (Regulator2).**

```
Input: $k = \mathbb{F}_q$ and $D \in k[x]$ monic, squarefree of even
    degree.
Output: $R$, the regulator of $k(x)(\sqrt{D})$.

1. If $g = 1$, set $s \leftarrow \lfloor q^{1/3} \rfloor$;  $G \leftarrow \lfloor q^{1/2} \rfloor$;
       $E \leftarrow q + 1$;  $L \leftarrow \lceil \sqrt{2}\, q^{1/4} \rceil$.
   If $g = 2$, set $s \leftarrow \lfloor q^{2/3} \rfloor$;  $G \leftarrow \lfloor q^{4/3} \rfloor$;
       $E \leftarrow q^2 + 6q + 1$;  $L \leftarrow \lceil 2\, q^{1/4} \sqrt{q + 1} \rceil$.
   If $g \ge 3$, set $s \leftarrow \lfloor q^{(2g-1)/5} \rfloor$;  $G \leftarrow \lfloor q^{(4g-2)/5} \rfloor$;
       $w \leftarrow \operatorname{rnd}((2g - 1)/5)$; compute $E$ and $L$ by
       (4–4), (4–6), (4–7), and (4–8).
2. Use Algorithm 3.8 to test whether $R \le G$. If
   $R \le G$, return $R$.
3. We have $R > G$ and $|h - E| < L^2$. Compute a
   multiple $h_0 = h^* R$ of $R$ such that $h_0 < E + L^2$,
   as follows:
   a. Determine $\mathfrak{a}_k = \mathfrak{a}(E)$, $\delta_k$, $\mathfrak{a}_s = \mathfrak{a}(L)$, and $\delta_s$.
   b. Let $\mathfrak{b}_1 \leftarrow \bar{\mathfrak{a}}_k$ and proceed in baby steps from $\mathfrak{b}_1$
      to produce the ideals $\mathfrak{b}_1, \mathfrak{b}_2, \mathfrak{b}_3, \dots, \mathfrak{b}_t$ with dis-
      tance $\delta'_1, \delta'_2, \dots, \delta'_t$, where $\delta'_i \leftarrow \delta(\mathfrak{b}_i, \mathfrak{b}_1)$, until
      $\delta'_t > \delta_s + \frac{1}{2} \deg D$. Put $\mathcal{S} = \{\mathfrak{b}_1, \mathfrak{b}_2, \mathfrak{b}_3, \dots, \mathfrak{b}_t\}$.
   c. Set $\mathfrak{c}_1 \leftarrow \mathfrak{a}_s$ and $\delta^*_1 \leftarrow \delta_s$. For $j \ge 2$ define $\mathfrak{c}_j$
      and $\delta^*_j$ recursively by
          $(\mathfrak{c}_j, f_j) \leftarrow \mathfrak{c}_1 * \mathfrak{c}_{j-1}$,   $\delta^*_j \leftarrow \delta(\mathfrak{c}_j, \mathfrak{a}_1)$,
      proceeding until $\mathfrak{c}_j \in \mathcal{S}$ or $\bar{\mathfrak{c}}_j \in \mathcal{S}$ for some $j$.
   d. If $\mathfrak{c}_j = \mathfrak{b}_i$ then $h_0 \leftarrow \delta^*_j - \delta(\mathfrak{b}_i, \mathfrak{a}_1)$.
      If $\bar{\mathfrak{c}}_j = \mathfrak{b}_i$ then $h_0 \leftarrow \delta^*_j + \delta(\mathfrak{b}_i, \mathfrak{a}_1) - \deg N(\mathfrak{b}_i)$.
4. We have $h_0 = h^* R$, where $h_0 < E + L^2$. Put
   $B \leftarrow (E + L^2)/G$ and $h^* \leftarrow 1$. For each rational
   prime divisor $r$ of $h_0$ such that $r < B$, do:
   a. Compute $\mathfrak{a}(h_0/r^\beta)$ for $\beta = 1, 2, \dots$ until find-
      ing the least $\beta$ such that $|N(\mathfrak{a}(h_0/r^\beta))| \ne 1$.
   b. Set $h^* \leftarrow h^*\, r^{\beta-1}$;  $B \leftarrow B/r^{\beta-1}$.
5. Set $R \leftarrow h_0/h^*$ and return $R$.
```

In step 3 we have $|h - E| < L^2$ by (3–13) and (4–9). If $\delta(\mathfrak{a}_v, \mathfrak{a}_1) = h = h'R$, it is likely that $\mathfrak{a}_v$ will tend to have distance from $\mathfrak{a}_1$ which is close to $E$ rather than farther away. In the case of quadratic number fields this was observed by Nield and Shanks [1974]. Thus, it is most efficient to start searching for $\mathfrak{a}_v$ by examining those ideals which are closest to $E$ and then moving farther away in each direction. That this sort of search can be easily conducted is demonstrated by the following theorem.

**Theorem 4.5.** *If $\delta^*_n > L^2 + \deg D$, then $\mathfrak{c}_j$ or $\bar{\mathfrak{c}}_j \in \mathcal{S}$ for some $j$ such that $1 \le j \le n$.*

*Proof.* We consider two cases, depending on whether or not $h \ge \delta(\mathfrak{a}_k, \mathfrak{a}_1) - \deg N(\mathfrak{a}_k)$. Since both cases have similar proofs, we will provide a proof for the case when $h \ge \delta(\mathfrak{a}_k, \mathfrak{a}_1) - \deg N(\mathfrak{a}_k)$ only. We will make use of the notation established above.

Since $\delta(\mathfrak{a}_k, \mathfrak{a}_{k-1}) \le \frac{1}{2} \deg D$, we have

$$\begin{aligned}-\deg N(\mathfrak{a}_k) \le \delta_m - \delta_k &\le h'\, R - E + \tfrac{1}{2} \deg D \\ &< L^2 + \tfrac{1}{2} \deg D.\end{aligned}$$

Also, by (3–10) and Remark 3.6

$$\delta_k = t_1 R - \delta(\bar{\mathfrak{a}}_k, \mathfrak{a}_1) + \deg N(\mathfrak{a}_k)$$

for some $t_1 \in \mathbb{Z}$; thus,

$$0 < \delta_v + \tilde{\delta}_k - t_1 R < L^2 + \deg D.$$

Let $F = \delta_v + \tilde{\delta}_k - t_1 R$ and there exists $j \leq n$ such that $\delta^*_{j-1} \leq F < \delta^*_j$; hence, if $s = \delta^*_j - F$, we have $0 < s \leq \delta^*_1$. Since

$$\tilde{\delta}_k + s \equiv \delta^*_j (\operatorname{mod} R),$$

we must have $\mathfrak{c}_j \in \mathcal{S}$ by Lemma 4.3. □

Notice that we must find some $\mathfrak{c}_j$ or $\bar{\mathfrak{c}}_j \in \mathcal{S}$ by performing only $O(L)$ giant steps and $O(L)$ baby steps. Furthermore, if $\mathfrak{c}_j = \mathfrak{b}_i$, then $R \mid \delta^*_j - \delta(\mathfrak{b}_i, \mathfrak{a}_1)$ and if $\bar{\mathfrak{c}}_j = \mathfrak{b}_i$, then $R \mid \delta^*_j + \delta(\mathfrak{b}_i, \mathfrak{a}_1) - \deg N(\mathfrak{b}_i)$. Thus, this theorem provides us with an algorithm which finds an integral multiple of $R$ in $O(L)$ polynomial operations. As $j$ here increases we are searching the region bounded by $E - L^2$ and $E + L^2$ by starting near $E$ and moving farther and farther from $E$ in both directions in order to find $h^*R$ such that $h^*R < E + L^2$. In step 4 of Algorithm 4.4, we compute $h^*$. We first note that $h^* < (E + L^2)/R < B$. Thus, if $r$ is a rational prime divisor of $h^*$, then $r$ must be a divisor of $h^*R$ and $r < B$. Also, if $r^{\beta-1} \parallel h^*$, then $N(\mathfrak{a}(h^*R/r^\beta)) \neq 1$, and $N(\mathfrak{a}(h^*R/r^i)) = 1$ for $1 \leq i \leq \beta - 1$. The method in step 4 certainly determines $h^*$ and then $R = h^*R/h^*$.

Now we discuss the correct choice of $w$ for $g \geq 3$. If we always assume that $n$ is sufficiently small compared to $q$, we obtain from Theorem 4.1, Corollary 4.2 and (4–4) that $E(w, D) = O(q^g)$, $\psi(w, D) = O(q^{(-w-1)/2})$, $L(w, D) = O(q^{(g/2)-(w+1)/4})$, and $L(w, D) = \Omega(q^{(g/2)-(w+1)/4})$. Because there are only $O(q^w)$ primes $P$ such that $|P| \leq q^w$ and because the evaluation of the symbol $\left[\frac{D}{P}\right]$ can be done in $O(\deg D + \log q)$ operations, we see that the evaluation of $E = E(w, D)$ can be done in $O(q^w)$ polynomial operations. We then let

$$G := E(w, D)/\sqrt{q\ L(w, D)} = O(q^{(3/4)g+(w-3)/8}).$$

We thus obtain $B = (E(w, D) + L(w, D)^2)/G = O(q^{(g/4)-(\alpha-3)/8})$. From this we derive that the optimal choice for $w$ is $w = (2g - 1)/5$, and Algorithm 4.4 determines $R$ unconditionally in

$$O(q^{(2/5)g}) = O(|D|^{1/5})$$

polynomial operations. In particular, in the case $g \equiv 3 \pmod 5$, Algorithm 4.4 performs $O(q^{(2g-1)/5})$ polynomial operations. For instance, if $g = 3$, Algorithm 4.4 determines $R$ in $O(q)$ polynomial operations. In the cases $g = 1$ or 2, we derive faster methods, since the approximation of $h$ is given directly by (3–13). By the same arguments as above, we can find $R$ unconditionally in $O(q^{1/4})$ or $O(q^{3/4})$ polynomial operations if $g = 1$ or 2, respectively.

The methods of Buchmann and Williams [1989] can be employed to provide an algorithm which will find $h'$ (given a divisor $\tilde{h}$ of $h'$) in $O(q^{\deg D}/(R\tilde{h})^2)$ polynomial operations. Also, if $h' < q^\beta$, then we can compute $h$ in $O(q^{2\beta}/(\tilde{h})^2)$ polynomial operations; thus, if, as is frequently the case, $h'$ is small, we can compute $h'$ quickly. We do this by putting $H = h'/\tilde{h}$, and $\tilde{H}$ =Ne$(E'(w, D)/(\tilde{h}R))$, where $E'(w, D)$ is given by (4–6). Here, we make use of $\psi(w, D)$ as defined in (4–4), or any other upper bound on $|B(w, D)|$. If we put

$$F = \left| \frac{E'(w, D)}{(\tilde{h}R)} - \tilde{H} \right|,$$

then $H = \tilde{H}$ when $w$ is large enough that

$$\log \frac{\tilde{H} + 1}{\tilde{H} + F} > \psi(w, D).$$

## 5. COMPUTATIONS

### 5A. General Features

Our computations were run on a Sun SPARC Ultra 1/140 under Solaris 2.5. We made use of the computer algebra system SIMATH [Zimmer et al. 1997], written in C and developed by the research group of Prof. H. G. Zimmer at the Universität des Saarlandes in Saarbrücken, Germany. All our computations were done over prime fields $\mathbb{F}_p$, i.e., $q = p$ prime, and $p < 2^{30} - 1$. The discriminants $D$ were selected as follows: For an even number $n$ and a prime $p$ we randomly constructed a monic, squarefree polynomial $D$ of degree $n$ in $\mathbb{F}_p[x]$. For small regulators ($R \leq 10^6$), Algorithm 3.8 is completely sufficient. We were more interested in what happens if the regulator becomes large. When will Algorithm 4.4 be faster? And, what will be its limit of utility? In view of the condition $\psi(w, D) < 1$ and the limits for the approximation (see below), we restricted our attention for $p$ and $n = \deg D$ to the range in Table 1.

| $p$ | $n$ | $p$ | $n$ | $p$ | $n$ |
|---|---|---|---|---|---|
| 3 | 40–50 | 11 | 10–34 | 41–113 | 4–18 |
| 5 | 20–44 | 13, 17 | 4–28 | 127–1409 | 4–14 |
| 7 | 16–38 | 19–37 | 4–24 | 1423–$2^{30}$ | 4–8 |

**TABLE 1.** Computation range

Moreover, we generally bounded the number of baby steps in Algorithm 3.8 by 100000 because of space restrictions, since, for each computed ideal, one has to store 2 polynomials of degree less than or equal $g$, and one integer $\delta$ which represents the distance of the stored ideal. For the baby step – giant step part of Algorithm 4.4 we limited the number of baby steps to 20000, when $p^g < 10^{12}$. In general, the maximal number of baby steps was set to 100000 except for $g=1$ or 2. When $g=1$, 2, we limited the number of baby steps to 400000 and 300000, respectively. Algorithm 4.4 works best in those cases where the genus is small. If, in addition, $p$ is large, the approximation is more accurate, since then, by (4–4), $\psi(w, D)$ is small. The crossover, where Algorithm 4.4 becomes more efficient than the optimized baby step – giant step algorithm, occurs pretty early. Indeed, we discovered that Algorithm 4.4 should be used as soon as $R \geq 10^8$.

To get an accurate approximation, however, we restricted ourselves to the case $\psi(w, D) < 1$. This condition is true for $p = 3$ and $w \geq 8$, for $p = 5$ and $w \geq 4$, for $p = 7$ and $w \geq 3$, for $p = 11$ and $w \geq 2$, for $p \geq 13$ and $w \geq 1$.

## 5B. Approximation Details

To compute the approximation

$$E(w, D) = \operatorname{rnd}(E'(w, D))$$

of $h$, we used the formula

$$E'(w, D) = \frac{q^{g+1}}{q-1} \prod_{\nu=1}^{w} F(\nu, D),$$

where, for $1 \leq \nu \leq \alpha$,

$$F(\nu, D) = \prod_{|P|=q^\nu} \frac{q^\nu}{q^\nu - \chi(P)} = \left(\frac{q^\nu}{q^\nu - 1}\right)^{s_\nu} \left(\frac{q^\nu}{q^\nu + 1}\right)^{t_\nu},$$

and $s_\nu$, $t_\nu$ denote the sum over all monic prime polynomials of degree $\nu$ with $\chi(P) = 1$ and $\chi(P) = -1$, respectively. For each $\nu$ we first generated all monic, prime polynomials $P$ of degree $\nu$ and then computed $\chi(P) = \left[\frac{D}{P}\right]$. Finally, two binary exponentiations yield $F(\nu, D)$. Note that the generation of all monic, prime polynomials of a given degree could be precomputed. But, since the time for this step is very small compared to the evaluation of the $\left[\frac{D}{P}\right]$, we included the generation in the algorithm and thus in the total running time.

Note that each monic polynomial of degree 1 is prime. For the generation of all monic, prime polynomials of a degree $\nu \geq 2$, we used a sieving procedure analogous to the sieve of Eratosthenes. We installed an array LP of dimension $\nu$ with $p^{\nu-1}(p-1)$ entries. Each dimension $l$ of the array, $1 \leq l \leq \nu$, represents the possible coefficients for $x^{l-1}$ over $\mathbb{F}_p$. First, we put $LP[i_1][i_2]\dots[i_\nu] \leftarrow 0$ for $0 \leq i_1, i_2, \dots, i_{\nu-1} \leq p-1$ and $1 \leq i_\nu \leq p-1$. We then set $LP[i_1][i_2]\dots[i_\nu]$ to 1, if its corresponding polynomial $x^\nu + i_1 x^{\nu-1} + i_2 x^{\nu-2} + \dots + i_{\nu-1}x + i_\nu$ has a factor of degree less than $\nu$. The remaining entries of the array with value 0 then represent the monic, prime polynomials of degree $\nu$. Of course, this method caused restrictions in the choice of $p$ and $n$ because of space limitations (see Table 1).

Most of the time needed by Algorithm 4.4 is spent on the search for a multiple of the regulator in the approximated interval and the test of whether $R$ is less than the bound $G$. In comparison to these steps, the approximation, most of whose time is spent on the evaluation of the Artin symbols, takes much less time. For instance, if $q = 1000003$ and $D = x^8 + 17174x^7 + 4215x^6 + 77454x^5 + 97416x^4 + 68883x^3 + 51968x^2 + 59249x + 98911$, the approximation took 13.25 sec, whereas the total running time was 4 min 23.42 sec, and the search for a multiple was performed in 2 min 4.88 sec. For $q = 2999999$ and $D = x^8 + 1714883x^7 + 2925166x^6 + 256938x^5 + 2705750x^4 + 722268x^3 + 1261069x^2 + 2139572x + 1286480$, the approximation took 8 min 10.66 sec, the search for a multiple 9 h 7 min 3.46 sec, and the total running time was 9 h 24 min 15.58 sec.

## 5C. Examples

We calculated the regulator $R$ of $\mathbb{F}_q(x)(\sqrt{D})$ for representative examples. There are two weighted parameters, $q$ and $D$; increasing one of them, the degree of $D$ or $q$, causes the value of $h$ (and frequently

| $p$ | $D$ | $R$ | $h'$ | $T_1$ | $T_2$ |
|---|---|---|---|---|---|
| 5 | $x^{28}+3x^{27}+2x^{26}+2x^{25}+3x^{22}+x^{21}+x^{20}+x^{18}+x^{16}+4x^{15}+x^{14}+x^{13}+2x^{12}+2x^{11}+4x^{10}+x^9+x^8+2x^7+2x^5+3x^4+x^3+x^2+3x$ | 1711004395 | 1 | $1\frac{1}{2}$ m | 11.9 s |
| 13 | $x^{18}+5x^{17}+8x^{16}+6x^{14}+x^{13}+9x^{12}+5x^{11}+3x^{10}+2x^9+9x^7+x^6+10x^5+11x^4+5x^3+7x^2+4x+4$ | 905254803 | 1 | 28.8 s | 6.3 s |
| 17 | $x^{12}+9x^{11}+9x^{10}+7x^9+6x^8+8x^7+12x^6+15x^5+4x^4+13x^3+x^2+13x+1$ | 533867 | 2 | 0.3 s | 0.3 s |
| 17 | $x^{18}+10x^{17}+15x^{16}+13x^{15}+13x^{14}+13x^{13}+11x^{12}+16x^9+15x^8+7x^7+11x^6+9x^5+2x^4+9x^3+16x^2+3x+2$ | 10073466875 | 1 | $2\frac{1}{2}$ m | 13.2 s |
| 37 | $x^8+27x^7+28x^6+25x^5+11x^4+10x^3+16x^2+24x+32$ | 43190 | 1 | 0.06 s | 0.12 s |
| 37 | $x^{10}+34x^9+24x^8+8x^7+9x^6+30x^5+16x^4+7x^3+9x^2+8x+21$ | 999683 | 2 | 0.48 s | 0.40 s |
| 37 | $x^{16}+9x^{15}+20x^{14}+23x^{13}+15x^{12}+34x^{11}+10x^{10}+14x^9+x^8+32x^7+10x^6+21x^5+26x^4+33x^3+21x^2+30x+10$ | 59424264612 | 2 | $13\frac{3}{4}$ m | 38 s |
| 67 | $x^{14}+37x^{13}+22x^{12}+31x^{11}+28x^{10}+46x^9+53x^8+7x^7+66x^6+13x^5+47x^4+12x^3+13x^2+23x+41$ | 120619212829 | 1 | 20 m | 20 s |
| 113 | $x^{12}+89x^{11}+36x^{10}+32x^9+20x^8+9x^7+91x^6+79x^5+112x^4+103x^3+102x^2+100x+79$ | 4260652533 | 4 | $1\frac{3}{4}$ m | 12 s |
| 991 | $x^8+587x^7+816x^6+53x^5+655x^4+593x^3+145x^2+845x+141$ | 961388306 | 1 | 15.8 s | 1.5 s |
| 1409 | $x^8+912x^7+195x^6+297x^5+992x^4+536x^3+187x^2+1267x+1194$ | 2778312114 | 1 | 25.6 s | 2 s |
| 4999 | $x^8+4191x^7+3516x^6+263x^5+4611x^4+2053x^3+4470x^2+3811x+480$ | 62540548337 | 2 | $4\frac{3}{4}$ m | 8.5 s |
| 10009 | $x^6+5900x^5+7039x^4+7066x^3+2077x^2+1695x+847$ | 17016964 | 6 | 10.7 s | 0.5 s |
| 10000019 | $x^4+4550373x^3+3927926x^2+2605091x+5654317$ | 10000600 | 1 | 13.2 s | 0.2 s |
| 100000007 | $x^4+48629505x^3+48744281x^2+80197137x+17182861$ | 50001969 | 2 | 14.1 s | 0.3 s |
| 1000000007 | $x^4+557289356x^3+722527380x^2+352336240x+641315936$ | 1000041901 | 1 | 22.4 s | 0.5 s |

**TABLE 2.** Comparison of running times for regulator computations, using SIMATH implementations on a Sun SPARC Ultra 1/140 running Solaris 2.5. $T_1$ is the time needed with Algorithm 3.8, the baby step – giant step method, and $T_2$ the time needed for determining the regulator with Algorithm 4.4, by approximating $h$.

the regulator) to increase. Table 2 compares the running times of Algorithm 3.8 and Algorithm 4.4.

Note that $h$ is just the product of $h'$ and $R$. The computation of the ideal class number does not need additional time if the methods in the end of Section 4B apply. In fact, the time needed to compute $h'$ is equivalent to the time needed to compute the approximation, which, as mentioned above, is considerably less than the total running time of the regulator algorithm. In all cases $\tilde{h} = 1$ was sufficient.

Table 3 lists examples with large regulators, which can not be computed in a reasonable amount of time by the baby step – giant step algorithm.

## ACKNOWLEDGMENTS

We thank two anonymous referees for helpful comments. Furthermore, the first author is indebted to Hugh Williams for his support and the invitation to work with him at the University of Manitoba in

| $p$ | $D$ | $R$ | $h'$ | $T_2$ |
|---:|---|---:|---:|---:|
| 3 | $x^{50}+x^{48}+x^{46}+x^{44}+x^{42}+x^{41}+x^{40}+x^{38}+x^{36}+x^{34}+x^{32}+x^{30}+2x^{27}+2x^{25}+2x^{23}+x^{22}+x^{20}+x^{18}+x^{17}+2x^{15}+x^{14}+x^{12}+x^{11}+2x^{9}+x^{8}+x^{6}+x^{4}+x^{3}+x^{2}+1$ | 823335273345 | 1 | $10\frac{1}{2}$ m |
| 13 | $x^{28}+3x^{25}+5x^{24}+10x^{23}+3x^{22}+9x^{21}+12x^{20}+x^{19}+10x^{18}+4x^{17}+7x^{16}+2x^{15}+2x^{14}+x^{13}+3x^{12}+12x^{11}+5x^{9}+2x^{8}+6x^{7}+x^{6}+2x^{5}+10x^{4}+x^{3}+11x^{2}+10x+5$ | 167061012368298 | 2 | $1\frac{1}{4}$ h |
| 17 | $x^{20}+2x^{19}+8x^{18}+12x^{17}+5x^{16}+15x^{15}+3x^{14}+4x^{13}+16x^{12}+13x^{11}+4x^{10}+5x^{9}+7x^{8}+9x^{7}+6x^{6}+4x^{5}+13x^{4}+2x^{3}+9x^{2}+7$ | 164483425957 | 1 | $1\frac{1}{4}$ m |
| 37 | $x^{22}+31x^{21}+17x^{20}+33x^{19}+33x^{18}+27x^{17}+25x^{16}+4x^{15}+16x^{14}+35x^{13}+9x^{12}+19x^{11}+16x^{10}+2x^{9}+26x^{8}+3x^{7}+15x^{6}+6x^{5}+x^{4}+2x^{3}+8x^{2}+7x+2$ | 143889561838517 | 32 | $2\frac{1}{4}$ h |
| 113 | $x^{16}+28x^{15}+83x^{14}+102x^{13}+92x^{12}+71x^{11}+6x^{10}+98x^{9}+104x^{8}+12x^{7}+66x^{6}+14x^{5}+100x^{4}+72x^{3}+7x^{2}+76x+9$ | 222317710463877 | 1 | 18 m |
| 1409 | $x^{12}+458x^{11}+978x^{10}+339x^{9}+372x^{8}+874x^{7}+806x^{6}+511x^{5}+73x^{4}+1388x^{3}+852x^{2}+1337x+869$ | 664973740977494 | 8 | $24\frac{1}{4}$ m |
| 2999999 | $x^{8}+637021x^{7}+1126126x^{6}+1503554x^{5}+1345264x^{4}+2946924x^{3}+1822234x^{2}+1118142x+203383$ | 2701685961518879123 | 10 | $3\frac{3}{4}$ h |
| 2999999 | $x^{8}+1714883x^{7}+2925166x^{6}+256938x^{5}+2705750x^{4}+722268x^{3}+1261069x^{2}+2139572x+1286480$ | 9001031984873848717 | 3 | $9\frac{1}{2}$ h |
| 4000037 | $x^{8}+1951801x^{7}+3708092x^{6}+3700497x^{5}+33188x^{4}+3264226x^{3}+1754294x^{2}+3133810x+2240125$ | 32003976721016837378 | 2 | $17\frac{1}{2}$ h |
| 10000019 | $x^{6}+497381x^{5}+8594888x^{4}+1683380x^{3}+8440589x^{2}+93784x+2625724$ | 24992015081505 | 4 | $3\frac{1}{4}$ m |
| 100000007 | $x^{6}+63507230x^{5}+401005x^{4}+88907241x^{3}+87113022x^{2}+12543588x+67407187$ | 10000127721908079 | 1 | $16\frac{1}{2}$ m |
| 1073741741 | $x^{6}+205912371x^{5}+859304427x^{4}+77543919x^{3}+603307144x^{2}+131571390x+807786564$ | 288230461703812884 | 4 | $36\frac{1}{2}$ m |

**TABLE 3.** Regulator computations with Algorithm 4.4 for large examples. $T_2$ is the running time, as in Table 2.

Winnipeg. This work was completed during a postdoctoral stay of the first author at the Department of Computer Science.

## REFERENCES

[Artin 1924a] E. Artin, "Quadratische Körper im Gebiete der höheren Kongruenzen I", *Mathematische Zeitschrift* **19** (1924), 153–206.

[Artin 1924b] E. Artin, "Quadratische Körper im Gebiete der höheren Kongruenzen II", *Mathematische Zeitschrift* **19** (1924), 208–246.

[Buchmann and Williams 1989] J. Buchmann and H. C. Williams, "On the computation of the class number of an algebraic number field", *Math. Comp.* **53**:188 (1989), 679–688.

[Deuring 1973] M. Deuring, *Lectures on the theory of algebraic functions of one variable*, Lecture Notes in Math. **314**, Springer, Berlin, 1973.

[Eichler 1966] M. Eichler, *Introduction to the theory of algebraic numbers and functions*, Pure Appl. Math. **23**, Academic Press, New York, 1966.

[Lenstra 1982] H. W. Lenstra, Jr., "On the calculation of regulators and class numbers of quadratic fields", pp. 123–150 in *Journées arithmetiques* 1980 (Exeter), edited by J. V. Armitage, London Math. Soc. Lec. Note Ser. **56**, Cambridge U. Press, Cambridge, 1982.

[Neild and Shanks 1974] C. Neild and D. Shanks, "On the 3-rank of quadratic fields and the Euler product", *Math. Comp.* **28** (1974), 279–291.

[Perron 1913] O. Perron, *Die Lehre von den Kettenbrüchen*, Teubner, Leipzig, 1913.

[Reichardt 1936] H. Reichardt, "Der Primdivisorsatz für algebraische Funktionenkörper über einem endlichen Konstantenkörper", *Mathematische Zeitschrift* **40** (1936), 713–719.

[Scheidler et al. 1996] R. Scheidler, A. Stein, and H. C. Williams, "Key-exchange in real quadratic congruence function fields", *Design Codes Cryptogr.* **7**:1-2 (1996), 153–174. Special issue dedicated to Gustavus J. Simmons.

[Schmidt 1931] F. K. Schmidt, "Analytische Zahlentheorie in Körpern der Charakteristik $p$", *Mathematische Zeitschrift* **33** (1931), 1–32.

[Schoof 1982] R. J. Schoof, "Quadratic fields and factorization", pp. 235–286 in *Computational methods in number theory II*, edited by H. W. Lenstra and R. Tijdemans, Mat. Centrum Tracts **155**, Math. Centrum, Amsterdam, 1982.

[Shanks 1971] D. Shanks, "Class number, a theory of factorization and genera", pp. 415–440 in 1969 *Number Theory Institute* (Stony Brook), Proc. Symp. Pure Math. **20**, Amer. Math. Soc., Providence, 1971.

[Shanks 1972] D. Shanks, "The infrastructure of a real quadratic field and its applications", pp. 217–224 in *Proceedings of the Number Theory Conference* (Boulder, 1972), Univ. Colorado, Boulder, CO, 1972.

[Stein 1992] A. Stein, *Baby Step-Giant Step-Verfahren in reell-quadratischen Kongruenzfunktionenkörpern mit Charakteristik ungleich* 2, Diplomarbeit, Univ. des Saarlandes, Saarbrücken, 1992.

[Stein and Zimmer 1991] A. Stein and H. G. Zimmer, "An algorithm for determining the regulator and the fundamental unit of a hyperelliptic congruence function field", pp. 183–184 in *ISSAC* '91 (Bonn, 1991), edited by S. M. Watt, ACM Press, New York, 1991.

[Stephens and Williams 1988a] A. J. Stephens and H. C. Williams, "Some computational results on a problem concerning powerful numbers", *Math. Comp.* **50**:182 (1988), 619–632.

[Stephens and Williams 1988b] A. J. Stephens and H. C. Williams, "Computation of real quadratic fields with class number one", *Math. Comp.* **51**:184 (1988), 809–824.

[Weis and Zimmer 1991] B. Weis and H. G. Zimmer, "Artins Theorie der quadratischen Kongruenzfunktionenkörper und ihre Anwendung auf die Berechnung der Einheiten- und Klassengruppen", *Mitt. Math. Ges. Hamburg* **12**:2 (1991), 261–286.

[Williams and Wunderlich 1987] H. C. Williams and M. C. Wunderlich, "On the parallel generation of the residues for the continued fraction factoring algorithm", *Math. Comp.* **48**:177 (1987), 405–423.

[Zimmer et al. 1997] H. G. Zimmer et al., "SIMATH Manual", Technical report, Saarbrücken, 1997. See http://www.math.uni-sb.de/software.html.

Andreas Stein, Department of Combinatorics and Optimization, University of Waterloo, Waterloo, Ontario, Canada N2L 3G1 (astein@cacr.math.uwaterloo.ca)

Hugh C. Williams, Hugh C. Williams, Department of Computer Science, University of Manitoba, Winnipeg, Manitoba, Canada R3T 2N2 (hugh_williams@csmail.cs.umanitoba.ca)

Received September 23, 1997; accepted in revised form June 16, 1998