GLASNIK MATEMATIČKI
Vol. 44(64)(2009), 89 – 126

EXPLICIT INFRASTRUCTURE FOR REAL QUADRATIC FUNCTION FIELDS AND REAL HYPERELLIPTIC CURVES

Andreas Stein
Carl-von-Ossietzky Universität Oldenburg, Germany

Abstract. In 1989, Koblitz first proposed the Jacobian of a an imaginary hyperelliptic curve for use in public-key cryptographic protocols. This concept is a generalization of elliptic curve cryptography. It can be used with the same assumed key-per-bit strength for small genus. More recently, real hyperelliptic curves of small genus have been introduced as another source for cryptographic protocols. The arithmetic is more involved than its imaginary counterparts and it is based on the so-called infrastructure of the set of reduced principal ideals in the ring of regular functions of the curve. This infrastructure is an interesting phenomenon. The main purpose of this article is to explain the infrastructure in explicit terms and thus extend Shanks' infrastructure ideas in real quadratic number fields to the case of real quadratic congruence function fields and their curves. Hereby, we first present an elementary introduction to the continued fraction expansion of real quadratic irrationalities and then generalize important results for reduced ideals.

1. Introduction

In 1989, Koblitz [14] first proposed the Jacobian of the imaginary model of a hyperelliptic curve for key exchange protocols as a natural extension to protocols based on elliptic curves. In recent years, hyperelliptic curves of small genus have become very popular research topics with a variety of interesting results making its arithmetic almost comparable in speed to elliptic curve arithmetic. In [23], real hyperelliptic curves have been introduced as another source for cryptographic protocols. Its underlying key space was the set of reduced principal ideals in the ring of regular functions of the curve, together

2000 *Mathematics Subject Classification.* 11R58, 11Y16, 11Y65, 11M38.
Key words and phrases. Real hyperelliptic function field, real hyperelliptic curve, infrastructure and distance, reduced ideals, regulator, continued fraction expansion.

with its group-like infrastructure. The arithmetic turned out to be more involved, however the main operation, a *giant step*, is ideal multiplication plus reduction and it is comparable in efficiency to that of the imaginary model as explained in [30]. More recently, in [12] the authors showed that the arithmetic in the real model is almost as fast as the one in imaginary model. The same observation has been made by comparing explicit formulas in the imaginary model (see e.g. [15]) with the real model (see [8]) of small genus. For details on general arithmetic of hyperelliptic curves we refer to [18, 10, 5, 12], and for recent results on real hyperelliptic curves we refer to [34, 23, 33, 19, 30, 7, 12, 11]. There exists an explicit correspondence between real quadratic function fields and real hyperelliptic curves. We refer to [17, 11, 12, 19] for details. From now on, we only consider the arithmetic in the notation of function fields à la Artin.

Since any hyperelliptic function field can be represented as a real quadratic function field, it is important to investigate the arithmetic in real quadratic function fields in detail. We summarize some basic properties and provide elementary proofs of some results. In this view, this paper is intended as a "low-brow" approach to the theory of real quadratic function fields. For the number-theoretic background, we refer to the excellent books of Stichtenoth [38] and Rosen [22]. For the purpose of this paper, only an elementary knowledge of the subject is needed, and we mainly follow the introductory notes of Artin [2]. Most of the results in this paper are stated for convenience in terms of an odd characteristic field. However, all of them carry through to even characteristic fields (see [7, 42, 43, 44]).

Let $k = \mathbb{F}_q$ be a finite field of odd characteristic and let $K = k(x)(\sqrt{D})$, where D is a squarefree polynomial. Such a field is known as a *quadratic function field* over k (of odd characteristic). Throughout, the following terminology will be fixed. The integral closure of $k[x]$ in K is given by $\mathcal{O}_K = \overline{k[x]}$ and is called the *ring of integers of* K. Let $E = {\mathcal{O}_K}^*$ the *group of units* in $\mathcal{O}_K$. If in addition D is monic and of even degree, then K is called a *real quadratic function field* over k (of odd characteristic). If D is monic and of odd degree, we call K imaginary quadratic. For real quadratic function fields of characteristic 2, we refer to [42]. The relationship between the imaginary and the real model has been explained in detail in [19, 29, 30]

If $K = k(x)(\sqrt{D})$ is real quadratic, where $D \in k[x]$ is monic and squarefree, then the *genus* of K is defined by $g = \deg(D)/2 - 1$. K is a Galois extension of the rational function field $k(x)$ with Galois group $\{1, \sigma\}$, where σ is the K-automorphism which takes $\sqrt{D}$ to $-\sqrt{D}$. The *conjugate* of an $\alpha = u + v\sqrt{D} \in K$ with $u, v \in k(x)$ is given by $\overline{\alpha} = \sigma(\alpha) = u - v\sqrt{D}$. The *norm* of α is defined by $N(\alpha) = \alpha \cdot \overline{\alpha} = u^2 - v^2 D$, which gives a rational function. The decomposition of the infinite place $\mathfrak{P}_\infty$ of $k(x)$ in K is $\mathfrak{P}_\infty = \mathfrak{P}_1 \cdot \mathfrak{P}_2$, where $\mathfrak{P}_1$ and $\mathfrak{P}_2$ are the infinite places of K/k. Because

there are exactly two extensions of the infinite place from $k(x)$ to K we can conclude from the Dirichlet unit theorem (see for example [40]) that

$$E = k^* \times \langle \epsilon \rangle,$$

where $\epsilon \in K$ is a fundamental unit. If we denote by $v_{\mathfrak{P}_1}$ and $v_{\mathfrak{P}_2}$ the two normalized extensions of the negative degree valuation $v_{\mathfrak{P}_\infty}$ from $k(x)$ to K, we call the positive integer

$$R = \left| v_{\mathfrak{P}_1}(\epsilon) \right| = \left| v_{\mathfrak{P}_1}(\epsilon) \right| \geq 1$$

the *regulator of K/k with respect to $\mathcal{O}_K$*. We remark here that the regulator is one of the important invariants in real quadratic function fields. A result of F. K. Schmidt [25] shows its connection to further invariants, namely

$$h = R \cdot h',$$

where h' denotes the *ideal class number of K with respect to $\mathcal{O}_K$* and h the *divisor class number of K*. The meaning of these quantities is described in [2, 6].

The purpose of this paper is to show how the infrastructure techniques of Shanks [27], originally applied to real quadratic number fields, can be applied to real quadratic function fields. In order to do this we must first discuss the continued fraction expansion of elements of K. This algorithm goes back to Artin [2] and has been implemented by Weis [39]. We then modify the techniques of [41], [37], and [36] in order to apply Shanks's infrastructure ideas to K. These results, discussed in much greater detail in [34] and [28], provide us new insight into the infrastructure of the ideal class group.

2. Continued Fractions in the Fields of Puiseux Series

The classical method to calculate the fundamental unit of K and the regulator of K is based on the continued fraction expansion of $\alpha = \sqrt{D}$. Many properties of these continued fractions can be found in [2], and [39]; many others can easily be established by proceeding in complete analogy to the case of real numbers, as for instance done in [20] and [41]. Further references are [37, 36, 1]. Therefore let $L := k(x)_{\mathfrak{P}_\infty}$ be the completion of $k(x)$ with respect to $\mathfrak{P}_\infty$. Then L is the field of Puiseux series and the completions of K with respect to $\mathfrak{P}_1$ and $\mathfrak{P}_2$ are isomorphic to L:

$$K_{\mathfrak{P}_1} \cong K_{\mathfrak{P}_2} \cong k(x)_{\mathfrak{P}_\infty} = k((1/x)).$$

Also, K is a subfield of $k((1/x))$, $K \leq k((1/x))$. Now, we only have to fix one of the two places. Let $\mathfrak{P}_1$ be the place which corresponds to the case where $\sqrt{1} = 1$. Then we define continued fraction expansions in K via Puiseux series at $\mathfrak{P}_1$ in the variable $1/x$.

In this section, k can be an arbitrary field. If k is not finite, then we put $q = 2$. For an $\alpha \in L = k((1/x))$ such that $0 \neq \alpha = \sum_{i=-\infty}^{m} c_i x^i$ and $c_m \neq 0$, we define

$$\left\{ \begin{array}{rcl} \deg(\alpha) & = & m, \\ |\alpha| & = & q^m, \\ \operatorname{sgn}(\alpha) & = & c_m, \\ \lfloor \alpha \rfloor & = & \sum_{i=0}^{m} c_i x^i. \end{array} \right\} \tag{2.1}$$

If m is negative, then we have that $\lfloor \alpha \rfloor = 0$. For completeness, we set $\deg(0) = -\infty$ and $|0| = 0$. Now, we introduce continued fraction expansions in L in the sense of Artin. Let $\alpha \in L$ and

$$\left\{ \begin{array}{ll} \alpha_0 := \alpha, & a_0 := \lfloor \alpha_0 \rfloor \\ \alpha_{i+1} := \dfrac{1}{\alpha_i - a_i}, & a_{i+1} := \lfloor \alpha_{i+1} \rfloor \end{array} \right\} \qquad (i \in \mathbb{N}_0). \tag{2.2}$$

Because $\lfloor \alpha \rfloor$ is the unique polynomial such that $|\alpha - \lfloor \alpha \rfloor| < 1$, we note that

$$|\alpha_i| = |a_i| \geq q > 1 \qquad (i \in \mathbb{N}) \,. \tag{2.3}$$

We get

$$\alpha = \alpha_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\ddots}}}} =: [\, a_0,\, a_1,\, a_2,\, \ldots \,] \,. \tag{2.4}$$

As usual, we define

$$\left\{ \begin{array}{lll} p_{-2} := 0; & & q_{-2} := 1 \\ p_{-1} := 1; & & q_{-1} := 0 \\ p_i \;\; := a_i p_{i-1} + p_{i-2}; & & q_i \;\; := a_i q_{i-1} + q_{i-2} \quad (i \in \mathbb{N}_0) \end{array} \right\} . \tag{2.5}$$

We derive by induction that

$$|q_i| > |q_{i-1}| \qquad \text{and} \qquad |q_i| \geq q^i \qquad (i \in \mathbb{N}_0) \,. \tag{2.6}$$

The polynomials p_i and q_i satisfy, for all $i \in \mathbb{N}_0$,

$$\frac{p_i}{q_i} = [\, a_0,\, a_1,\, a_2,\, \ldots,\, a_i \,] \,, \tag{2.7}$$

$$\alpha = \frac{p_i \alpha_{i+1} + p_{i-1}}{q_i \alpha_{i+1} + q_{i-1}} \qquad (i \geq -1) \,, \tag{2.8}$$

or, equivalently,

$$\alpha_{i+1} = -\frac{q_{i-1}\alpha - p_{i-1}}{q_i \alpha - p_i} \qquad (i \geq -1) \,. \tag{2.9}$$

Furthermore,

$$q_i p_{i-1} - p_i q_{i-1} = (-1)^i \qquad (i \geq -1) \tag{2.10}$$

and

$$\alpha - \frac{p_i}{q_i} = \frac{(-1)^i}{q_i(q_i\alpha_{i+1} + q_{i-1})} \qquad (i \geq -1)\,. \tag{2.11}$$

For an $\alpha \in L$ we put

$$\theta_1 := 1 \qquad \theta_{i+1} := \prod_{j=1}^{i} \frac{1}{\alpha_j} \qquad (i \in \mathbb{N}_0), \tag{2.12}$$

and we derive from (2.9) and (2.12) that

$$\theta_{i+1} = (-1)^i\,(p_{i-1} - \alpha q_{i-1}) \qquad (i \in \mathbb{N}_0)\,. \tag{2.13}$$

In contrast to real quadratic number fields it does not suffice to analyze the period of the continued fraction expansion of quadratic irrationalities because the quasi-period plays a more important role. Therefore, we have to distinguish two forms of periodic behavior. Let $\alpha \in L$. We say the continued fraction expansion of α is *quasi-periodic* if there are integers $\nu > \nu_0 \geq 0$ and a constant $c \in k^*$ such that

$$\alpha_\nu = c\,\alpha_{\nu_0}. \tag{2.14}$$

The smallest positive integer $\nu - \nu_0$ for which (2.14) holds is called the *quasi-period* of the continued fraction expansion of α. The continued fraction expansion of α is called *periodic* if (2.14) holds with $c = 1$. The smallest positive integer $\nu - \nu_0$ for which (2.14) holds with $c = 1$ is called the *period* of the continued fraction expansion of α. From [39, Proposition 3.5], we know:

Proposition 2.1. *If the continued fraction expansion of $\alpha \in L$ is periodic with period n, then it is quasi-periodic with quasi-period m and m divides n.*

It is easy to see that for $\alpha \in L$ the period n and the quasi-period m start at the same index ν_0. Thus, the nonnegative integer ν_0 is minimal such that

$$\alpha_{\nu_0+m} = c\,\alpha_{\nu_0} \qquad \text{and} \qquad \alpha_{\nu_0+n} = \alpha_{\nu_0} \tag{2.15}$$

with $c \in k^*$. By induction we get the following helpful lemma:

Lemma 2.2. *If the continued fraction expansion of $\alpha \in L$ is quasi-periodic with quasi-period m then, with ν_0 and c chosen as in (2.15), we have that*

$$\alpha_{i+\lambda m} = c_i^{1+(-1)^m+\ldots+(-1)^{(\lambda-1)m}}\,\alpha_i \qquad (i \geq \nu_0\,,\ \lambda \geq 0)\,,$$

where

$$c_i := c^{(-1)^{i-\nu_0}}.$$

To obtain more information about the relation between the period and the quasi-period we have to distinguish between even and odd periods. In special cases, we will obtain explicit results for even periods.

COROLLARY 2.3. *Let α be an arbitrary element of L.*

(a) *If the continued fraction expansion of α is quasi-periodic with odd quasi-period m, then it is periodic with period n, and $n = m$ or $n = 2m$.*
(b) *If the continued fraction expansion of α is periodic with odd period, then it is quasi-periodic with quasi-period $m = n$.*

PROOF. The first assertion is clear from the above lemma. The second assertion immediately follows from the first assertion and Proposition 2.1. □

3. Real Quadratic Irrationalities and Reduction

Now, let k be a field of odd characteristic. We consider the continued fraction expansion of expressions of the form

$$\alpha = \frac{P + \sqrt{\Delta}}{Q} \qquad (\, 0 \neq Q,\ P,\ \Delta \ \in\ k[x]\,)\,, \tag{3.1}$$

where $\alpha \in L - k(x)$, $0 < \deg(\Delta)$ even, Δ not a perfect square in $k[x]$, and $Q|\left(\Delta - P^2\right)$. We call such an element a *real quadratic irrationality*. In this situation, we put $Q_0 = Q$, $P_0 = P$, $\alpha_0 = \alpha$, $Q_{-1} = (\Delta - P^2)/Q$, and $d = \lfloor \sqrt{\Delta} \rfloor$. For $i \in \mathbb{N}_0$ we use the recursions

$$\left\{ \begin{array}{l} P_{i+1} = a_i Q_i - P_i; \\ Q_{i+1} = \dfrac{\Delta - P_{i+1}^2}{Q_i}\ . \end{array} \right\} \tag{3.2}$$

We immediately have

$$\alpha_i = \frac{P_i + \sqrt{\Delta}}{Q_i} \qquad (i \in \mathbb{N}_0)\,, \tag{3.3}$$

where $0 \neq Q_i, P_i \in k[x]$ and $Q_i|\left(\Delta - P_i^2\right)$. We compute $a_i = \lfloor \alpha_i \rfloor$ by

$$a_i = (P_i + d) \operatorname{div} Q_i \qquad (i \in \mathbb{N}_0)\,. \tag{3.4}$$

Here, we use div and mod, respectively, to denote division and remainder when dividing two polynomials. First, we see from (3.2) that

$$Q_i = Q_{i-1} + a_i(P_i - P_{i+1}) \qquad (i \in \mathbb{N}_0)\,. \tag{3.5}$$

Defining $r_i \in k[x]$ to be the remainder when dividing $P_i + d$ by Q_i, i.e.

$$P_i + d = a_i Q_i + r_i, \text{where } \ 0 \leq \deg(r_i) < \deg(Q_i) \qquad (i \in \mathbb{N}_0)\,, \tag{3.6}$$

we then optimize the formulas as follows:

$$\left\{ \begin{array}{ll} P_{i+1} = d - r_i & (i \in \mathbb{N}_0)\,; \\ Q_{i+1} = Q_{i-1} + a_i(r_i - r_{i-1}) & (i \in \mathbb{N})\,; \\ a_i = (P_i + d\,) \operatorname{div} Q_i & (i \in \mathbb{N}_0)\,; \\ r_i = (P_i + d\,) \bmod Q_i & (i \in \mathbb{N}_0)\,. \end{array} \right\} \tag{3.7}$$

These optimized formulas are an adaptation of the so-called *Tenner's algorithm* known from the real quadratic number field case. We notice that the computation of r_i requires no further effort. Also, by applying (3.3) to (2.9) and comparing rational and irrational parts, we get for $i \in \mathbb{N}_0$:

$$\left\{ \begin{array}{l} \Delta q_{i-1} = P_i(p_{i-1}Q_0 - P_0 q_{i-1}) + Q_i(p_{i-2}Q_0 - P_0 q_{i-2}); \\ Q_0 P_{i-1} = q_{i-1}P_i + q_{i-2}Q_i + P_0 q_{i-1}. \end{array} \right\} \tag{3.8}$$

Finally, we deduce that

$$\mathrm{N}(\theta_{i+1}) = \theta_{i+1}\overline{\theta}_{I+1} = (-1)^i \, \frac{Q_i}{Q_0} \qquad (i \in \mathbb{N}_0)\,. \tag{3.9}$$

A real quadratic irrationality is called *reduced* if $|\overline{\alpha}| < 1 < |\alpha|$, where $\overline{\alpha}$ is the conjugate of α. In view of (3.1), the conjugate of α is $\overline{\alpha} = (P - \sqrt{\Delta})/Q$. So, α is reduced if and only if

$$|P - \sqrt{\Delta}\,| < |\,Q\,| < |P + \sqrt{\Delta}\,|.$$

Remark 3.1. If the real quadratic irrationality α of the form (3.1) is reduced, then we have:

(a) $|P| = |\sqrt{\Delta}\,| = |d|$.
(b) $\mathrm{sgn}(P) = \mathrm{sgn}(\sqrt{\Delta}) = \mathrm{sgn}(d)$. Even the two highest degree coefficients must be equal.
(c) $|Q| < |\sqrt{\Delta}| = |P + \sqrt{\Delta}\,|$.

The proof of this remark is easy and can be found in [2, p. 194]. Also Artin, showed that if α_i is reduced for $i \in \mathbb{N}_0$, then α_j is reduced for $j \geq i$. Combining this fact with the above remark and (3.2) we get the following

Proposition 3.2. *If, in the continued fraction expansion of a real quadratic irrationality α, it happens that α_{i_0} is reduced for some $i_0 \geq 0$, then it follows for $i \geq i_0$:*

(a) $|P_i| = |P_i + \sqrt{\Delta}\,| = |\sqrt{\Delta}\,| = |d|$.
(b) *sgn*$(P_i) =$ *sgn*$(\sqrt{\Delta}) =$ *sgn*(d). *Even the two highest coefficients must be equal.*
(c) $|a_i Q_i| = |\sqrt{\Delta}|$. *In particular, we have that*

$$1 < |a_i| \leq |\sqrt{\Delta}\,|, \quad 1 \leq |Q_i| < |\sqrt{\Delta}\,|.$$

It is well-known that the continued fraction algorithm can be interpreted as a reduction process. In the continued fraction expansion of a real quadratic irrationality there is an index $i_0 \geq 0$ such that α_i is reduced for $i \geq i_0$. We give an explicit bound for this index i_0. But, this bound is not minimal and can not be used for algorithmic purposes. In fact, we are able to solve this problem. Hereby, we apply the same beautiful ideas that Kaplan and Williams [13] used to prove the corresponding sharp result in real quadratic number fields.

THEOREM 3.3. *Let α be a real quadratic irrationality. Then α_i is reduced for*

$$i > i_0 := \max\left\{ 0\,,\ \tfrac{1}{2}\deg(Q_0) - \tfrac{1}{4}\deg(\Delta) + 1 \right\}.$$

PROOF. Let $i \in \mathbb{N}$ be chosen such that $i > i_0$. First, note that $i \in \mathbb{N}$, and we know from (2.3) that $|\alpha_i| > 1$. Now, $i > i_0$ is equivalent to

$$\frac{|Q_0|}{|\sqrt{\Delta}|} < q^{2i-2}.$$

From (2.6) we know that $|q_{i-1}| \geq q^{i-1}$ and therefore

$$|\alpha_0 - \overline{\alpha}_0| = \left| \frac{P_0 + \sqrt{\Delta}}{Q_0} - \frac{P_0 - \sqrt{\Delta}}{Q_0} \right| = \frac{|\sqrt{\Delta}\,|}{|Q_0|} > \frac{1}{|q_{i-1}|^2}.$$

On the other side, we get from (2.10) and (2.11) for $i \in \mathbb{N}_0$:

$$(-1)^i(\alpha - \overline{\alpha}) = \frac{1}{q_{i-1}(q_{i-1}\overline{\alpha}_i + q_{i-2})} - \frac{1}{q_{i-1}(q_{i-1}\alpha_i + q_{i-2})}. \tag{3.10}$$

Assuming that α_i is not reduced, i.e. $|\overline{\alpha}_i| \geq 1$, we have that

$$|q_{i-1}\alpha_i + q_{i-2}| = |q_{i-1}\alpha_i| \quad \text{and} \quad |q_{i-1}\overline{\alpha}_i + q_{i-2}| = |q_{i-1}\overline{\alpha}_i|.$$

Hence,

$$\begin{aligned} |\alpha_0 - \overline{\alpha}_0| &\leq \max\left\{ \frac{1}{|q_{i-1}||q_{i-1}\overline{\alpha}_i + q_{i-2}|}\,,\ \frac{1}{|q_{i-1}||q_{i-1}\alpha_i + q_{i-2}|} \right\} \\ &= \frac{1}{|q_{i-1}|^2} \max\left\{ \frac{1}{|\overline{\alpha}_i|}\,,\ \frac{1}{|\alpha_i|} \right\} \\ &\leq \frac{1}{|q_{i-1}|^2}, \end{aligned}$$

because $|\alpha_i| > 1$, and, by assumption, $|\overline{\alpha}_i| \geq 1$. This leads to a contradiction, and the assertion is proved. □

THEOREM 3.4. *Let α be a real quadratic irrationality and let $i \in \mathbb{N}_0$. Then α_{i+1} is reduced if and only if $|Q_i| < |\sqrt{\Delta}\,|$.*

PROOF. If α_{i+1} is reduced, we have by definition that $|\overline{\alpha}_{i+1}| < 1 < |\alpha_{i+1}|$. From (3.2) and (3.3) it is easy to see that

$$\overline{\alpha}_{i+1} = \frac{P_{i+1} - \sqrt{\Delta}}{Q_{i+1}} \cdot \frac{P_{i+1} + \sqrt{\Delta}}{P_{i+1} + \sqrt{\Delta}} = -\frac{Q_i}{P_{i+1} + \sqrt{\Delta}}. \tag{3.11}$$

Together with Proposition 3.2, we have that

$$|Q_i| = |\overline{\alpha}_{i+1}||P_{i+1} + \sqrt{\Delta}\,| = |\overline{\alpha}_{i+1}||\sqrt{\Delta}\,| < |\sqrt{\Delta}\,|.$$

Conversely, let $i \in \mathbb{N}_0$ with $|Q_i| < |\sqrt{\Delta}|$. By (2.3) we have to show that $|\overline{\alpha}_{i+1}| < 1$ or, equivalently, that $|P_{i+1} - \sqrt{\Delta}\,| < |Q_{i-1}|$. From (3.7) we know that $P_{i+1} = d - r_i$, and by (3.6) we then obtain that

$$0 \leq |r_i| < |Q_i| < |\sqrt{\Delta}\,| = |d|.$$

Because the characteristic of k is different from 2, we deduce that

$$|P_{i+1} + \sqrt{\Delta}\,| = |\sqrt{\Delta}\,| = |P_{i+1}|.$$

Substituting this into (3.2), we get

$$\begin{aligned} |Q_{i+1}| &= \frac{|\Delta - P_{i+1}^2|}{|Q_i|} = \frac{|\sqrt{\Delta} + P_{i+1}|}{|Q_i|} \cdot |\sqrt{\Delta} - P_{i+1}| \\ &= \frac{|\sqrt{\Delta}|}{|Q_i|} \cdot |\sqrt{\Delta} - P_{i+1}| \\ &> |\sqrt{\Delta} - P_{i+1}|, \end{aligned}$$

by assumption. □

LEMMA 3.5. *Let α be a real quadratic irrationality. If there exists a minimal $i_0 \in \mathbb{N}$ such that $|Q_{i_0}| < |\sqrt{\Delta}|$, i.e. $|Q_j| \geq |\sqrt{\Delta}|$ for $j \in \{0, \ldots, i_0 - 1\}$, then α_{i_0} is not reduced.*

PROOF. (3.11) together with the assumption leads to

$$|\,\overline{\alpha}_{i_0}\,| = \frac{|\,Q_{i_0-1}\,|}{|\,P_{i_0} + \sqrt{\Delta}\,|} \geq \frac{|\,\sqrt{\Delta}\,|}{|\,P_{i_0} + \sqrt{\Delta}\,|}.$$

Suppose that α_{i_0} is reduced. We then deduce from Proposition 3.2 that

$$|\,\overline{\alpha}_{i_0}\,| \geq \frac{|\,\sqrt{\Delta}\,|}{|\,\sqrt{\Delta}\,|} = 1,$$

which gives a contradiction. □

We are now able to provide a simpler proof of Theorem 3.3 by using the above lemma, (2.12), and (3.9). Let $l \in \mathbb{N}$ be minimal such that α_{l+1} is reduced. It follows from Theorem 3.4 that $\deg(Q_l) \leq \deg(\Delta)/2 - 1$, and we then have that α_i is reduced for $i \geq l + 1$. However, we derive from the above lemma that α_l is not reduced. Thus, by Theorem 3.4, we have that $\deg(Q_{l-1}) \geq \deg(\Delta)/2$ and $\deg(\overline{\alpha}_l) \geq 0$. Since we also have that α_i is not reduced for $i = 1, \ldots, l-1$, we must have that $\deg(\alpha_i) \geq 1$ and that $\deg(\alpha_i) = \deg(\overline{\alpha}_i) = \deg(P_i) - \deg(Q_i) \geq 1$ $(1 \leq i \leq l-1)$. By (2.12), and

(3.9), we then easily see that

$$\begin{aligned}\deg(Q_0) &= \deg(Q_{l-1}) + \sum_{i=1}^{l-1} \deg(\alpha_i) + \sum_{i=1}^{l-1} \deg(\overline{\alpha}_i) \\ &\geq \tfrac{1}{2}\deg(\Delta) + 2(l-1),\end{aligned}$$

or, equivalently,

$$l \leq \tfrac{1}{2}\deg(Q_0) - \tfrac{1}{4}\deg(\Delta) + 1.$$

The bounds in Proposition 3.2 and Theorem 3.4 for the polynomials P_i and Q_i lead to the periodicity of the continued fraction expansion of a real quadratic irrationality in the case of a finite field k. Now, we summarize our results in the following theorem. We remark that the proof of "$(c) \Rightarrow (a)$" can be shown similar to [21, Lagrange's Theorem, p. 378].

THEOREM 3.6. *Let α be an element of $L - k(x)$, where k is a finite field of odd characteristic. Then the following statements are equivalent:*

(a) *The continued fraction expansion of α is periodic.*
(b) *The continued fraction expansion of α is quasi-periodic.*
(c) *α is a real quadratic irrationality.*

Next, we state that the reduction of a real quadratic irrationality by means of the continued fraction algorithm is equivalent to the computation of the pre-period. This is a well-known result and can be shown as in the case of a real number quadratic number field (see for example [20]).

THEOREM 3.7. *If the continued fraction expansion of the real quadratic irrationality $\alpha \in L$ is periodic, then it is purely periodic, i.e. the period begins at $\nu_0 = 0$, if and only if α is reduced.*

Finally, we develop properties for the polynomials P_i and Q_i in view of their periodic behavior. We apply Lemma 2.2 to (3.3) and obtain

PROPOSITION 3.8. *If the continued fraction expansion of a real quadratic irrationality α is quasi-periodic with quasi-period m and $\nu_0 \geq 0$, then we have for $i \geq \nu_0$ and $\lambda \geq 1$ that*

$$\begin{aligned}P_i &= P_{i+\lambda m}, \\ Q_i &= c_i^{1+(-1)^m+\ldots+(-1)^{(\lambda-1)m}} Q_{i+\lambda m},\end{aligned}$$

where $c_i := c^{(-1)^{i-\nu_0}}$ and $c \in k^*$ is defined as in (2.15).

4. SYMMETRIES

The case $\alpha = \sqrt{D}$ plays a particular role because the fundamental unit of a real quadratic function field $k(x)(\sqrt{D})$ can be calculated by applying the continued fraction algorithm to the element $\alpha = \sqrt{D}$. Also, there are

symmetries with respect to the period and to the quasi-period. Throughout, let k be a field of characteristic different from 2, and let $\alpha \in L - k(x)$ with

$$\alpha = \sqrt{\Delta},\ 0 < \deg(\Delta) \quad \text{even}, \tag{4.1}$$

where Δ is not a perfect square. Of course, α is a real quadratic irrationality in the sense of (3.1), where $P = 0$, $Q = 1$ and $1|(\Delta - 0^2)$. Also, note that the case $\alpha = \sqrt{D}$ is included in these considerations, since D is squarefree.

Furthermore, we assume that the continued fraction expansion of α is periodic. For example, this is true if k is a finite field. We easily see that α is not reduced. However, we know from Theorem 3.4 that α_i is reduced for $i \in \mathbb{N}$. Theorem 3.7 implies that the period starts at $\nu_0 = 1$. If $c \in k^*$ is such that

$$\alpha_{1+m} = c\,\alpha_1 \qquad \text{and} \qquad \alpha_{1+n} = \alpha_1, \tag{4.2}$$

then $\alpha_{i+n} = \alpha_i$ for $i \in \mathbb{N}$. Results concerning periodicity can be deduced in the same way as for real numbers. We list them without proof.

THEOREM 4.1. *If the continued fraction expansion of $\alpha = \sqrt{\Delta}$ is periodic with period n, then we have the following symmetries:*

$$\begin{aligned} a_n &= 2a_0, \\ a_i &= a_{n-i} && (\, i = 1, \ldots, n-1\,), \\ \alpha_{i+1} &= -\frac{1}{\overline{\alpha}_{n-i}} && (\, i = 0, \ldots, n-1\,), \\ P_{i+1} &= P_{n-i} && (\, i = 1, \ldots, n-1\,), \\ Q_i &= Q_{n-i} && (\, i = 1, \ldots, n\,). \end{aligned}$$

In particular, we have $Q_{\lambda n} = Q_n = Q_0 = 1$ for $\lambda \geq 1$.

The additional fact of the theorem provides us with a criterion to recognize the period. Now, we give an analogous criterion to recognize the quasi-period.

THEOREM 4.2. *If the continued fraction expansion of $\alpha = \sqrt{\Delta}$ is periodic with period n and quasi-period m, then $Q_s \in k^*$ if and only if $s = \lambda m$ for some $\lambda \in \mathbb{N}_0$.*

PROOF. Let $s = \lambda m$. If $\lambda = 0$ or $n = m$, then there is nothing to show. Now, let $n = lm$ where $l \geq 2$. Defining $c_m = c^{(-1)^{m-1}}$, we see from Proposition 3.8 that

$$Q_m = c_m^{1+(-1)^m+\ldots+(-1)^{(\lambda-2)m}}\, Q_{\lambda m} \quad (\lambda \geq 2). \tag{4.3}$$

Therefore, we only have to prove that $Q_m \in k^*$. But, the assertion follows from the same result with $\lambda = l$ and $Q_{lm} = Q_n = 1$. Conversely, let $Q_s \in k^*$. If $s = 0$, then the assertion is true. Therefore, let $s \geq 1$. We have to show that $m = s$. From the first assertion we have that $m \geq s$, because

$Q_m \in k^*$. It suffices to show that $\alpha_{s+1} = c\alpha_1$, since then $m \leq s$. First, we know that $P_0 = 0$, $Q_0 = 1$, $a_0 = d = \lfloor\sqrt{\Delta}\rfloor$, $P_1 = d$, and $Q_1 = \Delta - d^2$. Furthermore, $\alpha_s = (P_s + \sqrt{\Delta})/Q_s = (P_s + \sqrt{\Delta})/c$ is reduced. This means that $|\overline{\alpha}_s| = |P_s - \sqrt{\Delta}| < 1$. Consequently $P_s = \lfloor\sqrt{\Delta}\rfloor = d$ and $a_s = 2d/c$. Also, $P_{s+1} = d = P_1$ and $Q_{s+1} = Q_1/c$. We get $\alpha_{s+1} = c\alpha_1$ and the assertion is proved. □

COROLLARY 4.3. *In the situation of Theorem 4.2 we have that*

$$N(\overline{\theta}_{\lambda m+1}) = p_{\lambda m-1}^2 - \Delta\, q_{\lambda m-1}^2 \in k^* \qquad (\lambda \in \mathbb{N}).$$

PROOF. See (3.9), (2.13), and Theorem 4.2. □

LEMMA 4.4. *Let the continued fraction expansion of $\alpha = \sqrt{\Delta}$ be periodic with period n and quasi-period m. Then, for every $\lambda \in \mathbb{N}$ there exists a constant $c(\lambda) \in k^*$ such that*

$$\overline{\theta}_{\lambda m+1} = c(\lambda)\,(\overline{\theta}_{m+1})^{\lambda}.$$

PROOF. From Lemma 2.2 we get for $i \in \mathbb{N}$ that

$$\alpha_{i+\lambda m} = c_i^{1+(-1)^m+\ldots+(-1)^{(\lambda-1)m}}\ \alpha_i,$$

where $c_i := c^{(-1)^{i-1}}$. By (2.12) we derive that

$$\prod_{j=\lambda m+1}^{\lambda m+m} \frac{1}{\overline{\alpha}_j} = \prod_{j=1}^{m} \frac{1}{\overline{\alpha}_{\lambda m+j}} = \hat{c}\cdot\overline{\theta}_{m+1},$$

where

$$\hat{c} = \prod_{j=1}^{m} c_j^{-1-(-1)^m-\ldots-(-1)^{(\lambda-1)m}}.$$

Then, the assertion easily follows by induction. □

Now, we use symmetries with respect to the period to derive relations between the period and the quasi-period.

THEOREM 4.5. *Let the continued fraction expansion of $\alpha = \sqrt{\Delta}$ be periodic with period n.*

(a) *If there exists an index ν, $1 \leq \nu \leq n-1$, such that $P_\nu = P_{\nu+1}$, then $n = 2\nu$. Conversely, if $n = 2\nu$ for some $\nu \in \mathbb{N}$, then $P_\nu = P_{\nu+1}$.*

(b) *If there exists an index μ, $0 \leq \mu \leq n-1$, such that $Q_\mu = Q_{\mu+1}$, then $n = 2\mu+1$. Conversely, if $n = 2\mu+1$ for some $\mu \in \mathbb{N}_0$, then $Q_\mu = Q_{\mu+1}$.*

PROOF. Easy. See [20, p. 24]. □

COROLLARY 4.6. *Let the continued fraction expansion of $\alpha = \sqrt{\Delta}$ be periodic with period n and quasi-period m. Then there are three cases that can occur:*

(a) *$n = m$ odd;*
(b) *$n = m$ even;*
(c) *$n = 2m$ even, m odd.*

PROOF. If the period n is odd, then we know from Corollary 2.3 that $n = m$, and thus both m and n are odd. Now, let n be even and $n \neq m$. First, we know from Proposition 2.1 that $n = lm$ with $l \geq 2$. We get

$$\begin{aligned} P_{m+1} &= P_{(l-1)m+1} && \text{from Proposition 3.8,} \\ &= P_{n-(l-1)m} && \text{from Theorem 4.1,} \\ &= P_m, \end{aligned}$$

because $n = lm$. From Theorem 4.5 we deduce that $n = 2m$. Assuming that $m = 2s$ even, we conclude as above that

$$P_{s+1} = P_{m+s+1} = P_{n-(m+s)} = P_s,$$

since $n - (m + s) = 2m - (m + s) = m - s = 2s - s = s$. Again, we deduce that $n = 2s = m$, which contradicts the fact that $n \neq m$. Therefore, m is odd. □

Note that all three cases do occur and that there is exactly one nontrivial case, i.e. one case where the period is different from the quasi-period. Next, we develop symmetries with respect to the quasi-period.

THEOREM 4.7. *If the continued fraction expansion of $\alpha = \sqrt{\Delta}$ is periodic with period n and quasi-period m, then we have the following symmetries with respect to the quasi-period:*

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

where $c \in k^*$ is given as in (4.2).

PROOF. If $n = m$, then there is nothing to prove, because the symmetries can be deduced from Theorem 4.1 with $c = 1$. Therefore, let $n = 2m$, m odd. From Proposition 3.8 we have that

$$P_{i+1} = P_{i+m+1} \qquad \text{and} \qquad Q_i = c^{(-1)^{i-1}} \cdot Q_{i+m}.$$

Furthermore, we know from Theorem 4.1 that

$$P_{i+m+1} = P_{n-(i+m)} \qquad \text{and} \qquad Q_{i+m} = Q_{n-(i+m)},$$

and the symmetries hold true, since $n = 2m$. The index transformation $i \to i+1$ for Q_i and (3.3) leads to

$$c^{(-1)^i} \cdot \alpha_{i+1} = c^{(-1)^i} \cdot \left(\frac{P_{i+1} + \sqrt{\Delta}}{Q_{i+1}} \right) = \frac{P_{m-i} + \sqrt{\Delta}}{Q_{m-i-1}} = -\frac{1}{\overline{\alpha}_{m-i}}.$$

□

THEOREM 4.8. *Let the continued fraction expansion of $\alpha = \sqrt{\Delta}$ be periodic with period n and quasi-period m.*

(a) *If there exists an index ν, $1 \leq \nu \leq m-1$, such that $P_\nu = P_{\nu+1}$, then $m = 2\nu = n$. Conversely, if $m = 2\nu$ for some $\nu \in \mathbb{N}$, then $P_\nu = P_{\nu+1}$ and $n = m$.*

(b) *If there exists an index μ, $0 \leq \mu \leq m-1$, such that $Q_{\mu+1} = c' \cdot Q_\mu$, where $c' \in k^*$, then $m = 2\nu + 1$. If in addition $c' = 1$, then $n = m$. If $c' \neq 1$, then $n = 2m$. Conversely, if $m = 2\mu + 1$ for some $\mu \in \mathbb{N}_0$, then there exists a $c' \in k^*$ such that $Q_{\mu+1} = c' \cdot Q_\mu$.*

PROOF. If $P_\nu = P_{\nu+1}$, then we know from Theorem 4.5 that $n = 2\nu$. Since $\nu \leq m-1$, Corollary 4.6 tells us that $m = 2\nu = n$. Conversely, if $m = 2\nu$, then we conclude from Corollary 4.6 that $n = m$, and the assertion follows from Theorem 4.5. To prove the second statement we use (3.3) and Theorem 4.7 to derive that

$$\alpha_{m-\mu} = \frac{P_{m-\mu} + \sqrt{\Delta}}{Q_{m-\mu}} = c^{(-1)^{\mu-1}} \cdot \left(\frac{P_{\mu+1} + \sqrt{\Delta}}{Q_\mu} \right) = c' \cdot c^{(-1)^{\mu-1}} \cdot \alpha_{\mu+1}.$$

Because m is minimal with this property we deduce that $m - \mu = \mu + 1$, or, equivalently, that $m = 2\mu + 1$ odd. The final part is trivial. □

We wish to finish the continued fraction algorithm at about $m/2$ steps in the continued fraction expansion. In this context, we have to consider different constants. We use the constant $c \in k^*$ of (4.2) only for theoretical purposes. The further constant $c' \in k^*$ can be determined after half of the quasi-period has been computed:

$$c' = \frac{\operatorname{sgn}(Q_{\mu+1})}{\operatorname{sgn}(Q_\mu)}.$$

We need the further constant

$$c(\mu) = \prod_{j=0}^{\mu} c^{(-1)^j} \in k^*. \tag{4.4}$$

The following remark shows how $c(\mu)$ can be computed and how it is related to c, c'. The proof of this remark is easy.

REMARK 4.9. In above notation we get:

(a) $c' = c^{(-1)^\mu}$,

(b) $c(\mu) = \begin{cases} c', & \mu \text{ even} \\ 1, & \mu \text{ odd} \end{cases}$.

Finally, we are able to formulate the duplication formulas. They are based on symmetries with respect to the quasi-period.

THEOREM 4.10. *Let the continued fraction expansion of $\alpha = \sqrt{\Delta}$ be periodic with period n and quasi-period m.*

(a) *If there exists an index ν, $1 \leq \nu \leq m-1$, such that $P_\nu = P_{\nu+1}$, then we have that*

$$\overline{\theta}_{m+1} = (-1)^\nu \cdot \frac{\overline{\theta}_{\nu+1}}{\theta_{\nu+1}} = \frac{\overline{\theta}_{\nu+1}^2}{Q_\nu} = \frac{Q_\nu}{\theta_{\nu+1}^2}.$$

(b) *If there exists an index μ, $0 \leq \mu \leq m-1$, such that $Q_{\mu+1} = c' \cdot Q_\mu$, where $c' \in k^*$, then we have that*

$$\overline{\theta}_{m+1} = c(\mu) \cdot \frac{\overline{\theta}_{\mu+1}\overline{\theta}_{\mu+2}}{Q_{\mu+1}} = -c(\mu) \cdot \overline{\theta}_{\mu+1}^2 \frac{\overline{\alpha}_{\mu+1}}{Q_\mu} = -c(\mu) \cdot \frac{\alpha_{\mu+1} Q_\mu}{\theta_{\mu+1}^2},$$

where $c(\mu)$ is defined as above.

PROOF. In the first case, we know from Theorem 4.8 that $n = m = 2\nu$. By using Theorem 4.7, we get

$$\prod_{j=\nu+1}^{m} \frac{1}{\overline{\alpha}_j} = \prod_{j=0}^{\nu-1} \frac{1}{\overline{\alpha}_{m-j}} = \prod_{j=0}^{\nu-1} (-\alpha_{j+1}) = \frac{(-1)^\nu}{\theta_{j+1}}.$$

Thus,

$$\overline{\theta}_{m+1} = \prod_{j=1}^{m} \frac{1}{\overline{\alpha}_j} = \prod_{j=1}^{\nu} \frac{1}{\overline{\alpha}_j} \cdot \prod_{j=\nu+1}^{m} \frac{1}{\overline{\alpha}_j} = \overline{\theta}_{\nu+1} \cdot \frac{(-1)^\nu}{\theta_{\nu+1}}.$$

This proves the first equality. The other equalities follow from (3.9). In the second case, we see that $n = 2\mu + 1$. Let $c \in k^*$ as in (4.2) and $c(\mu)$ as in (4.4). Again, by using Theorem 4.7 and (2.12) we get

$$\prod_{j=\mu+1}^{m} \frac{1}{\overline{\alpha}_j} = \prod_{j=0}^{\mu} \frac{1}{\overline{\alpha}_{m-j}} = \frac{(-1)^{\mu+1} \cdot c(\mu)}{\theta_{\mu+2}}.$$

Thus,

$$\overline{\theta}_{m+1} = \prod_{j=1}^{m} \frac{1}{\overline{\alpha}_j} = \prod_{j=1}^{\mu} \frac{1}{\overline{\alpha}_j} \cdot \prod_{j=\mu+1}^{m} \frac{1}{\overline{\alpha}_j} = \overline{\theta}_{\mu+1} \cdot \frac{(-1)^{\mu+1} \cdot c(\mu)}{\theta_{\mu+2}}.$$

The statements can now be derived from (3.9) and the fact that

$$\frac{1}{\overline{\alpha}_{\mu+1}} = -\alpha_{\mu+1} \cdot \frac{Q_{\mu+1}}{Q_\mu}. \tag{4.5}$$

□

Since we are also interested in the degree of $\overline{\theta}_{m+1}$, or more generally in the degree of θ_{i+1}, we introduce the positive numbers

$$A_{i+1} = \sum_{j=1}^{i} \deg(a_j) \qquad (i \in \mathbb{N}). \tag{4.6}$$

By (2.12) and (3.9), we see that

$$A_{i+1} = -\deg(\theta_{i+1}) = \deg(\overline{\theta}_{i+1}) + \deg(Q_i). \tag{4.7}$$

COROLLARY 4.11. *Let the continued fraction expansion of $\alpha = \sqrt{\Delta}$ be periodic with period n and quasi-period m.*

(a) *If there exists an index ν, $1 \le \nu \le m-1$, such that $P_\nu = P_{\nu+1}$, then we have that*

$$\deg(\overline{\theta}_{m+1}) = 2\deg(\overline{\theta}_{\nu+1}) - \deg(Q_\nu) = 2A_{\nu+1} + \deg(Q_\nu).$$

(b) *If there exists an index μ, $0 \le \mu \le m-1$, such that $Q_{\mu+1} = c' \cdot Q_\mu$, where $c' \in k^*$, then we have that*

$$\deg(\overline{\theta}_{m+1}) = 2\deg(\overline{\theta}_{\mu+1}) - \deg(Q_\mu) + \deg(a_{\mu+1}) = 2A_{\mu+1} + \deg(\sqrt{\Delta}).$$

PROOF. We can immediately derive the statements from Theorem 4.10. Note that for the second equality in the second statement we apply Proposition 3.2 to derive that

$$\deg(\sqrt{\Delta}) = \deg(a_{\mu+1}) + \deg(Q_{\mu+1}) = \deg(a_{\mu+1}) + \deg(Q_\mu),$$

since we must have that $Q_{\mu+1} = c' \cdot Q_\mu$ in this case. □

COROLLARY 4.12. *Let the continued fraction expansion of $\alpha = \sqrt{\Delta}$ be periodic with period n and quasi-period m and let $c(\mu)$ be defined as in (4.4).*

(a) *If there exists an index ν, $1 \le \nu \le m-1$, such that $P_\nu = P_{\nu+1}$, then we have that*

$$p_{m-1} = p_{\nu-1}q_{\nu-2} + p_\nu q_{\nu-1},$$
$$q_{m-1} = q_{\nu-1}(q_\nu + q_{\nu-2}).$$

(b) *If there exists an index μ, $0 \le \mu \le m-1$, such that $Q_{\mu+1} = c' \cdot Q_\mu$, where $c' \in k^*$, then we have that*

$$p_{m-1} = \frac{c(\mu)}{c'} \cdot (p_\mu q_\mu + c' p_{\mu-1} q_{\mu-1}),$$
$$q_{m-1} = \frac{c(\mu)}{c'} \cdot (q_\mu^2 + c' q_{\mu-1}^2).$$

PROOF. In the first case, we have $m = n = 2\nu$, and we can apply Theorem 4.10 with

$$Q_\nu \cdot \overline{\theta}_{m+1} = \overline{\theta}_{\nu+1}^2.$$

By equating rational and irrational parts, we deduce from (2.13) that

$$\left\{ \begin{array}{l} Q_\nu p_{m-1} = p_{\nu-1}^2 + q_{\nu-1}^2 \Delta; \\ Q_\nu q_{m-1} = 2 p_{\nu-1} q_{\nu-1}. \end{array} \right\}$$

Hence, by (3.9) and (3.8), we have that

$$Q_\nu p_{m-1} = (-1)^\nu Q_\nu + q_{\nu-1}(p_{\nu-1} 2P_\nu + 2p_{\nu-2} Q_\nu).$$

From (3.2) and the fact that $P_\nu = P_{\nu+1}$ we derive that $a_\nu Q_\nu = 2P_\nu$. Therefore, we can delete Q_ν on both sides. Then the assertion for p_{m-1} follows from (2.10) and (2.5). Again, by (3.8) and the above equation, we see that

$$Q_\nu q_{m-1} = q_{\nu-1}(q_{\nu-1} 2P_\nu + 2q_{\nu-2} Q_\nu).$$

Because $a_\nu Q_\nu = 2P_\nu$, we delete Q_ν on both sides. Then the assertion follows from (2.5). In the second case, we have that $m = 2\mu + 1$, and we can apply Theorem 4.10 with

$$Q_{\mu+1} \cdot \overline{\theta}_{m+1} = c(\mu) \cdot \overline{\theta}_{\mu+1} \cdot \overline{\theta}_{\mu+2}.$$

By using the same reasoning as above, we get

$$\left\{ \begin{array}{l} Q_{\mu+1} \cdot p_{m-1} = c(\mu)(p_{\mu-1} p_\mu + q_{\mu-1} q_\mu \Delta) \\ Q_{\mu+1} \cdot q_{m-1} = c(\mu)(p_{\mu-1} q_\mu + q_{\mu-1} p_\mu) \end{array} \right\}.$$

Hence, by (3.8) and (3.2), we have that

$$Q_{\mu+1} \cdot p_{m-1} = c(\mu)(p_{\mu-1} q_\mu a_\mu Q_\mu + p_{\mu-1} q_{\mu-1} Q_{\mu+1} + p_{\mu-2} Q_\mu q_\mu).$$

Since $Q_{\mu+1} = c' \cdot Q_\mu$, we can delete Q_μ on both sides. Together with (2.5) we see that

$$c' p_{m-1} = c(\mu)(q_\mu p_\mu + c' q_{\mu-1} p_{\mu-1}).$$

By using (3.8) twice, we get

$$Q_{\mu+1} \cdot q_{m-1} = c(\mu)(q_\mu^2 Q_\mu + q_{\mu-1}^2 Q_{\mu+1}).$$

Replacing $Q_{\mu+1}$ by $c' \cdot Q_\mu$ and deleting Q_μ on both sides leads to

$$c' q_{m-1} = c(\mu)(q_\mu^2 + c' q_{\mu-1}^2).$$

□

5. Fundamental Unit and Regulator

Let $K = \mathbb{F}_q(x)(\sqrt{D})$ be a real quadratic function field over the finite field $\mathbb{F}_q$ of odd characteristic, where $D \in \mathbb{F}_q[x]$ is a monic, squarefree polynomial of even degree. From Theorem 3.6 we know that the continued fraction expansion of $\alpha = \sqrt{D}$ is periodic and quasi-periodic. First, we need a simple remark.

Remark 5.1. Let $\eta = U + V \cdot \sqrt{D} \in \mathcal{O}_K$, where U, $V \in \mathbb{F}_q[x]$. Then η is a unit in $\mathcal{O}_K$ if and only if $N(\eta)$ is a trivial unit, i.e. $N(\eta) \in k^*$.

Proof. see [2, p. 195]. □

Theorem 5.2. *Let $D \in \mathbb{F}_q[x]$ be a monic, squarefree polynomial of even degree. Then the continued fraction expansion of $\alpha = \sqrt{D}$ is periodic and quasi-periodic. If m denotes the quasi-period, then*

$$\epsilon = p_{m-1} + q_{m-1} \cdot \sqrt{D}$$

is a fundamental unit of $K = \mathbb{F}_q(x)(\sqrt{D})$ and

$$E = k^* \times \langle\, \overline{\theta}_{m+1} \,\rangle = k^* \times \langle\, p_{m-1} + q_{m-1} \cdot \sqrt{D} \,\rangle.$$

Proof. The second equality follows from (2.13). We have to show that $E = k^* \times \langle\, \overline{\theta}_{m+1} \,\rangle$. " $\subseteq$ " is an easy consequence of Corollary 4.3 and the above remark. To show " $\supseteq$ " we choose an arbitrary unit $\eta = U + V \cdot \sqrt{D} \in E$, where U, $V \in \mathbb{F}_q[x]$. If $|\eta| = 1$, then the assertion is trivial. Let $|\eta| > 1$. In a first step, we prove that there exists a $c_0 \in k^*$ and an index $j \geq 0$ such that

$$U = c_0 \cdot p_{j-1}, \qquad V = c_0 \cdot q_{j-1}.$$

From the above remark we know that $N(\eta) \in k^*$. On the other side,

$$N(\eta) = U^2 - V^2 \cdot D = c_0^2 \left(p_{j-1}^2 - q_{j-1}^2 \cdot D \right) = c_0^2 \cdot (-1)^j \cdot Q_j,$$

by (3.9). Thus, $Q_j \in k^*$. Theorem 4.2 and Lemma 4.4 then imply that

$$\eta = \hat{c} \cdot \overline{\theta}_{m+1}^{\,t},$$

with $\hat{c} \in k^*$ and $t \in \mathbb{N}$. If $|\eta| < 1$, then $|\overline{\eta}| = |\frac{1}{\eta}| > 1$, and we use $1/\eta$ instead of η. □

Corollary 5.3. *In the situation of Theorem 5.2, we have that*

$$R = \deg(\overline{\theta}_{m+1}) = A_{m+1},$$

where R is the regulator of K/k with respect to $\mathcal{O}_K$, and A_i is defined in (4.6).

Proof. The first equality follows from Theorem 5.2, since the regulator is defined to be the degree of the fundamental unit. The second equality is a consequence of (4.7) and Theorem 4.2. We have $Q_m \in k^*$, and therefore $\deg(Q_m) = 0$, $\deg(a_m) = \deg(\Delta)/2$. □

From the above theorem and corollary one can derive algorithms to compute the fundamental unit and the regulator of K. For the fundamental unit, we calculate recursively the quantities a_i, r_i, p_i, q_i, P_i, Q_i, where we use (2.5) and the optimized formulas in (3.7). We terminate the algorithm as soon as one of the conditions of Corollary 4.12 is satisfied. To calculate the regulator, we don't need the quantities p_i, q_i. Instead, we calculate the additional quantities A_i. Note that the A_i's are nonnegative integers. It is a great advantage to avoid the computation of the polynomials p_i and q_i, because they both increase in degree, as can be deduced from (2.6). Whereas, we see from Proposition 3.2 that a_i, r_i, P_i, Q_i are bounded in its degree because α_i is reduced ($i \in \mathbb{N}$).

6. Ideals

In the previous section we have presented in detail a baby step algorithm for computing the regulator R of K with respect to $\mathcal{O}_K$. This has been done via the computation of the continued fraction algorithm of a real quadratic irrationality. There exists a well-known connection between the continued fraction expansion of $\alpha = \sqrt{D}$ as defined in the previous section and reduced $\mathcal{O}_K$-ideals. As in real quadratic number fields, we will show in the remainder of this article that using ideal arithmetic allows one to improve on the methods presented above by making use of the infrastructure. In Section 11, we will present baby step-giant step algorithms that combine the continued fraction algorithm (baby steps) with the infrastructure ideas (giant steps). Further and more advanced optimizations of these ideas by making use of the zeta function have been presented in [32, 33, 31].

In this section, we summarize some important facts about $\mathcal{O}_K$-ideals in a quadratic function field $K = k(x)(\sqrt{D})$, where $\mathcal{O}_K = k[x][\sqrt{D}]$ and k is an arbitrary field of odd characteristic. Here, D is a squarefree polynomial in $k[x]$. The properties of the ideals and the corresponding proofs can be found in [2]. We call a non-zero subset $\mathfrak{a}$ of K an *$\mathcal{O}_K$-ideal*, or simply an *ideal*, if $\mathfrak{a}$ possesses the properties:

(a) if $\lambda_1, \lambda_2 \in \mathcal{O}_K$ and $\alpha_1, \alpha_2 \in \mathfrak{a}$, then $\lambda_1\alpha_1 + \lambda_2\alpha_2 \in \mathfrak{a}$;
(b) there exists a $\lambda(\neq 0) \in \mathcal{O}_K$ such that $\lambda\mathfrak{a} \subseteq \mathcal{O}_K$.

If the second condition holds with $\lambda = 1$, we say that $\mathfrak{a}$ is an *integral $\mathcal{O}_K$-ideal*. For elements $\alpha_1, \alpha_2, \ldots, \alpha_r \in K$ the set

$$(\alpha_1, \alpha_2, \ldots, \alpha_r) := \left\{ \sum_{i=1}^{r} \lambda_i\alpha_i;\ \lambda_i \in \mathcal{O}_K, i = 1, \ldots, r \right\}$$

is clearly an ideal, and it is called the ideal *generated* by $\alpha_1, \alpha_2, \ldots, \alpha_r$. If $\mathfrak{a}$ is generated by a single element $\alpha \in K$, i.e. $\mathfrak{a} = (\alpha) = \alpha\mathcal{O}_K$, we call $\mathfrak{a}$ a

principal $\mathcal{O}_K$-ideal. For $\omega_1, \omega_2, \ldots, \omega_r \in \mathcal{O}_K$ we let

$$[\omega_1, \omega_2, \ldots, \omega_r] := \left\{ \sum_{i=1}^{r} A_i \omega_i;\ A_i \in k[x], i = 1, \ldots, r \right\} \quad \subseteq \quad \mathcal{O}_K.$$

If this set is an integral ideal, and $\omega_1, \omega_2, \ldots, \omega_r$ are linearly independent over $k[x]$, then $\{\omega_1, \omega_2, \ldots, \omega_r\}$ is called a $k[x]$-*basis* of $\mathfrak{a}$.

In [2] it is shown that every $k[x]$-base of an integral ideal $\mathfrak{a}$ consists of two elements.

THEOREM 6.1. *A 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 $Q|(D - P^2)$ such that*

$$\mathfrak{a} = \left[SQ, SP + S\sqrt{D} \right]. \tag{6.1}$$

We say that an integral $\mathcal{O}_K$-ideal $\mathfrak{a}$ is *primitive*, if in (6.1), S can be chosen to be 1, i.e. if

$$\mathfrak{a} = \left[Q, P + \sqrt{D} \right]$$

with $Q|(D - P^2)$. A $k[x]$-base of an integral ideal $\mathfrak{a}$ can be chosen to be in *adapted* form, meaning that

$$\mathfrak{a} = \left[T, R + S\sqrt{D} \right] \qquad (T, R, S \in k[x]), \tag{6.2}$$

where $\deg(R) < \deg(T)$. The polynomials T, R, S are unique up to constant factors. More precisely, if $\operatorname{sgn}(T) = \operatorname{sgn}(S) = 1$, then the adapted representation is unique.

Let $\mathfrak{a}$ be an integral $\mathcal{O}_K$-ideal given with an arbitrary $k[x]$-base $\{\omega_1, \omega_2\}$. It is easy to see that $\mathfrak{a} = [\omega_1, \omega_2] = (\omega_1, \omega_2)$. We define the *norm* of $\mathfrak{a}$, $N(\mathfrak{a}) \in k[x]$, by

$$\left| \begin{array}{cc} \omega_1 & \omega_2 \\ \overline{\omega}_1 & \overline{\omega}_2 \end{array} \right|^2 = c^2 \cdot \left(N(\mathfrak{a})^2 \right) \cdot D,$$

where $c \in k^*$ and $\operatorname{sgn}(N(\mathfrak{a})) = 1$. The norm of an $\mathcal{O}_K$-ideal does not depend on the given $k[x]$-base. If an integral $\mathcal{O}_K$-ideal $\mathfrak{a}$ is given with a $k[x]$-base as in (6.1), we see that

$$N(\mathfrak{a}) = \frac{Q \cdot S^2}{\operatorname{sgn}\left(Q \cdot S^2 \right)} \in k[x]. \tag{6.3}$$

Note that $\operatorname{sgn}(N(\mathfrak{a})) = 1$.

Next, we generally define the *product* of two $\mathcal{O}_K$-ideals $\mathfrak{a}$ and $\mathfrak{b}$ by

$$\mathfrak{a} \cdot \mathfrak{b} := \left\{ \sum_{i=1}^{n} a_i b_i;\ n \in \mathbb{N}, a_i \in \mathfrak{a}, b_i \in \mathfrak{b}, i = 1, \ldots, n \right\}.$$

Again, this set represents an $\mathcal{O}_K$-ideal. For $\beta, \alpha_1, \alpha_2, \ldots, \alpha_r \in K$, we calculate $(\beta) \cdot (\alpha_1, \alpha_2, \ldots, \alpha_r) = (\beta\alpha_1, \beta\alpha_2, \ldots, \beta\alpha_r)$, and $(\alpha_1, \alpha_2) \cdot (\beta_1, \beta_2) = (\alpha_1\beta_1, \alpha_1\beta_2, \alpha_2\beta_1, \alpha_2\beta_2)$. For any $\mathcal{O}_K$-ideal $\mathfrak{a}$, the $\mathcal{O}_K$-ideal

$$\overline{\mathfrak{a}} := \{\overline{\alpha};\ \alpha \in \mathfrak{a}\}$$

is called the *conjugate $\mathcal{O}_K$-ideal* of $\mathfrak{a}$. If $\mathfrak{a} = \{\alpha_1, \alpha_2, \ldots, \alpha_r\}$, then $\overline{\mathfrak{a}} = \{\overline{\alpha}_1, \overline{\alpha}_2, \ldots, \overline{\alpha}_r\}$. The following lemma describes some properties of the norm and the conjugate of an integral $\mathcal{O}_K$-ideal.

LEMMA 6.2. *Let $\mathfrak{a}$ and $\mathfrak{b}$ be integral $\mathcal{O}_K$-ideals.*

(a) *We have that $\mathfrak{a}\overline{\mathfrak{a}} = (N(\mathfrak{a}))$.*
(b) *We have that $N(\mathfrak{a}\mathfrak{b}) = N(\mathfrak{a})N(\mathfrak{b})$.*
(c) *If $\mathfrak{a}$ is principal, i.e. $\mathfrak{a} = (\alpha)$, where $\alpha \in \mathcal{O}_K$, then there exists a $c \in k^*$ such that $N(\mathfrak{a}) = cN(\alpha)$.*

Finally, 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 non-zero elements $\alpha, \beta \in \mathcal{O}_K$ such that $(\alpha)\mathfrak{a} = (\beta)\mathfrak{b}$.

7. Ideal Product

For an efficient arithmetic in quadratic function fields, we have to define an operation that corresponds to the group operation in a finite abelian group. The first step is to compute the product of two $\mathcal{O}_K$-ideals $\mathfrak{a}_1$ and $\mathfrak{a}_2$ given with their unique adapted $k[x]$-bases. By Theorem 6.1 and (6.2), there exist $S_i, Q_i, P_i \in k[x]$ $(i = 1, 2)$ such that $Q_i | (D - P_i^2)$, and

$$\mathfrak{a}_i = (S_i)\left[Q_i, P_i + \sqrt{D}\right] = (S_i)\mathfrak{a}_i' \quad (i = 1, 2),$$

where $\mathfrak{a}_i' = \left[Q_i, P_i + \sqrt{D}\right]$ is a primitive $\mathcal{O}_K$-ideal. Then $\mathfrak{a}_1 \cdot \mathfrak{a}_2 = (S_1S_2)\mathfrak{a}_1' \cdot \mathfrak{a}_2'$ and we have to compute the product of the primitive $\mathcal{O}_K$-ideals $\mathfrak{a}_1'$ and $\mathfrak{a}_2'$. Without loss of generality, we therefore assume that $\mathfrak{a}_1$ and $\mathfrak{a}_2$ are primitive, i.e. $S_i = 1$, and that they are given with their unique adapted bases. This means that

$$\mathfrak{a}_i = \left[Q_i, P_i + \sqrt{D}\right],$$

where $Q_i, P_i \in k[x]$, $Q_i | (D - P_i^2)$, and

$$\deg(P_i) < \deg(Q_i) \quad \text{and} \quad \operatorname{sgn}(Q_i) = 1.$$

To compute the product of $\mathfrak{a}_1$ and $\mathfrak{a}_2$, we use the same ideas as Shanks, [26], as employed, for example, in [16] or [37]. Our aim is to find a primitive $\mathcal{O}_K$-ideal $\mathfrak{c} = [Q, P + \sqrt{D}]$ and a polynomial $S \in k[x]$ such that $\mathfrak{a}_1\mathfrak{a}_2 = (S)\mathfrak{c}$, where

$Q|(D-P^2)$, $\deg(P) < \deg(Q)$ and $\operatorname{sgn}(Q) = 1 = \operatorname{sgn}(S)$. We obtain

$$S = \gcd(Q_1, Q_2, P_1 + P_2), \tag{7.1}$$

$$Q = \frac{Q_1 Q_2}{S^2}, \tag{7.2}$$

$$P \equiv \left(P_1 + \frac{Q_1}{S}\left[U(P2 - P_1) + W\left(\frac{D - P_1^2}{Q_1}\right)\right]\right) \pmod{Q}, \tag{7.3}$$

where $U, V, W \in k[x]$ are polynomials such that $S = UQ_1 + VQ_2 + W(P_1 + P_2)$. Therefore, we proceed as follows: using the extended Euclidean algorithm, we compute polynomials S_1, X_1 such that $S_1 = \gcd(Q_1, Q_2) \equiv X_1 Q_1 \pmod{Q_2}$. By using the extended Euclidean algorithm again, we compute polynomials S, X_2, Y_2 such that $S = \gcd(G_1, P_1 + P_2) = X_2 S_1 + Y_2(P_1 + P_2)$. Thus, $U = X_2 X_1$ and $W = Y_2$. Finally, we can apply the formulas for P and Q. In many cases, we have $S_1 = 1$, and we continue with $S = 1$, $X_2 = 1$, $Y_2 = 0$.

8. Reduced Ideals in the Real Case

Here and throughout the remainder of this paper, we consider K to be a real quadratic function field over the finite field $k = \mathbb{F}_q$ of odd characteristic, i.e. $K = k(x)(\sqrt{D})$, where D is a monic, squarefree polynomial in $k[x]$ of even degree. First, we state a helpful Lemma which describes equivalent ideals in the real case.

Lemma 8.1. *If $\mathfrak{a}$ and $\mathfrak{b}$ are two equivalent integral $\mathcal{O}_K$-ideals, then there exists a $\gamma \in \mathfrak{a}$ such that*

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

where $0 < |\gamma| \leq |N(\mathfrak{a})|$.

Proof. Since $\mathfrak{a}$ and $\mathfrak{b}$ are equivalent and integral, there exist nonzero $\alpha, \beta \in \mathcal{O}_K$ such that

$$(\alpha)\mathfrak{a} = (\beta)\mathfrak{b}.$$

From Lemma 6.2 it follows that

$$c_1 \alpha \overline{\alpha} N(\mathfrak{a}) = c_2 \beta \overline{\beta} N(\mathfrak{b})$$

for some $c_1, c_2 \in k^*$. We put

$$\gamma' = c_1 \cdot \frac{\overline{\alpha}}{\overline{\beta}} \cdot N(\mathfrak{a}) = c_2 \cdot \frac{\beta}{\alpha} \cdot N(\mathfrak{b}).$$

Then $0 \neq \gamma' \in \mathfrak{a}$, since $N(\mathfrak{b}) \in \mathfrak{b}$. Furthermore, we have that

$$(\alpha)(\gamma')\mathfrak{b} = (\beta)(N(\mathfrak{b}))\mathfrak{b} = (\alpha)\,(N(\mathfrak{b}))\,\mathfrak{a}.$$

Deleting (α) on both sides leads to $(\gamma')\mathfrak{b} = (N(\mathfrak{b}))\,\mathfrak{a}$. In view of Theorem 5.2, the unit group E is nontrivial in the real quadratic case. Therefore, let $\epsilon \in E$ with $|\epsilon| > 1$. If we choose a nonegative integer n_0 such that

$$\frac{|\gamma'|}{|\epsilon|^{n_0}} \le |N(\mathfrak{a})|,$$

then the assertion follows with $\gamma := \epsilon^{-n_0} \cdot \gamma'$. □

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 $k[x]$-base of the form $\{Q, P + \sqrt{D}\}$ with polynomials $Q, P \in \mathbb{F}_q[x]$, $Q|(D - P^2)$ and

$$|P - \sqrt{D}| < |Q| = |N(\mathfrak{a})| < |P + \sqrt{D}|,$$

or, equivalently, if $(P + \sqrt{D})/Q$ is a reduced real quadratic irrationality. The equality $|Q| = |N(\mathfrak{a})|$ is an immediate consequence of (6.3). In this case, we call the $k[x]$-base $\{Q, P + \sqrt{D}\}$ a reduced $k[x]$-base of $\mathfrak{a}$. If $\operatorname{sgn}(Q) = 1$, then the reduced $k[x]$-base is unique. We can characterize reduced ideals as follows.

THEOREM 8.2. *A primitive $\mathcal{O}_K$-ideal $\mathfrak{a}$ is reduced if and only if*

$$|N(\mathfrak{a})| < \left|\sqrt{D}\right|.$$

PROOF. If $\mathfrak{a}$ is a reduced $\mathcal{O}_K$-ideal, then $\mathfrak{a} = \left[Q, P + \sqrt{D}\right]$, where $Q, P \in k[x]$ are such that $Q|(D - P^2)$ and

$$|P - \sqrt{D}| < |Q| = |N(\mathfrak{a})| < |P + \sqrt{D}|.$$

This can only happen if $|P| = \left|\sqrt{D}\right|$ and even the two highest degree coefficients of P and $\sqrt{D}$ are equal (note that the characteristic of k is different from 2). Thus,

$$|N(\mathfrak{a})| = |Q| < |P + \sqrt{D}| = \left|\sqrt{D}\right|.$$

Conversely, if $\mathfrak{a}$ is a primitive $\mathcal{O}_K$-ideal with $|N(\mathfrak{a})| < \left|\sqrt{D}\right|$, then $\mathfrak{a} = \left[Q, P + \sqrt{D}\right]$ with $Q, P \in k[x]$. We put

$$P' := P - \left\lfloor \frac{P - \sqrt{D}}{Q} \right\rfloor \cdot Q.$$

Clearly, $\mathfrak{a} = \left[Q, P' + \sqrt{D}\right]$ and $\left|P' - \sqrt{D}\right| < |Q|$, since

$$\left| \frac{P' - \sqrt{D}}{Q} \right| = \left| \frac{P - \sqrt{D}}{Q} - \left\lfloor \frac{P - \sqrt{D}}{Q} \right\rfloor \right| < 1.$$

Furthermore, we see that

$$\left|P' + \sqrt{D}\right| = \left|\left(P' - \sqrt{D}\right) + 2\sqrt{D}\right| = \left|\sqrt{D}\right| > |Q|\,,$$

by assumption. Therefore, $\left\{Q, P' + \sqrt{D}\right\}$ is a reduced $k[x]$-base of $\mathfrak{a}$, and thus $\mathfrak{a}$ is reduced. □

LEMMA 8.3. *If $\mathfrak{a}$ is a reduced $\mathcal{O}_K$-ideal, then there does not exist any nonzero $\alpha \in \mathfrak{a}$ such that*

$$|\alpha| < |N(\mathfrak{a})| \quad \textit{and} \quad |\overline{\alpha}| \leq |N(\mathfrak{a})|.$$

PROOF. We have $\mathfrak{a} = \left[Q, P + \sqrt{D}\right]$ where $Q, P \in k[x]$ and

$$\left|P - \sqrt{D}\right| < |Q| = |N(\mathfrak{a})| < \left|P + \sqrt{D}\right|.$$

For any nonzero $\alpha \in \mathfrak{a}$ there exist $U, V \in k[x]$ such that

$$\alpha = UQ + V\left(P + \sqrt{D}\right) \qquad \text{and} \qquad \overline{\alpha} = UQ + V\left(P - \sqrt{D}\right).$$

If $V = 0$ then $U \neq 0$, i.e. $|U| \geq 1$, and $|\alpha| = |\overline{\alpha}|$. Hence

$$|\alpha| = |UQ| \geq |Q| = |N(\mathfrak{a})|\,.$$

and the assertion is true. Now, let $V \neq 0$, i.e. $|V| \geq 1$. We distinguish between two cases. If $|U| \leq |V|$, then $|UQ| < |V|\left|P + \sqrt{D}\right|$, by assumption. Thus

$$|\alpha| = |V|\left|P + \sqrt{D}\right| \geq \left|P + \sqrt{D}\right| > |N(\mathfrak{a})|\,.$$

If $|U| > |V|$, then we analogously show that $|\overline{\alpha}| > |N(\mathfrak{a})|$. □

9. Continued Fractions and Ideals

In this section, we show that the continued fraction expansion of real quadratic irrationalities and the continued fraction expansion of primitive ideals is closely related. Let $\mathfrak{a}$ be any primitive $\mathcal{O}_K$-ideal, and let $Q, P \in \mathbb{F}_q[x]$ with $Q|(D - P^2)$ be such that $\mathfrak{a} = [Q, P + \sqrt{D}]$. If we set $\alpha := (P + \sqrt{D})/Q$, then α is a real quadratic irrationality, and we can compute the continued fraction expansion of α. With $Q_i, P_i \in \mathbb{F}_q[x]$ defined as in (3.2), we let $\mathfrak{a}_1 = \mathfrak{a}$, $Q_0 = Q$, $P_0 = P$, and for $i \in \mathbb{N}$, we let

$$\mathfrak{a}_i = \left[Q_{i-1}, P_{i-1} + \sqrt{D}\right]. \tag{9.1}$$

From (3.3) we know that $\alpha_{i-1} = (P_{i-1} + \sqrt{D})/Q_{i-1}$, for $i \in \mathbb{N}$, where $0 \neq Q_{i-1}, P_{i-1} \in \mathbb{F}_q[x]$ and $Q_{i-1}|(D - P_{i-1}^2)$. 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 which can be found, for example, in [41]. However, we shall prove them using the terminology of integral ideals.

First, we show that each $\mathfrak{a}_i$ is equivalent to $\mathfrak{a} = \mathfrak{a}_1$. By (3.2), we notice that

$$\mathfrak{a}_i = \left[Q_{i-1}, -P_i + \sqrt{D}\right] \quad (i \in \mathbb{N}), \tag{9.2}$$

$$\left(\sqrt{D} - P_i\right) \mathfrak{a}_{i+1} = (Q_i)\, \mathfrak{a}_i \quad (i \in \mathbb{N}). \tag{9.3}$$

THEOREM 9.1. *If* $\mathfrak{a} = \left[Q, P + \sqrt{D}\right]$ *is any primitive* $\mathcal{O}_K$*-ideal and* $\mathfrak{a}_i$ *is defined as in* (9.1)*, then* $\mathfrak{a}_i$ *is a primitive* $\mathcal{O}_K$*-ideal for* $i \in \mathbb{N}$*, and we have that*

$$(Q_0\theta_i)\, \mathfrak{a}_i = (Q_{i-1})\, \mathfrak{a}_1 \quad (i \in \mathbb{N}),$$

where $Q_0\theta_i, Q_0\overline{\theta}_i \in \mathcal{O}_K$.

PROOF. Let $i \in \mathbb{N}$. We know from (2.13) that $Q_0\theta_i, Q_0\overline{\theta}_i \in \mathcal{O}_K$. The main assertion can be proved by induction. For $i = 1$, we trivially have that $(Q_0\theta_1)\mathfrak{a}_1 = (Q_{i-1})\mathfrak{a}_1$. Since $D - P_i^2 = Q_iQ_{i-1}$, we find that

$$\alpha_i = \frac{P_i + \sqrt{D}}{Q_i} = \frac{Q_{i-1}}{\sqrt{D} - P_i}.$$

It follows by (2.12) that

$$Q_{i-1}\theta_{i+1} = \left(\sqrt{D} - P_i\right)\theta_i. \tag{9.4}$$

Using this fact and (9.3) we obtain

$$(Q_{i-1})\,(Q_0\theta_{i+1})\,\mathfrak{a}_{i+1} = (Q_0\theta_i)\,(Q_i)\,\mathfrak{a}_i.$$

By induction, the last term equals $(Q_{i-1})(Q_i)\mathfrak{a}_1$. Thus, we can delete (Q_{i-1}) on both sides and our result follows. □

In view of (6.3), the statement of the theorem is equivalent to

$$(N(\mathfrak{a})\theta_i)\, \mathfrak{a}_i = (N(\mathfrak{a}_i))\, \mathfrak{a}, \tag{9.5}$$

COROLLARY 9.2. *In the situation of Theorem 9.1, we have for* $i \in \mathbb{N}$ *that*

$$\mathfrak{a}_1 = [Q_0\theta_i, Q_0\theta_{i+1}].$$

PROOF. From (9.4) and (9.2), we derive that

$$(Q_{i-1})\,[Q_0\theta_i, Q_0\theta_{i+1}] = (Q_0\theta_i)\,\mathfrak{a}_i$$

and the statement is an immediate consequence of Theorem 9.1. □

Next, we deal with the question, whether there is an index $i \in \mathbb{N}_0$ such that $\mathfrak{a}_{i+1}$ is reduced. We are interested in finding a criterion which is sufficient for this property.

REMARK 9.3. If, in the continued fraction expansion of $\alpha = \alpha_0 := (P_0 + \sqrt{D})/Q_0$, there is an index $i \in \mathbb{N}_0$ such that $\alpha_i = (P_i + \sqrt{D})/Q_i$ is reduced, then the ideal $\mathfrak{a}_{i+1}$ is reduced, because the reduced $k[x]$-base for $\mathfrak{a}_{i+1}$ is given by $\{Q_i, P_i + \sqrt{D}\}$.

THEOREM 9.4. *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*

$$i > I_0 := \max\{1, \deg(Q_0)/2 - (g+1)/2 + 2\}.$$

PROOF. See Theorem 3.3, Remark 9.3, and note that the genus of K is defined by $g = \deg(D)/2 - 1$. □

Conversely, if $\mathfrak{a}_i$ is reduced, the basis representation in (9.1) need not be the reduced one. This means that α_{i-1} is not necessarily reduced.

LEMMA 9.5. *If $\mathfrak{a}_i$ is reduced for an index $i \in \mathbb{N}$, then α_i is reduced.*

PROOF. This follows from Theorem 8.2 and Theorem 3.4. □

Using similar ideas as those employed in the proof of Theorem 4.3 of [41], we can prove the following Lemma, where $\alpha = \alpha_0 := (P_0 + \sqrt{D})/Q_0$.

LEMMA 9.6. *If, in the continued fraction expansion of α, there exists a minimal $l \in \mathbb{N}$ such that $|Q_{l-1}| < |\sqrt{D}|$, then $\mathfrak{a}_l$ is reduced, and*

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

PROOF. By the assumption and (6.3), we have that

$$|Q_l| = |N(\mathfrak{a}_l)| < \left|\sqrt{D}\right|.$$

Thus, we can apply Theorem 8.2 to conclude that $\mathfrak{a}_l$ is reduced. If $l = 1$, then $Q_{l-1} = Q_0$ and $\left|\overline{\theta}_1\right| = 1 = |\theta_1|$. Let $l \geq 2$. First, we notice that

$$|\overline{\alpha}_j| \geq 1 \quad (j \in \{1, \ldots, l-2\}).$$

If we assume that $|\overline{\alpha}_j| < 1$ for some index $j \in \{1, \ldots, l-2\}$, then α_j is reduced. By the above remark, $\mathfrak{a}_{j+1}$ is reduced, and by Theorem 8.2 we conclude that $|Q_j| = |N(\mathfrak{a}_{j+1})| < \left|\sqrt{D}\right|$, which is a contradiction to the minimality of l with this property.

Furthermore, we know from Lemma 3.5 that α_l is not reduced. Since $l \geq 1$, this happens only if $|\overline{\alpha}_l| \geq 1$. Thus, we see from (2.12) that

$$\left|\overline{\theta}_{l+1}\right| = \frac{1}{|\overline{\alpha}_l|} \prod_{j=1}^{l-1} \frac{1}{|\overline{\alpha}_j|} \leq 1.$$

The final part of the theorem follows from (3.9). □

The latter lemma gives an algorithmic criterion for recognizing an index l for which the ideal $\mathfrak{a}_l$ is reduced. Now, let $\mathfrak{b}$ be another reduced ideal which is equivalent to $\mathfrak{a} = \mathfrak{a}_1$. We would like to know if $\mathfrak{b}$ can appear among the ideals found by applying the continued fraction algorithm to $\mathfrak{a}$ in the above manner. The following theorem gives an answer to this question. It corresponds to [41]*Theorem 4.5, and a complete proof for the case of a real quadratic congruence function field is given in [28].

THEOREM 9.7. *Let $\mathfrak{a} = \mathfrak{a}_1$ and $\mathfrak{b}$ be two equivalent reduced integral $\mathcal{O}_K$-ideals, and let $\gamma \in \mathfrak{a}$ be 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 $\gamma = c\mathbb{N}(\mathfrak{a})\theta_\nu$.

PROOF. The existence of such a $\gamma \in \mathfrak{a}$ is guaranteed by Lemma 8.1. We prove the Theorem in several steps.

STEP 1: There exists an index $\nu \in \mathbb{N}$ such that

$$|N(\mathfrak{a})\theta_{\nu+1}| < |\gamma| \leq |N(\mathfrak{a})\theta_\nu|\,.$$

Proof of Step 1: Since $\mathfrak{a} = \mathfrak{a}_1$ is reduced, we know from Theorem 9.5 that α_i is reduced for $i \in \mathbb{N}$. Therefore $|\overline{\alpha}_i| < 1 < |\alpha_i|$. By (2.12) we get

$$|\theta_{i+1}| < |\theta_i|\ ,\ |\theta_1| = 1 \quad \text{and} \quad \left|\overline{\theta}_{i+1}\right| > \left|\overline{\theta}_i\right|. \tag{9.6}$$

Also, we see from (2.3) that $|\theta_{i+1}| \leq \dfrac{1}{q^i}$. This means that $\{|\theta_i|\}_{i\in\mathbb{N}}$ is strictly decreasing and converges to 0. Since $0 < |\gamma| \leq |N(\mathfrak{a})|$, there must exist some $\nu \in \mathbb{N}$ such that

$$|\theta_{\nu+1}| < \frac{|\gamma|}{|N(\mathfrak{a})|} \leq |\theta_\nu|\,.$$

STEP 2: We have that

$$\left|N(\mathfrak{a})\overline{\theta}_{\nu+1}\right| > |\overline{\gamma}|\,.$$

Proof of Step 2: By Corollary 9.2, we have that $N(\mathfrak{a})\theta_{\nu+1} \in \mathfrak{a}$. Hence,

$$N(\mathfrak{a})\theta_{\nu+1}N(\mathfrak{b}) \in (N(\mathfrak{b}))\,\mathfrak{a} = (\gamma)\mathfrak{b}$$

and $N(\mathfrak{a})\theta_{\nu+1}N(\mathfrak{b}) = \gamma\beta$ for some $0 \neq \beta \in \mathfrak{b}$. From the first step, we see that $|\beta| < |N(\mathfrak{b})|$. Since $\mathfrak{b}$ is reduced, we can apply Lemma 8.3 to deduce that

$$|N(\mathfrak{b})| < |\overline{\beta}| = \frac{\left|N(\mathfrak{a})\overline{\theta}_{\nu+1}\right|}{|\overline{\gamma}|}\,|N(\mathfrak{b})|\,,$$

and the assertion follows by deleting $|N(\mathfrak{b})|$ on both sides.

STEP 3: There exists a $c \in \mathbb{F}_q{}^*$ such that $\gamma = c \cdot N(\mathfrak{a})\theta_\nu$.

Proof of Step 3: Since $\gamma \in \mathfrak{a}$, Corollary 9.2 yields some polynomials $U, V \in k[x]$ such that

$$\gamma = UN(\mathfrak{a})\theta_\nu + VN(\mathfrak{a})\theta_{\nu+1} \quad \text{and} \quad \overline{\gamma} = UN(\mathfrak{a})\overline{\theta}_\nu + VN(\mathfrak{a})\overline{\theta}_{\nu+1}.$$

Suppose that $|U| \leq |V|$. Then,

$$|\overline{\gamma}| = \left|VN(\mathfrak{a})\overline{\theta}_{\nu+1}\right|.$$

It follows from the second step that we must have $|V| < 1$. Thus, $U = V = 0$ and $\gamma = 0$, which is a contradiction. Now, let $|U| > |V|$. Hence,

$$|\gamma| = |UN(\mathfrak{a})\theta_\nu|.$$

Using Step 1 we conclude that $|U| \leq 1$. Then $V = 0$ and $U = c$ for some $c \in {\mathbb{F}_q}^*$.

Step 4: We have that

$$N(\mathfrak{b}) = N(\mathfrak{a}_\nu).$$

Proof of Step 4: First, we obtain that $N(\mathfrak{a})N(\theta_\nu) = c_1 N(\mathfrak{a}_\nu)$ by applying Lemma 6.2 to (9.5). Step 3 yields $N(\gamma) = c_2 N(\mathfrak{a})^2 N(\theta_\nu) = c_3 N(\mathfrak{a})N(\mathfrak{a}_\nu)$. On the other hand, $N(\gamma) = c_4 N(\mathfrak{b})N(\mathfrak{a})$, since $(\gamma)\mathfrak{b} = (N(\mathfrak{b}))\,\mathfrak{a}$. We find that $N(\mathfrak{b}) = N(\mathfrak{a}_\nu)$, since $\operatorname{sgn}(N(\mathfrak{b})) = \operatorname{sgn}(N(\mathfrak{a}_\nu)) = 1$ (note that $c_1, c_2, c_3, c_4 \in k^*$).

Step 5: $\mathfrak{b} = \mathfrak{a}_\nu$.
Proof of Step 5: By Step 4, we have that

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

From (9.5) and Step 3, we know that the last term equals $(\gamma)\mathfrak{a}_\nu$. Thus, we must have that $\mathfrak{b} = \mathfrak{a}_\nu$. □

So far, we have proved that the continued fraction algorithm applied to a reduced ideal produces all equivalent, reduced ideals. This fact is essential for the establishment of our *giant steps*. In each $\mathcal{O}_K$-ideal class, we therefore have precisely one cycle of reduced ideals. Since k is finite, this cycle is finite. The continued fraction expansion applied to any primitive $\mathcal{O}_K$-ideal in a class yields a reduced $\mathcal{O}_K$-ideal in the same class after a finite number of steps and then produces all reduced ideals in the class. Thus, each ideal class can be represented by exactly one cycle of reduced ideals. Basically, one has a structure (the cycle of reduced ideals) within a structure (the ideal class group). This concept is called the *infrastructure* in real quadratic function fields and is due to Shanks [27]. These considerations correspond to the observations made in real quadratic number fields (see also [4]).

10. Distance and Giant Steps

We now introduce the concept of distance between equivalent, reduced ideals; this will allow us to provide an ordering of the reduced ideals belonging to the same ideal class. We will follow the notation of [37] which differs somewhat from that of [41]. Let $\mathfrak{a} = \mathfrak{a}_1$ and $\mathfrak{b}$ be two equivalent, reduced, integral $\mathcal{O}_K$-ideals. By Theorem 9.7, there exists some $\nu \in \mathbb{N}$ such that $\mathfrak{b} = \mathfrak{a}_\nu$, and by Theorem 9.1, 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

$$\delta(\mathfrak{b}, \mathfrak{a}) = \delta(\mathfrak{a}_\nu, \mathfrak{a}) := \deg\left(\overline{\theta}_\nu\right). \tag{10.1}$$

Remark 10.1. Distance is only defined between equivalent, reduced ideals. From (2.12) and because $\mathfrak{a}_i$ is reduced for $i \geq 1$, we deduce that the distance function δ_i is strictly increasing in i, i.e. $\delta(\mathfrak{a}_{i+1}, \mathfrak{a}) > \delta(\mathfrak{a}_i, \mathfrak{a})$. Since the values of the distance function are integers, we have $\delta_{t+i} \geq \delta_t + i$. Thus, if it happens that $\delta(\mathfrak{a}_i, \mathfrak{a}) = \delta(\mathfrak{a}_j, \mathfrak{a})$, we conclude that $\mathfrak{a}_i = \mathfrak{a}_j$. Especially, if there are $\nu, j, l \in \mathbb{N}$ such that $\delta(\mathfrak{a}_j, \mathfrak{a}) \leq \delta(\mathfrak{a}_\nu, \mathfrak{a}) \leq \delta(\mathfrak{a}_l, \mathfrak{a})$, then $\mathfrak{a}_\nu \in \{\mathfrak{a}_i; j \leq i \leq l\}$, and $\delta(\mathfrak{a}_i, \mathfrak{a}) = 0$ if and only if $\mathfrak{a}_i = \mathfrak{a}_1$. Conversely, if $\mathfrak{a}_i = \mathfrak{a}_j$ then $\delta(\mathfrak{a}_i, \mathfrak{a}) = \delta(\mathfrak{a}_j, \mathfrak{a}) + lR$, where R is the regulator of K. In this case, we deduce from Theorem 9.1 that $\overline{\theta}_i$ and $\overline{\theta}_j$ differ only by a $\mathcal{O}_K$-unit.

Furthermore, by (3.9), (2.12), and Proposition 3.2, we see that

$$\delta(\mathfrak{a}_i, \mathfrak{a}) = \tfrac{1}{2}\deg(D) - \deg(Q_0) + \sum_{j=1}^{i-2} \deg(a_j) \quad (i \in \mathbb{N}, i \geq 2). \tag{10.2}$$

In the sequel, we let $\mathfrak{r} = \mathfrak{r}_1 = (1) = \mathcal{O}_K = [1, \sqrt{D}]$. With reference to (9.1), we have $P_0 = P = 0$, $Q_0 = Q = 1$ and $\alpha_0 = \alpha = \sqrt{D}$. Clearly, $\mathfrak{r}$ is reduced, because $|N(\mathfrak{r})| = 1 < |\sqrt{D}|$. From Theorem 9.1 and (3.9), the ideals in (9.1) are reduced principal ideals, i.e. $\mathfrak{r}_{i+1} = (\overline{\theta}_{i+1})$, for $i \in \mathbb{N}_0$, where $\overline{\theta}_{i+1} \in \mathcal{O}_K$. We always put $\delta_i := \delta(\mathfrak{r}_i, \mathfrak{r})$. Then δ_i is defined for all $i \in \mathbb{N}$. Let $\mathfrak{b}$ be an arbitrary reduced $\mathcal{O}_K$-ideal. We develop the continued fraction expansion of $\mathfrak{b}$ as in (9.1) and denote by P_i', Q_i', θ_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 $S \in k[x]$ and a primitive $\mathcal{O}_K$-ideal $\mathfrak{c}$ such that $\mathfrak{r}_s\mathfrak{b}_t = (S)\mathfrak{c}$. We apply the continued fraction algorithm to $\mathfrak{c} = \mathfrak{c}_1$. By Theorem 9.4, it is guaranteed that, after a finite number of steps, we obtain a reduced ideal equivalent to $\mathfrak{c}$. We denote by P_i'', Q_i'' and θ_i'' the quantities appearing in the continued fraction expansion applied to $\mathfrak{c}$. In view of Lemma 9.6, 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

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

Thus, $\mathfrak{c}_l$ and $\mathfrak{b}$ are equivalent. Since they both are reduced, by Theorem 9.7 there must exist some $\nu \in \mathbb{N}$ such that $\mathfrak{c}_l = \mathfrak{b}_\nu$.

THEOREM 10.2. *In the above situation there exists some $C \in k^*$ such that*

$$\theta'_\nu = C\theta_s\, \theta'_t\, \frac{\theta''_l}{S}.$$

Furthermore, we have that

$$\delta'_\nu = \delta'_t + \delta_s - f,$$

where $f := \deg(S) - \deg(\overline{\theta''_l}) \in \mathbb{N}$ such that $0 \leq f \leq 2g$.

PROOF. From (9.5), we see that

$$(\theta_s)\mathfrak{r}_s = (N(\mathfrak{r}_s)),$$
$$(N(\mathfrak{b})\theta'_t)\mathfrak{b}_t = (N(\mathfrak{b}_t))\mathfrak{b},$$

and

$$(N(\mathfrak{c})\theta''_l)\mathfrak{c}_l = (N(\mathfrak{c}_l))\mathfrak{c}.$$

Since $\mathfrak{r}_s\mathfrak{b}_t = (S)\mathfrak{c}$, we can apply Lemma 6.2 to conclude that

$$N(\mathfrak{r}_s)N(\mathfrak{b}_t) = C_1 \cdot S^2 N(\mathfrak{c})$$

for some constant $C_1 \in k^*$. This yields

$$\left(N(\mathfrak{b})N(\mathfrak{c})S\theta_s\theta'_t\theta''_l\right)\mathfrak{c}_l = \left(S^2N(\mathfrak{c})N(\mathfrak{c}_l)\right)\mathfrak{b}.$$

Hence,

$$0 \neq \gamma := \frac{N(\mathfrak{b})N(\mathfrak{c})S\theta_s\theta'_t\theta''_l}{S^2N(\mathfrak{c})N(\mathfrak{c}_l)} \cdot N(\mathfrak{c}_l) = \theta_s\theta'_t\theta''_l \cdot \frac{N(\mathfrak{b})}{S}d \in \mathfrak{b}.$$

γ also has the property that $(\gamma)\mathfrak{c}_l = (N(\mathfrak{c}_l))\mathfrak{b}$. We also derive from (9.6) that

$$0 < |\gamma| \leq |N(\mathfrak{b})|.$$

Theorem 9.7 then says that there must exist some $\nu \in \mathbb{N}$ and a constant $C_2 \in k^*$ such that

$$\gamma = C_2 N(\mathfrak{b})\theta'_\nu.$$

By comparing this with the definition of γ, we find that

$$\theta'_\nu = C \cdot \theta_s\theta'_t\frac{\theta''_l}{S}$$

for some $C \in k^*$. Conjugation and evaluating degrees yields

$$\delta'_\nu = \delta'_t + \delta_s - f.$$

Finally, by (9.6), (9.5), and (3.9) we obtain

$$\frac{\left|\overline{\theta''_l}\right|}{|S|} \geq \frac{\left|\overline{\theta''_l}\theta''_l\right|}{|S|} \geq \frac{|N(\mathfrak{c}_l)|}{|S||N(\mathfrak{c})|} \geq \frac{1}{|N(\mathfrak{r}_s)||N(\mathfrak{b}_t)|},$$

since $|N(\mathfrak{r}_s)N(\mathfrak{b}_t)| = |S^2N(\mathfrak{c})|$ and $0 \neq S \in k[x]$. Equivalently, we have that

$$f \leq \deg(N(\mathfrak{r}_s)) + \deg(N(\mathfrak{b}_t)) \leq 2g,$$

since $\mathfrak{r}_s$ and $\mathfrak{b}_t$ are reduced, and from Theorem 8.2 we deduce

$$\deg(N(\mathfrak{r}_s)), \deg(N(\mathfrak{b}_t)) \leq \frac{1}{2}\deg(D) - 1 = g.$$

Thus, we proved the upper bound on f. The lower bound trivially follows from Lemma 9.6. □

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 nonnegative. In general, f is small compared to δ_s or δ'_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 large steps through the cycle of reduced ideals equivalent to $\mathfrak{b}$. In the situation of the theorem we define a new operation called *giant step* by

$$\mathfrak{r}_s * \mathfrak{b}_t := (\mathfrak{b}_\nu, f) = (\mathfrak{c}_l, f)\,. \tag{10.3}$$

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.

So far, we haven't used any information about periodicity and symmetry. Let m be the quasi-period of the continued fraction expansion of $\alpha = \sqrt{D}$. From Theorem 4.2, we deduce that $\mathfrak{r}_{m+1} = \mathfrak{r}_1$, and from Theorem 5.2, we see that $R = \delta_{m+1}$, where R is the regulator of K. By Proposition 3.8 we get

$$\mathfrak{r}_{\lambda m+i+1} = \mathfrak{r}_{i+1} \quad (i \in \mathbb{N})\,. \tag{10.4}$$

Also, by Lemma 4.4, Lemma 2.2, and 2.12, we get

$$\delta_{\lambda m+i+1} = \lambda \cdot R + \delta_{i+1} \quad (i, \in \mathbb{N})\,. \tag{10.5}$$

By Remark 10.1 and (10.2) with $t := 2$ and $i = t + (i-2)$ we have that

$$\delta_i \geq \frac{1}{2}\deg(D) + i - 2 = g + i - 1 \quad (i \in \mathbb{N}, i \geq 2)\,. \tag{10.6}$$

Next, we consider the effects of symmetries in the case $\alpha = \sqrt{D}$. We continue applying the continued fraction algorithm to $\mathfrak{r}_1 = \mathfrak{r} = \mathcal{O}_K$. For $\mathfrak{r}_i$ defined in (9.1), we get

$$\overline{\mathfrak{r}}_i = \left[Q_{i-1}, -P_{i-1} + \sqrt{D}\right] = \left[Q_{i-1}, P_i + \sqrt{D}\right] \quad (i \in \mathbb{N})\,, \tag{10.7}$$

where $\overline{\mathfrak{r}}_i$ denotes the conjugate ideal of $\mathfrak{r}_i$. We can improve this by making use of the following Proposition.

PROPOSITION 10.3. *Let $\tilde{\delta}_i := \delta(\overline{\mathfrak{r}}_i, \mathfrak{r})$. Then, we have for $i = 1, \ldots, m+1$:*

(a) $\overline{\mathfrak{r}}_i = \mathfrak{r}_{m-i+2}$;
(b) $\tilde{\delta}_i = \delta_{m-i+2}$;
(c) $R = \tilde{\delta}_i + \delta_i - \deg(Q_{i-1})$.

PROOF. This follows easily from Theorem 4.7 and (3.9). □

We see that the conjugate ideals are exactly those which occur before the quasi-period is reached.

11. Baby Step-Giant Step Algorithms in the Infrastructure

The goal of this section is to describe two variants of infrastructure methods for real quadratic function fields. The first algorithm is an immediate consequence of the results in Section 10. Baby steps are iterative steps in the continued fraction expansion. A giant step is the combined multiplication and reduction operation of (10.3). The idea is to create a stock of principal, reduced ideals up to an index s which we determine later for complexity reasons. By continued giant steps we jump to principal, reduced ideals in the same chain which lie about δ_s away from each other. Because of the quasi-periodicity of the continued fraction expansion of $\alpha = \sqrt{D}$ we must reach one of the stored ideals. We only have to guarantee that the step width is positive, and that the step width is not greater than the length of the initial interval. In the algorithm the quantity s is chosen sufficiently large such that we really take a step forward. This is guaranteed if $s \geq \frac{1}{2} \deg(D) + 1$. The inputs are $q \in \mathbb{N}$ such that $\mathbb{F}_q$ is a finite field with odd characteristic, and a monic squarefree polynomial $D \in \mathbb{F}_q[x]$ of even degree. The output is R, the regulator of the real quadratic function field $K = \mathbb{F}_q(x)(\sqrt{D})$.

Algorithm 11.1. **Regulator (original baby step-giant step)**
Input: q, D
Output: R

1.) Put $c_0 := 3/2$ and $s := \left[c_0 \cdot q^{\deg(D)/4} \right]$.

2.) By developing the continued fraction expansion of $\alpha = \sqrt{D}$, compute $\mathfrak{a}_i$ and δ_i for $i = 1, \ldots, s$, starting with $\mathfrak{a}_1 = (1) = \mathcal{O}_K$. Store them in the form

$$(\mathfrak{a}_i, \delta_i) = (N(\mathfrak{a}_i), P_{i-1}, \delta_i)$$

If $Q_j \in {\mathbb{F}_q}^*$ for a minimal $1 \leq j \leq s-1$ then

$$R := \delta_{j+1} \quad ; \quad \textbf{return}(R).$$

3.) $\mathfrak{b}_1 := \mathfrak{a}_s$; $f_1 := 0$; $\delta'_1 := \delta_s$; $j := 0$;

4.) **Do** {

$$\begin{aligned} j &:= j+1; \\ (\mathfrak{b}_{j+1}, f_{j+1}) &:= \mathfrak{a}_s * \mathfrak{b}_j; \\ \delta'_{j+1} &:= \delta_s + \delta'_j + f_{j+1}; \end{aligned}$$

}
while $(\mathfrak{b}_{j+1} \notin \{\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_s\})$;

5.) We have $\mathfrak{b}_{j+1} = \mathfrak{a}_i \in \{\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_s\}$ and then

$$R := \delta'_{j+1} - \delta_i; \quad \textbf{return}(R).$$

PROOF. If we can terminate the algorithm after the second step, we have $Q_j \in {\mathbb{F}_q}^*$. From Theorem 4.2 we know $m = j$, and the result is correct, because $R = \delta_{m+1} = \delta_{j+1}$.

In the other case we get $R > \delta_s = \delta'_1$. By definition of $\mathfrak{b}_j$ and Theorem 10.2 we deduce that for each $\mathfrak{b}_j$ there exists an index $\lambda_j \in \mathbb{N}$ such that $\mathfrak{b}_j = \mathfrak{a}_{\lambda_j}$, where

$$\delta'_{j+1} = \delta'_j + \delta_s + f_{j+1} \quad \text{and} \quad -\deg(D) + 2 \leq f_{j+1} \leq 0. \tag{11.1}$$

Certainly, we have

$$\delta'_{j+1} - \delta'_j \leq \delta_s.$$

Now, we easily see that

$$s \geq \frac{1}{2}\deg(D) + 1.$$

By (10.6) we conclude $\delta_s \geq \deg(D) - 1$. Inserting this in (11.1) leads to

$$\delta'_{j+1} > \delta'_j.$$

Since $R > \delta'_1$ and $\mathfrak{b}_j = \mathfrak{a}_{\lambda_j}$, there must be an index $\nu \in \mathbb{N}$ such that

$$\delta_{\lambda_\nu} = \delta'_\nu \leq R = \delta_{m+1} < \delta'_{\nu+1} = \delta_{\lambda_{\nu+1}}.$$

By Remark 10.1 we get $\lambda_{\nu+1} = m + i$, where $i \geq 2$. Using (10.5) we see that

$$\delta'_{\nu+1} = \delta_{m+i} = R + \delta_i,$$

and by (11.1), we conclude that

$$\delta_i = \delta'_{\nu+1} - R = \delta_s + \delta'_\nu + f_{\nu+1} - R \leq \delta_s.$$

Remark 10.1 says that $\mathfrak{a}_i \in \{\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_s\}$. Finally,

$$\mathfrak{b}_{\nu+1} = \mathfrak{a}_{\lambda_{\nu+1}} = \mathfrak{a}_{m+i} = \mathfrak{a}_i,$$

by (10.4), and $R = \delta'_{\nu+1} - \delta_i$. □

We now show how the symmetry results of the previous section apply to produce an even faster baby step-giant step method. With the knowledge of Proposition 10.3 we are able to take giant steps with step width about $2\delta_s$ with the same amount of storage. Again, we have to guarantee that the step width is not too great. Therefore, we enlarge the initial interval a little bit, i.e. we develop the continued fraction algorithm up to an index $s + T$. We only claim that $s \geq \frac{1}{2}\deg(D) + 1$ and $T \geq \frac{1}{4}\deg(D)$.

The inputs of the algorithm are $q \in \mathbb{N}$ such that $\mathbb{F}_q$ is a finite field with odd characteristic, and a monic squarefree polynomial $D \in \mathbb{F}_q[x]$ of even degree. The output is R, the regulator of the real quadratic function field $K = \mathbb{F}_q(x)(\sqrt{D})$.

ALGORITHM 11.2. **Regulator (optimized baby step-giant step)**
Input: q, D
Output: R

1.) Put $s := \left[q^{\deg(D)/4} \right]$ and $T := \left[\frac{1}{4} \deg(D) + 1 \right]$.

2.) By developing the continued fraction expansion of $\alpha = \sqrt{D}$, compute $\mathfrak{a}_i$ and δ_i for $i = 1, \ldots, s+T$, starting with $\mathfrak{a}_1 = (1) = \mathcal{O}_K$. Store them 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 $1 \leq \nu < s+T$ then

$$R := 2\delta_{\nu+1} - \deg(Q_\nu); \qquad \textbf{return}(R).$$

If $\dfrac{Q_\mu}{\operatorname{sgn}(Q_\mu)} = \dfrac{Q_{\mu+1}}{\operatorname{sgn}(Q_{\mu+1})}$ for a minimal $1 \leq \mu < s+T$ then

$$R := 2\delta_{\mu+1} - \deg(Q_\mu) + \deg(a_{\mu+1}); \qquad \textbf{return}(R).$$

3.) $(\mathfrak{b}_1, f_1) := \mathfrak{a}_s * \mathfrak{a}_s$; $\delta_1' := 2\delta_s + f_1$; $j := 1$;

4.) **While** $(\mathfrak{b}_j \notin \{\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_{s+T}\} \cup \{\overline{\mathfrak{a}}_1, \overline{\mathfrak{a}}_2, \ldots, \overline{\mathfrak{a}}_{s+T}\})$ {

$$\begin{aligned} (\mathfrak{b}_{j+1}, f_{j+1}) &:= \mathfrak{b}_1 * \mathfrak{b}_j; \\ \delta_{j+1}' &:= \delta_1' + \delta_j' + f_{j+1}; \\ j &:= j+1; \end{aligned}$$

}

5.) We have $\mathfrak{b}_j \in \{\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_{s+T}\} \cup \{\overline{\mathfrak{a}}_1, \overline{\mathfrak{a}}_2, \ldots, \overline{\mathfrak{a}}_{s+T}\}$.

If $\mathfrak{b}_j = \mathfrak{a}_i \in \{\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_{s+T}\}$ **then**

$$R := \delta_j' - \delta_i; \qquad \textbf{return}(R).$$

If $\mathfrak{b}_j = \overline{\mathfrak{a}}_l \in \{\overline{\mathfrak{a}}_1, \overline{\mathfrak{a}}_2, \ldots, \overline{\mathfrak{a}}_{s+T}\}$ **then**

$$R := \delta_j' + \delta_l - \deg(Q_{l-1}); \qquad \textbf{return}(R).$$

Proof. (*Sketch*) We mainly follow the ideas of the proof of Algorithm 11.1. If we can terminate the algorithm after the second step, it follows from Corollary 4.11 that the result is correct. Otherwise, we have $R \geq \delta_1'$ and we get from Theorem 10.2 that for all $j \in \mathbb{N}$ we have $\mathfrak{b}_j = \mathfrak{a}_{\lambda_j}$ with $\lambda_j \in \mathbb{N}$. Also

$$\delta_1' = 2\delta_s + f_1 \quad \text{and} \quad -\deg(D) + 2 \leq f_1 \leq 0,$$

$$\delta_{j+1}' = \delta_j' + \delta_1' + f_{j+1} \quad \text{and} \quad -\deg(D) + 2 \leq f_{j+1} \leq 0.$$

Then $\delta_1' \leq 2\delta_s$. Furthermore, by the choice of s, we see that $\delta_s \geq \deg(D) - 1$.It follows for $i \in \mathbb{N}$ that the step width is $\delta_{j+1}' - \delta_j' \leq \delta_1' \leq 2\delta_s$, and

$$\delta_{j+1}' = \delta_j' + 2\delta_s + f_1 + f_{j+1} > \delta_j'.$$

By Proposition 10.3, Remark 10.1 and (10.5) we conclude

$$\delta_{m+s+T} - \tilde{\delta}_{s+T} \geq 2\delta_s + 2T - \deg(Q_{s+T-1}) > 2\delta_s.$$

This is the length of the interval which we control. Then (10.4), Remark 10.1 and Proposition 10.3 imply that there must exist some $\mu \in \mathbb{N}$ such that

$$\mathfrak{b}_\mu \in \{\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_{s+T}\} \cup \{\overline{\mathfrak{a}}_1, \overline{\mathfrak{a}}_2, \ldots, \overline{\mathfrak{a}}_{s+T}\}.$$

If $\mathfrak{b}_\mu = \mathfrak{a}_i \in \{ \mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_s \}$, then $R = \delta'_\mu - \delta_i$ as in the proof of Algorithm 11.1. If $\mathfrak{b}_\mu = \overline{\mathfrak{a}}_l \in \{ \overline{\mathfrak{a}}_1, \overline{\mathfrak{a}}_2, \ldots, \overline{\mathfrak{a}}_{s+T} \}$, then we have from Proposition 10.3 that $\delta'_\mu = \tilde{\delta}_l = \delta_{m-l+2}$, and that

$$R = R + \delta'_\mu - \tilde{\delta}_l = \delta'_\mu + \delta_l - \deg(Q_{l-1}).$$

□

We end this section by a brief discussion of the complexity of the algorithms. The baby step-giant step algorithms to compute the regulator R of a real quadratic congruence function field K have a complexity

$$O\left(q^{\frac{1}{4} \deg(D)} \right),$$

where we use normal Big-O notation. This follows e.g. from a result of [9] which is known as the *Brauer-Siegel Theorem* for algebraic function fields:

$$\lim_{g \to \infty} \frac{\log(h)}{\log(q^{g-1})} = 1,$$

where g denotes the genus and h the divisor class number of K. Since $g = 1/2 \deg(D) - 1$, we may assume that

$$h = O\left(q^{\frac{1}{2} \deg(D)} \right).$$

On the other hand, we know that $h = R \cdot h'$, where h' denotes the ideal class number of K. In general, we expect on average that h' is small, and that h' is 1 almost always. If the regulator is big, we may assume that in most cases $h' = O(1)$, and then

$$R = O\left(q^{\frac{1}{2} \deg(D)} \right).$$

Furthermore, if we assume that an analogue result of *Levy's Theorem* is true (see for example [41], Theorem 5.1), then

$$m = O(R) = O\left(q^{\frac{1}{2} \deg(D)} \right).$$

We see that an optimal choice for the number of baby steps s should be

$$s \approx O\left(q^{\frac{1}{4} \deg(D)} \right),$$

and that the number of giant steps

$$z \approx O\left(q^{\frac{1}{4} \deg(D)} \right).$$

In the continued fraction expansion there are only operations which depend on polynomial arithmetic in finite fields. We know from Proposition 3.2 that the degrees of the polynomials are bounded by $\deg(D)$. The same argument holds for the quantities appearing in the ideal product, and by Theorem 9.4 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 $\deg(D)$,

i.e. $O(\,(\log(q))^{\epsilon}\,\deg(\,D\,)^{\beta}\,)$ for appropriate $\epsilon,\,\beta > 0$. Asymptotically, those factors are included in $O\,(\,q^{\,1/4\,\deg(\,D\,)}\,)$. Then the total complexity equals

$$O\,(\,s\,+\,z\,)\,=\,O\left(\,q^{\,\frac{1}{4}\,\deg(\,D\,)}\,\right).$$

The baby step algorithms have a complexity of

$$O\left(\,q^{\,\frac{1}{2}\,\deg(\,D\,)}\,\right),$$

because m iterations in the continued fraction expansion have to be performed. Thus, the combined baby step-giant step strategy produces a very quick method to calculate R.

In this paper, we have discussed various elementary results and algorithms in the infrastructure of real quadratic function fields of odd characteristic. In particular, we showed explicitly how Shanks' baby step-giant step algorithm known from the group-like setting also generalizes to the infrastructure in the ideal class group of a real quadratic function field. With this model, more involved methods such as the ones in [32, 33, 31] are applicable. There, the authors were able to optimize computations by making use of the arithmetic of the zeta function and an approximation of the divisor class number h of K. The idea in those papers is as follows: First, one uses the analytic class number formula for h in order to derive an approximation E of h. By evaluating all Euler factors up to a degree λ, one obtains E and also computes a real number U such that

$$|h - E| \leq U.$$

Thus $h \in [E - U, E + U]$. One then uses a generic method such as the baby step-giant step method or the Pollard rho method for searching through the interval $[E - U, E + U]$ to compute h. By choosing $\lambda \sim (2g - 1)/5$, one then obtains an approximate complexity of the algorithm of $O(q^{\frac{2g-1}{5}})$. For details on the complexity and an implementation, we mention [31]. For generalizations and further results, we refer to [35, 24].

Acknowledgements.

The author is indebted to an anonymous referee for carefully proof-reading the manuscript and for making valuable suggestions.

References

[1] W. W. Adams and M. J. Razar, *Multiples of points on elliptic curves and continued fractions* Proc. London Math Soc. (3) **41** (1980), 481–498.

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

[3] E. Artin, *Quadratische Körper im Gebiete der höheren Kongruenzen II*, Math. Z. **19** (1924), 207–246.

[4] H. Cohen, A Course in Computational Algebraic Number Theory, Springer-Verlag, Berlin, 1993.

[5] H. Cohen, G. Frey, R. Avanzi, C. Doche, T. Lange, K. Nguyen and F. Vercouteren, Handbook of Elliptic and Hyperelliptic Curve Cryptography, Discrete Mathematics and Its Applications **34**, Chapman & Hall/CRC, Boca Raton, 2006.
[6] M. Deuring, Lectures on the Theory of Algebraic Functions of One Variable, Lecture Notes in Mathematics **314**, Springer-Verlag, Berlin-Heidelberg, 1973.
[7] A. Enge, *How to distinguish hyperelliptic curves in even characteristic* in: Public-Key Cryptography and Computational Number Theory, eds. K. Alster, J. Urbanowicz, and H. C. Williams, De Gruyter, Berlin, 2001, 49–58.
[8] S. Erickson, M. J. Jacobson, Jr., N. Shang, S. Shen and A. Stein, *Explicit formulas for real hyperelliptic curves of genus* 2 *in affine representation*, in: International Workshop on the Arithmetic of Finite Fields – WAIFI 2007, Lect. Notes Comput. Sci. **4547**, Springer-Verlag, (2007), 202–218.
[9] S. K. Gogia and I. S. Luthar, *The Brauer-Siegel theorem for algebraic function fields*, J. Reine Angew. Math. **299/300** (1978), 28–37.
[10] M. J. Jacobson, Jr., A. J. Menezes and A. Stein, *Hyperelliptic curves and cryptography*, in: High Primes and Misdemeanours: lectures in honour of the 60th birthday of Hugh Cowie Williams, Fields Institute Communications **41**, American Mathematical Society, 2004, 255–282.
[11] M. J. Jacobson, Jr., R. Scheidler and A. Stein, *Fast arithmetic on hyperelliptic curves via continued fraction expansions*, in: Advances in Coding Theory and Cryptology, volume 3 of Series on Coding Theory and Cryptology 2, eds. T. Shaska, W. C. Huffman, D. Joyner, and V. Ustimenko, World Scientific Publishing Co. Pte. Ltd., Hackensack, New Jersey, 2007, 201–244.
[12] M. J. Jacobson, Jr., R. Scheidler and A. Stein, *Cryptographic protocols on real hyperelliptic curves*, Adv. Math. Commun. **1** (2007), 197–221.
[13] P. Kaplan and K. S. Williams, *The distance between ideals in the orders of a real quadratic field*, Enseign. Math. (2) **36** (1990), 321–358.
[14] N. Koblitz, *Hyperelliptic cryptosystems*, J. Cryptology **1** (1989), 139–150.
[15] T. Lange, *Formulae for arithmetic on genus 2 hyperelliptic curves*, Appl. Algebra Engrg. Comm. Comput. **15** (2005), 295–328.
[16] H. W. Lenstra, Jr., *On the calculation of regulators and class numbers of quadratic fields*, London. Math. Soc. Lecture Note Ser. **56** (1982), 123–150.
[17] D. Lorenzini, An invitation to arithmetic geometry, Graduate Studies in Mathematics **9**, AMS, Providence, 1996.
[18] A. J. Menezes, Y. Wu and R. J. Zuccherato, *An elementary introduction to hyperelliptic curves*, in: Koblitz, N.: Algebraic Aspects of Cryptography, Springer-Verlag, Berlin Heidelberg New York, 1998, 155–178.
[19] S. Paulus and H.-G. Rück, *Real and imaginary quadratic representations of hyperelliptic function fields*, Math. Comp. **68** (1999), 1233–1241.
[20] O. Perron, Die Lehre von den Kettenbrüchen, Teubner, Leipzig, 1913.
[21] K. H. Rosen, Elementary Number Theory and its Applications, Addison Wesley Publishing Company, Reading, 1993.
[22] M. Rosen, Number Theory in Function Fields, Springer-Verlag, New York, 2002.
[23] R. Scheidler, A. Stein and H. C. Williams, *Key-exchange in real quadratic congruence function fields*, Des. Codes and Cryptogr. **7** (1996), 153–174.
[24] R. Scheidler and A. Stein, *Class number approximation in cubic function fields*, Contrib. Discrete Math. **2** (2007), 107–132.
[25] F. K. Schmidt, *Analytische Zahlentheorie in Körpern der Charakteristik p*, Math. Z. **33** (1931), 1–32.
[26] D. Shanks, *Class number, a theory of factorization and genera*, in: Proc. Symp. Pure Math. 20, 1969, AMS, Providence, 1971, 415–440.

[27] D. Shanks, *The infrastructure of a real quadratic field and its applications*, in: Proceedings of the Number Theory Conference, Boulder, Colo., 1972, 1972, 217–224.
[28] A. Stein, Baby step-giant step-verfahren in reell-quadratischen kongruenzfunktionenkörpern mit charakteristik ungleich 2, Master's thesis, Universität des Saarlandes, Saarbrücken, Germany, 1992.
[29] A. Stein, *Equivalences between elliptic curves and real quadratic congruence function fields*, J. Théor. Nombres Bordeaux **9** (1997), 75–95.
[30] A. Stein, *Sharp upper bounds for arithmetics in hyperelliptic function fields*, J. Ramanujan Math. Soc. **16** (2001), 119–203.
[31] A. Stein and E. Teske, *Explicit bounds and heuristics on class numbers in hyperelliptic function fields*, Math. Comp. **71** (2002), 837–861.
[32] A. Stein and H. C. Williams, *An improved method of computing the regulator of a real quadratic function field*, in: Algorithmic Number Theory ANTS-III, Lecture Notes in Computer Science **1423**, Springer, Berlin, 1998, 607–620.
[33] A. Stein and H. C. Williams, *Some methods for evaluating the regulator of a real quadratic function field*, Experiment. Math. **8** (1999), 119–133.
[34] A. Stein and H. G. Zimmer, *An algorithm for determining the regulator and the fundamental unit of a hyperelliptic congruence function field*, in: Proc. 1991 Int. Symp. on Symbolic and Algebraic Computation, ISAAC, Bonn, July 15-17, pages 183–184, ACM Press, 1991.
[35] A. Stein and E. Teske, *The parallelized Pollard kangaroo method in real quadratic function fields*, Math. Comp. **71** (2002), 793–814.
[36] A. J. Stephens and H. C. Williams, *Computation of real quadratic fields with class number one*, Math. Comp. **51** (1988), 809–824.
[37] A. J. Stephens and H. C. Williams, *Some computational results on a problem concerning powerful numbers* Math. Comp. **50** (1988), 619–632.
[38] H. Stichtenoth, Algebraic Function Fields and Codes, Springer-Verlag, Berlin, 1993.
[39] B. Weis and H. G. Zimmer, Artin's Theorie der quadratischen Kongruenzfunktionenkörper und ihre Anwendung auf die Berechnung der Einheiten- und Klassengruppen, Mitt. Math. Ges. Hamburg **XII** (1991), 261-286.
[40] E. Weiss, Algebraic Number Theory, McGraw-Hill Book Co., Inc., New York-San Francisco-Toronto-London, 1963.
[41] H. C. Williams and M. C. Wunderlich, *On the parallel generation of the residues for the continued fraction algorithm*, Math. Comp. **48** (1987), 405–423.
[42] R. J. Zuccherato, *The continued fraction algorithm and regulator for quadratic function fields of characteristic 2*, J. Algebra **190** (1997), 563–587.
[43] R. J. Zuccherato, New applications of elliptic curves and function fields in cryptography, PhD thesis, Department of Combinatorics and Optimization, University of Waterloo, 1997.
[44] R. J. Zuccherato, *The equivalence between elliptic curve and quadratic function field discrete logarithms in characteristic 2*, in: Algorithmic Number Theory Symposium ANTS-III, Lecture Notes in Computer Science **1423**, Springer-Verlag, 1998, 621–638.

A. Stein
Institut für Mathematik
Carl-von-Ossietzky Universität Oldenburg
D-26111 Oldenburg
Germany
E-mail: andreas.stein1@uni-oldenburg.de

Received: 28.2.2008.
Revised: 30.9.2008.