EQUIVALENCES BETWEEN ELLIPTIC CURVES AND REAL QUADRATIC CONGRUENCE FUNCTION FIELDS

Andreas Stein

FB 9-Mathematik
Universität des Saarlandes
Postfach 15 11 50
D-66041 Saarbrücken
Germany
Phone: +49 (681) 302-2046
Fax: +49 (681) 302-4443
Email: andreas@math.uni-sb.de

EQUIVALENCES BETWEEN ELLIPTIC CURVES AND REAL QUADRATIC CONGRUENCE FUNCTION FIELDS

Andreas Stein

Abstract
In [11] Scheidler, Stein and Williams proposed a key exchange protocol which makes use of the set of reduced principal ideals of a real quadratic congruence function field as its underlying structure. The security of the protocol depends on a corresponding discrete logarithm problem (DLP). In this article we show that the DLP for real quadratic congruence function fields of genus one is equivalent to the DLP for elliptic curves over finite fields. We explicitly give the one-to-one correspondence between the set of reduced principal ideals of a real quadratic congruence function field of genus one and the group generated by a point on the corresponding elliptic curve (without the point itself) such that this one-to-one correspondence can be easily computed.

1. Introduction

In [11], it is shown how the theory of real quadratic congruence function fields can be used to produce a secure key distribution protocol. The method is an extension of the recent ideas of Scheidler, Buchmann and Williams [8] who make use of the infrastructure (see Shanks [10]) of the principal ideal class of a real quadratic number field. Both techniques are similar in concept to that of Diffie and Hellman [5] from 1976. Currently, the ElGamal signature scheme is also being extended to real quadratic congruence function fields (see [7]). In [1], Abel shows that the DLP in a real quadratic number field $\mathbb{Q}(\sqrt{\Delta})$ can be solved in time subexponential in $\log \Delta$. Also, any algorithm for solving the DLP can be used to find the regulator of this field. Knowledge of the regulator, together with a technique due to Schoof [9], can then in turn be used to factor Δ. Hence the DLP for real quadratic number fields is at least as difficult as the problem of factoring the integer Δ. A corresponding result in real quadratic congruence

[1]Key words: discrete logarithm, real quadratic congruence function field, continued fractions, infrastructure of reduced principal ideals, elliptic curves

function fields does not guarantee a similarly high level of security, since the factorization of polynomials is easy compared to the factorization of integers. In this article, we prove that the DLP in real quadratic congruence function fields $\mathbb{F}_q(x)(\sqrt{D})$, where $\deg(D) = 4$, is equivalent to the DLP for elliptic curves. So far, the only known algorithm for solving the DLP for elliptic curves is exponential (except for the supersingular case). For real quadratic congruence function fields of large genus, the DLP turned out to be of subexponential complexity (see [6]). The main results are stated in Theorem 12, Theorem 13, and also in Theorem 6, Theorem 7. Mostly, we derive the formulae from Adams and Razar [2] by combining their theorems with theorems about the arithmetic in elliptic congruence function fields (see [15], or [14]). We explicitly give the one-to-one correspondence between the set of reduced principal ideals of an elliptic congruence function field and the group $\langle \mathcal{P} \rangle \setminus \{\mathcal{P}\}$ where $\mathcal{P}$ denotes a $\mathbb{F}_q$-rational point $\mathcal{P}$ on the corresponding elliptic curve. We give answers to the following questions which are important for the equivalence:

- Does the set of reduced principal ideals form a group? (Theorem 7)
- Is there a computable relation between the distance δ_i and the index i? (Theorem 6)
- Is there a relation between the number of reduced principal ideals and the order of $\langle \mathcal{P} \rangle$? (Lemma 9)
- Let $\mathcal{Q} \in \langle \mathcal{P} \rangle \setminus \{\mathcal{P}\}$. Can the corresponding reduced principal ideal be easily computed? Conversely, let $\mathfrak{r}$ be a reduced principal ideal. Can the corresponding point be easily computed? (Theorem 12)

In the following Section, we describe the arithmetic in real quadratic congruence function fields. In Section 3., we state some facts for elliptic congruence function fields. The connection between elliptic curves and real quadratic congruence function fields is drawn in Section 4.. We conclude with the one-to-one correspondence and the equivalences in Section 5..

2. Real Quadratic Congruence Function Fields

In this section, we present the situation as described in [11], [13], [14], and [16]. Basic references for this subject are [3], [4], and [17]. Let $K/\mathbb{F}_q$ be a *real quadratic congruence function field* over a finite field $\mathbb{F}_q$ of *constants* of odd characteristic with q elements. Then $K = \mathbb{F}_q(x)(\sqrt{D}) = \mathbb{F}_q(x) + \mathbb{F}_q(x)\sqrt{D}$, where $D \in \mathbb{F}_q[x]$ is a squarefree polynomial of even degree whose leading coefficient is a square in ${\mathbb{F}_q}^* = \mathbb{F}_q \setminus \{0\}$. (This is in analogy to the case of a real quadratic number field $\mathbb{Q}(\sqrt{\Delta})$, where Δ is a positive, squarefree integer). The *ring of integers of* K is $\mathfrak{O} = \mathbb{F}_q[x][\sqrt{D}] = \mathbb{F}_q[x] + \mathbb{F}_q[x]\sqrt{D}$, and the *unit group* E of $K/\mathbb{F}_q$ is of the form $E = {\mathbb{F}_q}^* \times \langle \epsilon \rangle$, where $\epsilon \in K$ is a *fundamental unit* of K. For $\alpha = u + v\sqrt{D} \in K$ ($u, v \in \mathbb{F}_q(x)$), denote by $\overline{\alpha} = u - v\sqrt{D}$ its *conjugate*. Furthermore, if g denotes the *genus* of K, then $g = \frac{1}{2}\deg(D) - 1$. By choosing a suitable embedding of K into the field $\mathbb{F}_q((1/x))$ of power series in $1/x$, we can represent elements $\alpha \in K$ as Laurent series. If $\alpha = \sum_{i=-\infty}^{m} c_i x^i \in K^*$ with $c_m \neq 0$, we denote the *degree*, the *absolute value*, the *sign* and the *principal part* of α by $\deg(\alpha) = m$,

$|\alpha| = q^m$, $\mathrm{sgn}(\alpha) = c_m$, and $\lfloor \alpha \rfloor = \sum_{i=0}^{m} c_i x^i$, respectively. For negative m we set $\lfloor \alpha \rfloor = 0$. Put $\deg(0) = -\infty$ and $|0| = 0$. $R := \deg(\epsilon)$ is called the *regulator of K/k with respect to $\mathfrak{O}$*.

The continued fraction expansion (*Baby steps*) of an element $\alpha \in K$ is defined recursively by the formulae $\alpha_0 = \alpha$, $a_0 = \lfloor \alpha_0 \rfloor$, $\alpha_{i+1} = 1/(\alpha_i - a_i)$, $a_{i+1} = \lfloor \alpha_{i+1} \rfloor$ for $i \in \mathbb{N}_0$. Sometimes we write $\alpha_i(\beta)$ to express that we develop the continued fraction expansion of $\alpha_0 = \beta$. We say that 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

$$\alpha_\nu = c\alpha_{\nu_0} \ . \tag{2.1}$$

The smallest positive integer $\nu - \nu_0$ for which (2.1) holds is called the *quasi-period* of the continued fraction expansion of α. The expansion of α is called *periodic* if (2.1) holds with $c = 1$. The smallest positive integer $\nu - \nu_0$ for which (2.1) holds with $c = 1$ is called the *period* of the continued fraction expansion of α. It is well-known that, in the periodic case, the quasi-period divides the period, and that they both start at the same index. We easily derive the following

Remark 1 *Let $\alpha \in K$ and $c \in k$. Then, we have that*

$$\alpha_j(c \cdot \alpha) = c^{(-1)^j} \cdot \alpha_j \quad (\, j \in \mathbb{N}_0 \,) \ ,$$

where α_j denote the partial remainders of α.

Let $\alpha \in K$ be an element of the form $\alpha = (P + \sqrt{D})/Q$, where $0 \neq Q, P \in \mathbb{F}_q[x]$ and $Q|(D - P^2)$. Put $Q_0 = Q$, $P_0 = P$, $a_0 = d = \lfloor \sqrt{D} \rfloor$, $Q_{-1} = (D - P^2)/Q$, $r_0 = 0$. We compute Q_i, P_i, a_i, $r_i \in \mathbb{F}_q[x]$ for $i \in \mathbb{N}$ by using the formulae

$$\left\{ \begin{array}{l} P_i = a_{i-1} Q_{i-1} - P_{i-1} = d - r_{i-1} \\ Q_i = (\, D - P_i^2 \,)/Q_{i-1} = Q_{i-2} + a_{i-1} (\, r_{i-1} - r_{i-2} \,) \\ a_i = (\, P_i + d \,) \operatorname{div} Q_i \\ r_i = (\, P_i + d \,) \bmod Q_i \end{array} \right\} \tag{2.2}$$

and find that $\alpha_i = (P_i + \sqrt{D})/Q_i$, where $Q_i|(D - P_i^2)$. We notice that $\deg(r_i) < \deg(Q_i)$ for $i \geq 0$. If we define $\theta_1 = 1$ and

$$\theta_i = \prod_{j=1}^{i-1} \frac{1}{\alpha_j} \quad (\, i \geq 2 \,) \ , \tag{2.3}$$

then we get

$$\theta_i \, \overline{\theta}_i = (-1)^{i-1} \, Q_{i-1}/Q_0 \qquad (\, i \in \mathbb{N} \,) \ . \tag{2.4}$$

Remark 2 *The continued fraction expansion of $\alpha = \sqrt{D}$ is periodic with period n and quasi-periodic with quasi-period m. We know that $Q_s \in k^*$ if and only if $s = \lambda m$ ($s, \lambda \in \mathbb{N}_0$). Furthermore, $\epsilon = \overline{\theta}_{m+1}$ is a fundamental unit of K, and the regulator R of K/k with respect to $\mathfrak{O}$ satisfies $R = \deg(\overline{\theta}_{m+1})$.*

A subset $\mathfrak{a}$ of $\mathfrak{O}$ is an *(integral) ideal* if both $\mathfrak{a}+\mathfrak{a}$ and $\mathfrak{O} \cdot \mathfrak{a}$ are subsets of $\mathfrak{a}$. If $\mathfrak{a}$ is generated by a single element $\beta \in K$, i.e. $\mathfrak{a} = (\beta) = \beta\mathfrak{O}$, we call $\mathfrak{a}$ a *principal $\mathfrak{O}$-ideal*. We will only

be considering principal (integral) ideals. For $\beta, \gamma \in \mathfrak{O}$, we denote by $[\beta, \gamma]$ the module $\beta\mathbb{F}_q[x] + \gamma\mathbb{F}_q[x]$. Let $\mathfrak{a}$ be an (integral) ideal. Then there exist polynomials S, P, $Q \in \mathbb{F}_q[x]$ with $Q|(D - P^2)$ such that

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

The set $\{\, S\,Q,\ S\,P + S\sqrt{D}\,\}$ is called $\mathbb{F}_q[x]$-¡*base* of $\mathfrak{a}$. If we set $\mathrm{sgn}(S) = \mathrm{sgn}(Q) = 1$, then S and Q are unique. $\mathfrak{a}$ is called *primitive* if S can be chosen to be 1. Each ideal $\mathfrak{a}$ has an *adapted* $\mathbb{F}_q[x]$-*base*, meaning that there exists a $\mathbb{F}_q[x]$-base $\{\, S\,Q,\ S\,P + S\sqrt{D}\,\}$ with $\deg(P) < \deg(Q)$. A primitive ideal $\mathfrak{a}$ is called *reduced*, if there exists for $\mathfrak{a}$ an $\mathbb{F}_q[x]$-base of the form $\{\, Q,\ P + \sqrt{D}\,\}$ such that $|P - \sqrt{D}\,| < |Q| < |P + \sqrt{D}\,|$. If we let $\mathrm{sgn}(Q) = 1$, then this *reduced base* representation is unique.

Let $\mathfrak{a}_1 = \left[Q, P + \sqrt{D}\right]$ be a primitive ideal. Then the continued fraction expansion of $\alpha = (P + \sqrt{D})/Q$ yields a sequence of primitive ideals $\mathfrak{a}_i = [Q_{i-1}, P_{i-1} + \sqrt{D}]$ $(i \in \mathbb{N})$ with the quantities defined in (2.2). We have that $Q_0\theta_i$, $Q_0\overline{\theta}_i \in \mathfrak{O}$ and that

$$(\,Q_0\theta_i\,)\ \mathfrak{a}_i\ =\ (\,Q_{i-1}\,)\ \mathfrak{a}_1. \tag{2.5}$$

Properties of reduced ideals are summarized in the following Lemma (see [14] or [11]):

Lemma 3 *Let* $\mathfrak{a}_1 = \left[Q,\ P + \sqrt{D}\right]$ *be a primitive ideal. In the above notation, the following properties hold.*

a) $\mathfrak{a}_1$ *is reduced if and only if* $|Q| < |\sqrt{D}\,|$.

b) $\mathfrak{a}_i$ *is reduced for* $i > \max\left\{1,\ \frac{1}{2}\deg(Q) - \frac{1}{4}\deg(D) + 2\right\}$.

c) If $\mathfrak{a}_j$ *is reduced for some* $j \in \mathbb{N}$, *then* $\mathfrak{a}_i$ *is reduced for all* $i \geq j$, *and a reduced* $\mathbb{F}_q[x]$-*base for* $\mathfrak{a}_i$ *is given by* $\{\, Q_{i-1},\ P_{i-1} + \sqrt{D}\,\}$.

d) If $\mathfrak{a}_j$ *is reduced and* $\{\, Q_{j-1},\ P_{j-1} + \sqrt{D}\,\}$ *its reduced* $\mathbb{F}_q[x]$-*base, we have* $|P_{j-1}| = |\sqrt{D}|$, $1 \leq |Q_{j-1}| < |\sqrt{D}\,|$ *and* $sgn(\,P_{j-1}\,) = sgn(\,\sqrt{D}\,)$. *Even the two highest coefficients of* P_{j-1} *and* $\sqrt{D}$ *are equal. Furthermore, we get* $1 < |a_{j-1}| \leq |\sqrt{D}\,|$ *and* $|a_{j-1}Q_{j-1}| = |\sqrt{D}\,|$

e) If $\mathfrak{b}$ *is reduced and equivalent to* $\mathfrak{a}_1$, *then* $\mathfrak{b} = \mathfrak{a}_j$ *for a* $j \in \mathbb{N}$.

If we set $\mathfrak{r}_1 = \mathfrak{O} = [\,1,\ \sqrt{D}\,]$, then $\mathfrak{r}_1$ is reduced by Lemma 3 a). By developing the continued fraction expansion of $\alpha = \sqrt{D}$ with the formulae in (2.2), we obtain a sequence of reduced principal ideals $(\mathfrak{r}_i)_{i\in\mathbb{N}}$. This sequence is periodic, i.e. $\mathfrak{r}_{m+i} = \mathfrak{r}_i$ $(i \geq 1)$, where m denotes the quasi-period of $\alpha = \sqrt{D}$ (see [14].

It follows from Lemma 3 e) that the sequence $(\mathfrak{r}_i)_{i\in\mathbb{N}}$ contains all reduced principal ideals. By (2.5), we get $\mathfrak{r}_i = (\,\overline{\theta}_i\,)$ for $i \in \mathbb{N}$. The *distance* of $\mathfrak{r}_i$ is defined to be $\delta_i = \delta(\mathfrak{r}_i) = \deg(\,\overline{\theta}_i\,)$. Note that the distance δ_i is an integer-valued function which is only defined for reduced ideals and strictly increases as i increases. By Remark 2, we get for the regulator: $R = \delta_{m+1}$.

We know from [14], or [11], that there is an operation $*$ (multiply and reduce), which we also call *Giant step*, on the set of reduced principal ideals under which this set is closed. Let i, j be arbitrary, positive integers. We then have $\mathfrak{r}_i * \mathfrak{r}_j = \mathfrak{r}_k$, and

$$\delta_k \;=\; \delta_i \;+\; \delta_j \;+\; f \;, \tag{2.6}$$

where $2 - \deg(D) \leq f \leq 0$. Also, we know that $k \approx i + j$. As in [11], we define

Definition 4 *The discrete logarithm problem* (DLP) *for real quadratic congruence function fields is given as follows: for any reduced principal ideal* $\mathfrak{r}$, *find* $\delta(\mathfrak{r})$, $0 \leq \delta(\mathfrak{r}) < R$.

3. Elliptic Congruence Function Fields

Let $K = \mathbb{F}_q(x)(\sqrt{D})$, where $\deg(D) = 4$, i.e. $g = 1$, and $\mathrm{sgn}(D)$ is a square in $\mathbb{F}_q{}^*$. These fields are called *elliptic congruence function fields*. Let m be the quasi-period of the continued fraction expansion of $\alpha = \sqrt{D}$. Then, by Lemma 3 d) and Remark 2, we derive:

Proposition 5 *Let* $(\mathfrak{r}_i)_{i\in\mathbb{N}}$ *be the sequence of reduced principal ideals starting at* $\mathfrak{r}_1 = [\,1,\, \sqrt{D}\,]$. *Then, we have for the adapted base of* $\mathfrak{r}_i$*:*

$$\mathfrak{r}_i \;=\; \begin{cases} [\,1,\, \sqrt{D}\,] = \mathfrak{r}_1 = \mathfrak{O} & ,\quad \textit{if} \quad i-1 \text{ divides } m \\ [\,x \,+\, e_{i-1},\, f_{i-1} + \sqrt{D}\,] & ,\quad \text{otherwise} \end{cases} \;,$$

where $e_{i-1},\, f_{i-1} \in \mathbb{F}_q$.

From the following theorem, we can conclude that the distance is equal to the index in one round of the continued fraction expansion of $\alpha = \sqrt{D}$.

Theorem 6 *In the continued fraction expansion of* $\alpha = \sqrt{D}$, *we have for the distance* $\delta_i = \delta(\mathfrak{r}_i)$ *of a reduced principal ideal* $\mathfrak{r}_i$ *that*

$$\delta_i \;=\; i \quad (2 \;\leq i \leq m+1\,)\;.$$

This means, that $R = \delta_{m+1} = m + 1$. Next, we point out that the set of reduced principal ideals is "almost" a group under the Giant step operation $*$, but it still fails to be a group.

Theorem 7 *In the continued fraction expansion of* $\alpha = \sqrt{D}$, *let* $i,\, j \in \mathbb{N}$ *be such that* $1 \leq i,\, j \leq m$. *Then,*

$$\mathfrak{r}_i * \mathfrak{r}_j \;=\; \begin{cases} \mathfrak{r}_{i+j} & ,\quad \textit{if} \quad i+j \leq m+1 \\ \mathfrak{r}_{i+j-1} & ,\quad \textit{if} \quad i+j \geq m+2 \end{cases}$$

and

$$\delta(\mathfrak{r}_i * \mathfrak{r}_j) \;=\; \begin{cases} \delta_i + \delta_j - 1 & ,\quad \textit{if} \quad i+j = m+2 \\ \delta_i + \delta_j & ,\quad \textit{otherwise} \end{cases}$$

The full proofs of Theorem 6 and Theorem 7 can be found in [15].

4. The Quartic Model of an Elliptic Curve

We follow the notation of [2]. Let E be a non-singular elliptic curve over the finite field $k = \mathbb{F}_q$ of odd characteristic. We will assume E to be given in *short Weierstrass normal form*

$$E : \; w^2 \; = \; v^3 \; + \; Av \; + \; B \quad (A, \, B \; \in \mathbb{F}_q \;) \; , \tag{4.1}$$

where $\Delta = -4A^3 - 27B^2 \neq 0$. We consider the additive *group of all* $\mathbb{F}_q$*-rational points on* E

$$E(k) := \{ \, (v, w) \in k^2 \, | \, w^2 \; = \; v^3 \; + \; Av \; + \; B \, \} \cup \{ \mathcal{O} \}$$

with the *point at infinity*

$$\mathcal{O} \; = \; (\infty, \infty)$$

as the identity with respect to the usual group law on E. Let $K = \mathbb{F}_q(v, w)$. Let $\mathcal{P} = (a, b) \neq \mathcal{O}$ be any $\mathbb{F}_q$-rational point on E, i.e. $\mathcal{P} \in E(\mathbb{F}_q) \setminus \{\mathcal{O}\}$. We define

$$x \; := \; \frac{w + b}{v - a} \quad , \quad y \; := \; 2\,v \; + \; a \; - \left(\frac{w + b}{v - a} \right)^2 \; = \; 2\,v \; + \; a \; - \; x^2 \; , \tag{4.2}$$

and let $c := -4A - 3a^2$. Thus the curve

$$E_{\mathcal{P}} : \; y^2 \; = \; x^4 \; - \; 6ax^2 \; - \; 8bx \; + \; c =: \; D \tag{4.3}$$

is a plane quartic model for E with two points $\mathcal{O}$ and $\mathcal{P}$ at infinity. $D = D_{\mathcal{P}} \in \mathbb{F}_q[x]$ is a monic squarefree polynomial of degree 4, and $K = \mathbb{F}_q(x)(y) = \mathbb{F}_q(x)(\sqrt{D})$ is a real quadratic congruence function field of genus 1 with respect to $\mathfrak{O} = \mathfrak{O}_{\mathcal{P}} = \mathbb{F}_q[x][\sqrt{D}]$.

Conversely, let $K = \mathbb{F}_q(x)(\sqrt{D})$ be a real quadratic congruence function field of genus 1. Then D is a squarefree polynomial of degree 4 where $\mathrm{sgn}(D)$ is a square in $\mathbb{F}_q{}^*$. Without loss of generality, we assume D to be of the form in (4.3), i.e.

$$D \; = \; x^4 \; - \; 6ax^2 \; - \; 8bx \; + \; c \quad (\, a, \, b, \, c \in k \,) \; .$$

Otherwise, we use linear transformations to obtain $D' \in \mathbb{F}_q[x]$ such that D' has the desired form, under which the ring of integers does not change. We define

$$v \; := \tfrac{1}{2}(\, x^2 \; + \; y \; - \; a \,) \quad , \quad w \; := \tfrac{1}{2}(\, x^3 \; + \; xy \; - \; 3ax \; - 2b \,) \; , \tag{4.4}$$

and $A := -\frac{1}{4}c - \frac{3}{4}a^2$, $B := b^2 - a^3 - Aa$. These formulas yield an elliptic curve E such that E is given by the equation in (4.1) and a k-rational point $\mathcal{P} := (a, b) \in E(\mathbb{F}_q) \setminus \{\mathcal{O}\}$ on E. This means that (4.2) and (4.4) provide a birational equivalence between E and $E_{\mathcal{P}}$. Again, the function fields are equal, i.e. $K = \mathbb{F}_q(x)(\sqrt{D}) = \mathbb{F}_q(v, w)$.

If $\mathcal{Q} \neq \mathcal{O}, \mathcal{P}$ is a point on E, then we also denote the equivalent point on $E_{\mathcal{P}}$ by $\mathcal{Q}$. To distinguish between the two curves, we write for the coordinates $\mathcal{Q} = (v_{\mathcal{Q}}, w_{\mathcal{Q}})$, $\mathcal{Q} = (x_{\mathcal{Q}}, y_{\mathcal{Q}})$, if $\mathcal{Q}$ lies on E or $E_{\mathcal{P}}$, respectively. We also let $x_{\mathcal{Q}}$ be the value $x(\mathcal{Q})$ under the transformation (4.2) and $v_{\mathcal{Q}}$ be the value $v(\mathcal{Q})$ under the transformation (4.4). The conjugation in $K = \mathbb{F}_q(x)(y)$ yields a bi-regular $\mathbb{F}_q$-morphism of $E_{\mathcal{P}}(k)$, given by $\mathcal{Q} = (x_{\mathcal{Q}}, y_{\mathcal{Q}}) \mapsto \overline{\mathcal{Q}} = (x_{\mathcal{Q}}, -y_{\mathcal{Q}})$

for $\mathcal{Q} \neq \mathcal{O}$, $\mathcal{P}$, and $\overline{\mathcal{O}} = \mathcal{P}$, $\overline{\mathcal{P}} = \mathcal{O}$. The *discrete logarithm problem* (DLP) for elliptic curves over finite fields is defined as follows: given an elliptic curve E over a finite field k, and two k-rational points $\mathcal{Q}$ and $\mathcal{P}$ on E such that $\mathcal{Q} = l \cdot \mathcal{P}$ ($l \in \mathbb{N}$), find the integer l.

We now require the additional condition that the order of $\mathcal{P} = (a, b)$ is different from 2, i.e. $b \neq 0$. Furthermore, we assume $\mathcal{Q}$ to be a $\mathbb{F}_q$-rational point on E such that $\mathcal{Q} \neq \mathcal{P}$. As in [2], we define:

Definition 8 *Let $\mathcal{Q} \in E(\mathbb{F}_q)$ be such that $\mathcal{Q} \neq \mathcal{P}$. We set*

$$f_{\mathcal{Q}} := \begin{cases} \dfrac{v - v(\overline{\mathcal{Q}})}{x - x_{\mathcal{Q}}} & , \text{ if } \mathcal{Q} \neq \mathcal{O} \\ v - v(\overline{\mathcal{Q}}) & , \text{ if } \mathcal{Q} = \mathcal{O} \end{cases} .$$

By (4.4) and the definition of $\overline{\mathcal{Q}}$, we get for $\mathcal{Q} \neq \mathcal{O}$ that

$$f_{\mathcal{Q}} = \frac{x^2 - x_{\mathcal{Q}}^2 + y_{\mathcal{Q}} + \sqrt{D}}{2(x - x_{\mathcal{Q}})} , \tag{4.5}$$

and

$$f_{\mathcal{O}} = \tfrac{1}{2}\left(x^2 - 3a + \sqrt{D}\right) . \tag{4.6}$$

Since $k = \mathbb{F}_q$ is a finite field, we know that the continued fraction expansion of $f_{\mathcal{Q}}$ ($\mathcal{Q} \neq \mathcal{P}$) with respect to $\mathfrak{O} = \mathfrak{O}_{\mathcal{P}} = \mathbb{F}_q[x][\sqrt{D}]$ is periodic and quasi-periodic.

We develop the continued fraction expansion of $\sqrt{D}$, and obtain a sequence $\alpha_0 = \sqrt{D}$, α_1, α_2, ..., where, by (2.2), $\alpha_{i-1} = (P_{i-1} + \sqrt{D})/Q_{i-1}$ ($i \geq 2$) with $P_{i-1}, Q_{i-1} \in \mathbb{F}_q[x]$. The continued fraction expansion of $\sqrt{D}$ is periodic and quasi-periodic with quasi-period $m = m_{\mathcal{P}}$. As in Section 2., we compute the sequence of reduced principal ideals $(\mathfrak{r}_i)_{i \in \mathbb{N}}$, starting at $\mathfrak{r}_1 = \mathfrak{O} = [\,1, \sqrt{D}\,]$. This sequence is periodic with period m, i.e. $\mathfrak{r}_{m+i} = \mathfrak{r}_i$ ($i \geq 1$), and we have $\mathfrak{r}_i = [\,Q_{i-1}, P_{i-1} + \sqrt{D}\,]$.

Lemma 9 *Let E be a non-singular elliptic curve over a finite field $k = \mathbb{F}_q$, and let $\mathcal{P} \in E(\mathbb{F}_q)$ be such that $\mathcal{P} \neq \mathcal{O}$, and let $ord(\mathcal{P}) \neq 2$. Then the continued fraction expansion of $f_{\mathcal{O}}$ is pure quasi-periodic. Moreover,*

$$ord(\mathcal{P}) = m + 1 = R ,$$

where $m = m_{\mathcal{P}}$ is the quasi-period of $\sqrt{D}$, and $R = R_{\mathcal{P}}$ denotes the regulator of the field $k(x)(\sqrt{D})$ with respect to $\mathfrak{O} = \mathbb{F}_q[x][\sqrt{D}]$.

Proof: see Theorem 4.2 of [2]. ∎

This means that we have a connection between the order of the subgroup of $E(\mathbb{F}_q)$ generated by $\mathcal{P}$, i.e. $\#\langle P \rangle = m+1$, and the number of reduced principal ideals of $\mathfrak{O}$, i.e. $\#\{\mathfrak{r}_1, \ldots, \mathfrak{r}_m\} = m$. The question is whether there is a correspondence between $i\,\mathcal{P}$ and $\mathfrak{r}_i$ for each $i \in \mathbb{N}_0$. We will see that the answer to this question is more important for the equivalences between DLPs (see section 5.) than Lemma 9.

Remark 10 *As an application of the above Lemma, we show a method how to produce points of large order.*

a) Given appropriate series of real quadratic number fields with large fundamental unit (Williams, Shanks, Yamamoto, Halter-Koch).

b) Find analogue series of elliptic congruence function fields with large regulators.

c) Use the birational transformations (4.4) to compute elliptic curves and $\mathbb{F}_q$-rational points of large orders.

Here, we can make use of the criterion of Zhang [18] to ensure that the ideal class number h' is odd (see also [11]), i.e. that $\#E(\mathbb{F}_q)/ord(\mathcal{P})$ is odd. Furthermore, this method can be generalized to hyperelliptic curves.

5. Equivalences

First, we need an important relation between α_i and $f_{i\mathcal{P}}$ which is proven in [2]. Here, $f_{i\mathcal{P}}$ denotes the function $f_{\mathcal{Q}}$ for $\mathcal{Q} = i\,\mathcal{P}$. Remember that $\mathrm{ord}(\mathcal{P}) \neq 2$, and that $f_{i\mathcal{P}}$ is only defined for $i \neq 1$.

Lemma 11 *In the continued fraction expansions of $\alpha_0 = \sqrt{D}$, we have that*

$$f_{i\mathcal{P}} = c_i \cdot \alpha_{i-1} \quad (2 \leq i \leq m,\, c_i \in \mathbb{F}_q{}^*) \ .$$

Proof: See Corollary 3.6 of [2]. ∎

We denote by (x_i, y_i) the point $i\,\mathcal{P} =$ on $E_{\mathcal{P}}$ for $2 \leq i \leq m$. From Lemma 11, we know that $f_{i\mathcal{P}} = c_i \cdot \alpha_{i-1}$ with $c_i \in \mathbb{F}_q{}^*$. By (4.5) and (2.2), this relation is equivalent to

$$\frac{x^2 - x_i^2 + y_i + \sqrt{D}}{2\,(x - x_i)} = c_i \cdot \frac{(P_{i-1} + \sqrt{D})}{Q_{i-1}} \ ,$$

where $P_{i-1}, Q_{i-1} \in \mathbb{F}_q[x]$ and $\mathfrak{r}_i = [\,Q_{i-1},\, P_{i-1} + \sqrt{D}\,]$. Comparing rational and irrational part leads to

$$P_{i-1} = x^2 - x_i^2 + y_i \quad , \quad Q_{i-1} = 2\,c_i\,(x - x_i) \ .$$

Thus,

$$\mathfrak{r}_i = [\,x - x_i\,,\, x^2 - x_i^2 + y_i + \sqrt{D}\,] = [\,x - x_i\,,\, y_i + \sqrt{D}\,] \ .$$

For $i = m+1$, we have $i\,\mathcal{P} = \mathcal{O}$, $f_{i\mathcal{P}} = f_{\mathcal{O}}$, and $\mathfrak{r}_{m+1} = \mathfrak{r}_1 = [\,1,\, \sqrt{D}\,]$. We summarize this in the following

Theorem 12 *Let E be a non-singular elliptic curve over a finite field $\mathbb{F}_q$, and let $\mathcal{P} \in E(\mathbb{F}_q)$ be such that $\mathcal{P} \neq \mathcal{O}$, and $\mathrm{ord}(\mathcal{P}) \neq 2$. Then, there is a one-to-one correspondence between the sets $\{\mathcal{O}, 2\,\mathcal{P}, 3\,\mathcal{P}, \ldots, m\,\mathcal{P}\} = \langle \mathcal{P} \rangle \setminus \{\mathcal{P}\}$ and $\{\mathfrak{r}_1, \ldots, \mathfrak{r}_m\}$ as follows: Let $\mathcal{Q} \in \{\mathcal{O}, 2\,\mathcal{P}, 3\,\mathcal{P}, \ldots, m\,\mathcal{P}\}$. Then, $\mathcal{Q} = l\,\mathcal{P}$ for a l such that $2 \leq l \leq m$, or $\mathcal{Q} = \mathcal{O}$.*

$$\mathcal{Q} = l\,\mathcal{P} \longmapsto \mathfrak{r}_{\mathcal{Q}} = \mathfrak{r}_l = \begin{cases} [\,1, \sqrt{D}\,] & , \text{ if } \mathcal{Q} = \mathcal{O} \\ [\,x - x_{\mathcal{Q}}, y_{\mathcal{Q}} + \sqrt{D}\,] & , \text{ if } \mathcal{Q} = (\,x_{\mathcal{Q}}, y_{\mathcal{Q}}\,) \neq \mathcal{O} \end{cases} .$$

where $x_{\mathcal{Q}}$ and $y_{\mathcal{Q}}$ denote the coordinates of $\mathcal{Q}$ on $E_{\mathcal{P}}$. Conversely, let $\mathfrak{r} \in \{\mathfrak{r}_1, \ldots, \mathfrak{r}_m\}$. Then, $\mathfrak{r} = \mathfrak{r}_l$ for a l such that $1 \leq l \leq m$. Let $\mathfrak{r}$ be given in adapted form with respect to Proposition 5.

$$\mathfrak{r} = \mathfrak{r}_l \longmapsto \mathcal{Q} = l\,\mathcal{P} = \begin{cases} \mathcal{O} & , \text{ if } \mathfrak{r} = [\,1, \sqrt{D}\,] \\ (\,-e\,, f\,) & , \text{ if } \mathfrak{r} = [\,x + e\,, f + \sqrt{D}\,] \neq [\,1, \sqrt{D}\,] \end{cases} ,$$

where $e, f \in \mathbb{F}_q$, and $(-e, f)$ denotes the point $\mathcal{Q}$ on $E_{\mathcal{P}}$.

We illustrate the meaning of Theorem 12. For $i = 2, \ldots, m$, we denote the point $i\,\mathcal{P}$ on E, $E_{\mathcal{P}}$, respectively, by (v_i, w_i), (x_i, y_i).

$$\begin{array}{rcccccl}
 & & \mathcal{O} & \cong & \mathcal{O} & \longleftrightarrow & \mathfrak{r}_1 = [\,1, \sqrt{D}\,] \\
2\,\mathcal{P} & = & (v_2, w_2) & \cong & (x_2, y_2) & \longleftrightarrow & \mathfrak{r}_2 = [\,x - x_2, y_2 + \sqrt{D}\,] \\
3\,\mathcal{P} & = & (v_3, w_3) & \cong & (x_3, y_3) & \longleftrightarrow & \mathfrak{r}_3 = [\,x - x_3, y_3 + \sqrt{D}\,] \\
\vdots & & \vdots & & \vdots & & \vdots \\
l\,\mathcal{P} & = & (v_l, w_l) & \cong & (x_l, y_l) & \longleftrightarrow & \mathfrak{r}_l = [\,x - x_l, y_l + \sqrt{D}\,] \\
\vdots & & \vdots & & \vdots & & \vdots \\
m\,\mathcal{P} & = & (v_m, w_m) & \cong & (x_m, y_m) & \longleftrightarrow & \mathfrak{r}_m = [\,x - x_m, y_m + \sqrt{D}\,]
\end{array}$$

Theorem 13 *The discrete logarithm problem for real quadratic congruence function fields of genus 1 can be solved in polynomial time if and only if the discrete logarithm problem for (non-singular) elliptic curves can be solved in polynomial time.*

Proof: Here, we use Theorem 12 and Theorem 6. First, we assume that we can solve the DLP for real quadratic congruence function fields of genus 1 in polynomial time. Let E be an elliptic curve over a finite field $k = \mathbb{F}_q$ given, as in (4.1), in short Weierstrass normal form

$$E : w^2 = v^3 + Av + B \quad (A, B \in \mathbb{F}_q\,) ,$$

where $\Delta = -4A^3 - 27B^2 \neq 0$. Let $\mathcal{P} = (a, b) \in E(\mathbb{F}_q)$ be such that $\mathcal{P} \neq \mathcal{O}$. The case that $\mathcal{P}$ has order 2, is trivial. Therefore, let $\mathrm{ord}(\mathcal{P}) \neq 2$. Under the birational transformation (4.2), we obtain the curve

$$E_{\mathcal{P}} : y^2 = x^4 - 6ax^2 - 8bx + c =: D .$$

E and $E_{\mathcal{P}}$ are birationally equivalent, and the field $\mathbb{F}_q(x)(\sqrt{D})$ is a real quadratic congruence function field of genus 1 with respect to $\mathfrak{O} = \mathbb{F}_q[x][\sqrt{D}]$. Let m be the quasi-period of the continued fraction expansion of $\sqrt{D}$, and let R be the regulator of $\mathbb{F}_q(x)(\sqrt{D})$ with respect to $\mathfrak{O}$. Denote by $\{\mathfrak{r}_1, \ldots, \mathfrak{r}_m\}$ the set of reduced principal $\mathfrak{O}$-ideals starting at $\mathfrak{r}_1 = [\,1, \sqrt{D}\,]$.

Let $\mathcal{Q} \in E(\mathbb{F}_q)$ such that $\mathcal{Q} = l \cdot \mathcal{P}$, where $l \in \mathbb{N}$, $2 \leq l \leq \mathrm{ord}(\mathcal{P})$. By Lemma 9, we know that $\mathrm{ord}(\mathcal{P}) = m + 1 = R$. If $l = m + 1 = R$, then $\mathcal{Q} = \mathcal{O}$, and, by Theorem 12, this means that the corresponding reduced principal ideal is $\mathfrak{r}_{\mathcal{O}} = [\,1, \sqrt{D}\,] = \mathfrak{r}_1$. Thus, by assumption, the computation of $l = R$ can be done in polynomial time, since $\mathfrak{r}_1 = \mathfrak{r}_{m+1}$ and $R = \delta(\mathfrak{r}_{m+1})$. Now, let $\mathcal{Q} \neq \mathcal{O}, \mathcal{P}$, i.e. $2 \leq l \leq m$. Our aim is to compute l in polynomial time. We see from Theorem 12 that $\mathcal{Q}$ corresponds to the reduced principal ideal $\mathfrak{r}_{\mathcal{Q}} = [\,x - x_{\mathcal{Q}},\, y_{\mathcal{Q}} + \sqrt{D}\,]$, where $\mathfrak{r}_{\mathcal{Q}} = \mathfrak{r}_l$, and $x_{\mathcal{Q}}$ and $y_{\mathcal{Q}}$ denote the coordinates of $\mathcal{Q}$ on $E_{\mathcal{P}}$. By 4.2, $\mathfrak{r}_{\mathcal{Q}}$ can be computed from $\mathcal{Q}$ in polynomial time. From Theorem 6, we have $l = \delta_l = \delta(\mathfrak{r}_{\mathcal{Q}})$. Thus, by assumption, l can be computed in polynomial time.

We now assume that the discrete logarithm problem for (non-singular) elliptic curves can be solved in polynomial time. Let $K = \mathbb{F}_q(x)(\sqrt{D})$ be a real quadratic congruence function field of genus 1, where D is a squarefree polynomial of degree 4, and $\mathfrak{O} = \mathbb{F}_q[x][\sqrt{D}]$. Without loss of generality (see section 4.), we assume D to be of the form

$$D = x^4 - 6ax^2 - 8bx + c \quad (\,a,\, b,\, c \in \mathbb{F}_q\,)\ .$$

Let $E_{\mathcal{P}}$ be the curve given by

$$E_{\mathcal{P}} :\ y^2 = D\ .$$

The birational transformation in 4.4 yields a non-singular elliptic curve E in short Weierstrass normal form

$$E :\ w^2 = v^3 + Av + B\ ,$$

and a point $\mathcal{P} := (a, b) \in E(\mathbb{F}_q) \setminus \{\mathcal{O}\}$, such that E and $E_{\mathcal{P}}$ are birationally equivalent. Let m be the quasi-period of the continued fraction expansion of $\sqrt{D}$, and let R be the regulator of $\mathbb{F}_q(x)(\sqrt{D})$ with respect to $\mathfrak{O}$. Let $R = \mathrm{ord}(\mathcal{P}) \neq 2$ (the case $R = 2$, i.e. $m = 1$, is trivial). Denote by $\{\mathfrak{r}_1, \ldots, \mathfrak{r}_m\}$ the set of reduced principal $\mathfrak{O}$-ideals starting at $\mathfrak{r}_1 = [\,1, \sqrt{D}\,]$.

Let $\mathfrak{r}$ be a reduced principal $\mathfrak{O}$-ideal, i.e. $\mathfrak{r} \in \{\mathfrak{r}_1, \ldots, \mathfrak{r}_m\}$. If $\mathfrak{r} = [\,1, \sqrt{D}\,] = \mathfrak{r}_1$, then $\mathfrak{r}_1 = \mathfrak{r}_{m+1}$, and, by Lemma 9, $\delta(\mathfrak{r}) = \delta(\mathfrak{r}_{m+1}) = R = ord(\mathcal{P})$. Thus, by assumption, the computation of $\delta(\mathfrak{r})$ can be done in polynomial time.

Now, let $\mathfrak{r} = \mathfrak{r}_l$ such that $2 \leq l \leq m$. Our aim is to compute $\delta(\mathfrak{r})$ in polynomial time. We compute the adapted $\mathbb{F}_q[x]$-base of $\mathfrak{r}$ in polynomial time (see [14]), and obtain $\mathfrak{r} = [\,x + e,\, f + \sqrt{D}\,]$, where $e,\, f \in \mathbb{F}_q$. From Theorem 12, we conclude that $\mathfrak{r}$ corresponds to the point $\mathcal{Q} = (-e,\, f)$ on $E_{\mathcal{P}}$. By (4.4), the coordinates of $\mathcal{Q}$ on E can be computed in polynomial time. Furthermore, we know that $\mathcal{Q} = l\,\mathcal{P}$. From Theorem 6, we get $l = \delta_l$. Thus, by assumption, $\delta(\mathfrak{r}) = \delta(\mathfrak{r}_l) = l$ can be computed in polynomial time. ∎

We state the equivalence in terms of polynomial time algorithms, but the proof of Theorem 13 shows that only the transformations and the computation of the adapted base contribute to the equivalence. In fact, any fast method for solving one of the discrete logarithm problems gives rise to a fast solution of the other one.

References

[1] ABEL, C. S., Ein Algorithmus zur Berechnung der Klassenzahl und des Regulators reellquadratischer Ordnungen. Dissertation, Universität des Saarlandes, Saarbrücken (Germany) 1994.

[2] ADAMS, W. W., RAZAR, M. J., Multiples of Points on Elliptic Curves and Continued Fractions. Proc. London Math. Soc. **41**, 1980, 481-498.

[3] ARTIN, E., Quadratische Körper im Gebiete der höheren Kongruenzen I, II. Math. Zeitschr. **19**,1924, 153-206.

[4] DEURING, M.,, Lectures on the Theory of Algebraic Functions of One Variable. LNM **314**, Berlin 1973.

[5] DIFFIE, W., HELLMAN, M. E., New Directions in Cryptography. IEEE Trans. Inform. Theory **22**, no. 6, 1976, 644-654.

[6] MÜLLER, V., STEIN A., THIEL, C., Computing Discrete Logarithms in Real Quadratic Congruence Function Fields of Large Genus. Submitted Manuscript.

[7] SCHEIDLER, R., Cryptography in Real Quadratic Congruence Function Fields, To appear in Proceedings of Pragocrypt'96.

[8] SCHEIDLER, R., BUCHMANN, J. A., WILLIAMS, H. C., A Key Exchange Protocol Using Real Quadratic Fields. J. Cryptology **7**, 1994, 171-199.

[9] SCHOOF, R. J., Quadratic Fields and Factorization. in: Lenstra, H. W., Tijdemans, R., Computational Methods in Number Theory, Math. Centrum Tracts **155**, Part II, Amsterdam 1983.

[10] SHANKS, D., The Infrastructure of a Real Quadratic Field and its Applications. Proc. 1972 Number Theory Conf., Boulder, Colorado, 1972, 217-224.

[11] SCHEIDLER, R., STEIN, A., WILLIAMS, H. C., Key-exchange in Real Quadratic Congruence Function Fields. Designs, Codes and Cryptography **7**, no. 1/2, 1996, 153-174.

[12] SILVERMAN, J. H., The Arithmetic of Elliptic Curves. Springer, New York 1986.

[13] STEIN, A., ZIMMER, H. G., An Algorithm for Determining the Regulator and the Fundamental Unit of a Hyperelliptic Congruence Function Field. Proc. 1991 Int. Symp. on Symbolic and Algebraic Computation, Bonn (Germany), July 15-17, ACM Press, 183-184.

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

[15] STEIN, A., Elliptic Congruence Function Fields. To appear in Proceedings of ANTS II.

[16] WEIS, B., ZIMMER, H. G., Artin's Theorie der quadratischen Kongruenzfunktionenkörper und ihre Anwendung auf die Berechnung der Einheiten- und Klassengruppen. Mitt. Math. Ges. Hamburg, Sond. **XII**, no. 2, 1991.

[17] WEISS, E., Algebraic Number Theory. McGraw-Hill, New York 1963.

[18] ZHANG, X., Ambiguous Classes and 2-rank of Class Groups of Quadratic Function Fields. J. of China University of Science and Technology **17**, no. 4, 1987, 425-431.