Journal de Théorie des Nombres
de Bordeaux ***9*** *(1997), 75–95*

Equivalences Between Elliptic Curves and Real Quadratic Congruence Function Fields

par Andreas STEIN

Résumé. En 1994, le célèbre protocole d'échange de clefs de Diffie-Hellman fut pour la première fois implémenté dans un cas où l'espace des clefs sous-jacent n'a pas une structure de groupe : en effet l'ensemble des idéaux réduits principaux d'un corps de nombres quadratique réel n'est pas un groupe, mais néanmoins possède ce qu'on appelle une infrastructure. Récemment, ce principe a été étendu au cas des corps quadratiques réels de fonctions sur un corps fini. Comme toujours, la sécurité du protocole dépend d'un certain problème de logarithme discret (PLD). Dans cet article, nous démontrons que pour les corps quadratiques réels de fonctions sur un corps fini et de genre un, i.e les corps de fonctions elliptiques sur un corps fini, ce PLD est équivalent au PLD pour les courbes elliptiques définies sur un corps fini . Nous explicitons ici la correspondance entre ces deux PLD, et nous prouvons certaines propriétés n'ayant pas d'analogues dans le cas des corps de nombres quadratiques réels. De plus, nous montrons même que la structure de l'ensemble des idéaux réduits principaux est plus proche de celle d'un groupe dans le cas particuliers des corps de fonctions elliptiques sur un corps fini que dans le cas général, bien que ce ne soit pas un groupe.

Abstract. In 1994, the well-known Diffie-Hellman key exchange protocol was for the first time implemented in a non-group based setting. Here, the underlying key space was the set of reduced principal ideals of a real quadratic number field. This set does not possess a group structure, but instead exhibits a so-called infrastructure. More recently, the scheme was extended to real quadratic congruence function fields, whose set of reduced principal ideals has a similar infrastructure. As always, the security of the protocol depends on a certain discrete logarithm problem (DLP).

1991 *Mathematics Subject Classification.* 11A55, 11R58, 11T71, 11Y16, 68Q25, 94A60. .
Key words and phrases. real quadratic congruence function field, continued fractions, reduced ideals, elliptic curves, discrete logarithm..
Manuscrit reçu le 15 avril 1996.

In this paper, we show that for real quadratic congruence function fields of genus one, i.e. elliptic congruence function fields, this DLP is equivalent to the DLP for elliptic curves over finite fields. We present the explicit corresponce between the two DLPs and prove some properties which have no analogues for real quadratic number fields. Furthermore, we show that for elliptic congruence function fields, the set of reduced principal ideals is even "closer" to a group than in the general case, but still fails to be a group.

1. Introduction

In 1976 Diffie and Hellman [6] introduced their well-known protocol for exchanging a secret cryptographic key. Their scheme was based on arithmetic in the multiplicative group ${\mathbb{F}_p}^*$ of integers relatively prime to a large prime p, but can be extended to a more general setting of a finite group G such that $|G|$ $(= n)$ is large. Recently, Scheidler, Buchmann and Williams [9] were able, for the first time, to exhibit a secure key exchange protocol, similar in concept to that of Diffie-Hellman, which does not make use of a group as the underlying structure. This scheme is based on the infrastructure (see Shanks [13]) of the principal ideal class of a real quadratic number field. In [10], 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 ideas of Scheidler, Buchmann and Williams. As always, the security of the protocol depends on a certain discrete logarithm problem (DLP).

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 [12], 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 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 of genus 1, which we call *(real) elliptic congruence function fields*, 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 [8]).

The main results are stated in Theorem 7.3, Theorem 7.4, and also in Theorem 4.2, Theorem 4.10. We first explain the properties of the set of reduced principal ideals in elliptic congruence function fields (see also [17], [18], or [19]). Then, we draw the connection to elliptic curves by combining the results in elliptic congruence function fields with formulae derived from Adams and Razar [2]. 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. Furthermore, we give answers to the following questions which are important for the equivalence:

- Does the set of reduced principal ideals form a group? (Theorem 4.10)
- Is there a computable relation between the distance function δ_i and the index i? (Theorem 4.2)
- Is there a relation between the number of reduced principal ideals and the order of $\langle\mathcal{P}\rangle$? (Theorem 6.4)
- 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 7.3)

The underlying structure of the key exchange protocols in [9] and [10] is the set of reduced principal ideals. In either case, this set does not form a group; however, it is "almost" a group. For elliptic congruence function fields, we will prove (Theorem 4.8) that the set of reduced principal ideals is even "closer" to a group, but it still fails to be a group (Theorem 4.10). Furthermore, for real quadratic congruence function fields of arbitrary genus and for real quadratic number fields, we expect (see [22], [4], [17]) that the distance function is asymptotically linear in almost all cases, i.e., there is a real number γ, $1 \leq \gamma \leq 2$, such that

$$\delta_i \approx \gamma \cdot i \quad (i \in \mathbb{N})\ .$$

For any elliptic congruence function field K, it is true (Theorem 4.2) that

$$\delta_i = i \qquad (2 \leq i \leq m+1), \tag{1.1}$$

where m denotes the period of a reduced principal ideal. Thus, we have (Corollary 4.3) that

$$R = m + 1 \tag{1.2}$$

where R is the regulator of K. There exist no analogues for (1.1) or (1.2) in real quadratic number fields. It is an open question whether it is possible to construct any series of real quadratic number fields with these properties.

In Sections 2 and 3 of this paper, we present the arithmetic of reduced ideals in real quadratic congruence function fields of arbitrary genus. The situation in elliptic congruence function fields is described in Section 4. The connection between elliptic curves and real quadratic congruence function fields is drawn in Section 5 and 6. In Section 7, we outline the one-to-one correspondence and the equivalences.

2. Real Quadratic Congruence Function Fields

In this section, we present the situation as described in [16], [17], [19], [10] and [21]. Basic references for this subject are [3], [5], and [20].

Let $k = \mathbb{F}_q$ be a finite field of odd characteristic with q elements. A *quadratic congruence function field* K over the finite field k of *constants* is a quadratic extension of the rational function field $k(x)$, i.e. $K = k(x)(\sqrt{D})$, where $D \in k[x]$ is a squarefree polynomial. Let K be a *real quadratic congruence function field*. Then, $K = k(x)(\sqrt{D})$, where $D \in k[x]$ is a squarefree polynomial of even degree whose leading coefficient is a square in $k^* = k \setminus \{0\}$. For $\alpha = u + v\sqrt{D} \in K$ ($u, v \in k(x)$), denote by $\overline{\alpha} = u - v\sqrt{D}$ its *conjugate*. The *ring of integers of* K is $\mathfrak{O} = k[x][\sqrt{D}]$, and the *unit group* E of K/k is of the form $E = k^* \times \langle \epsilon \rangle$, where $\epsilon \in K$ is a *fundamental unit* of K.

We know that the the infinite place $\mathfrak{P}_\infty$ of $k(x)$ splits completely in K, so that $\mathfrak{P}_\infty = \mathfrak{P}_1 \cdot \mathfrak{P}_2$, where $\mathfrak{P}_1$ and $\mathfrak{P}_2$ are the infinite places of K/k. If $v_{\mathfrak{P}_1}$ and $v_{\mathfrak{P}_2}$ denote the two normed extensions of the negative degree valuation $v_{\mathfrak{P}_\infty}$ from $k(x)$ to K, we define the natural number $R := |v_{\mathfrak{P}_1}(\epsilon)| = |v_{\mathfrak{P}_2}(\epsilon)| \geq 1$ as the *regulator of* K/k *with respect to* $\mathfrak{O}$.

A result of F. K. Schmidt [11] shows its connection with two further invariants, namely the *ideal class number* h' and the *divisor class number* h,

$$h = R\,h'.$$

If we denote by $\mathcal{C}_0$ the group of all divisor classes of degree 0, then h is defined to be its order. Furthermore, if g denotes the *genus* of k, then $g = \frac{1}{2}\deg(D) - 1$.

It can be seen form [21] or [5] that $k(x)_{\mathfrak{P}_\infty}$, the completion of $k(x)$ with respect to $\mathfrak{P}_\infty$, is the field of power series in the variable $1/x$ and the completions of K with respect to $\mathfrak{P}_1$ and $\mathfrak{P}_2$ are isomorphic to $k(x)_{\mathfrak{P}_\infty}$. This means that $K_{\mathfrak{P}_1} \cong K_{\mathfrak{P}_2} \cong k(x)_{\mathfrak{P}_\infty} = k((1/x))$. We fix one of the two places at infinity by letting $\mathfrak{P}_1$ be the place which corresponds to the case where $\sqrt{1} = 1$. Also, K is a subfield of $k((1/x))$. Elements of K can then be considered as Laurent series at $\mathfrak{P}_1$ in the variable $1/x$. 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 $|0| = 0$. It follows that the regulator R is the degree of the fundamental unit, i.e. $R = \deg(\epsilon)$.

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 $i \in \mathbb{N}_0$. 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

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

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

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

where α_j denote the partial remainders of α.

3. Reduced Ideals and Continued Fractions

Let $\alpha \in K$ be an element of the form $\alpha = (P + \sqrt{D})/Q$, where $0 \neq Q$, $P, \in k[x]$ 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, $r_i \in k[x]$ for $i \in \mathbb{N}$ by using the formulae

$$\left\{ \begin{array}{l} P_i = a_{i-1} Q_{i-1} - P_{i-1} = d - r_{i-1} \\ Q_i = (D - P_i^2)/Q_{i-1} = Q_{i-2} + a_{i-1}(r_{i-1} - r_{i-2}) \\ a_i = (P_i + d) \operatorname{div} Q_i \\ r_i = (P_i + d) \bmod Q_i \end{array} \right\} \tag{3.1}$$

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

$$\theta_i = \prod_{j=1}^{i-1} \frac{1}{\alpha_j} \quad (i \geq 2) \quad , \tag{3.2}$$

then we get

$$\theta_i \, \overline{\theta}_i \;=\; (-1)^{i-1} \, Q_{i-1}/Q_0 \qquad (\, i \in \mathbb{N} \,) \quad . \tag{3.3}$$

The case $\alpha = \sqrt{D}$ plays an important role. We collect some properties of it in the following Remark.

REMARK 3.1. *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 β, $\gamma \in \mathfrak{O}$, we denote by $[\,\beta, \gamma\,]$ the module $\beta k[x] + \gamma k[x]$. Let $\mathfrak{a}$ be an (integral) ideal. Then there exist polynomials S, P, $Q \in k[x]$ with $Q|(D - P^2)$ such that

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

The set $\{\, S\,Q,\, S\,P + S\,\sqrt{D}\,\}$ is called $k[x]$*-base* of $\mathfrak{a}$. If we set $\operatorname{sgn}(S) = \operatorname{sgn}(Q) = 1$, 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 $k[x]$-base*, meaning that there exists a $k[x]$-base $\{\, S\,Q,\, S\,P + S\,\sqrt{D}\,\}$ with $\deg(P) < \deg(Q)$. The *conjugate ideal* of $\mathfrak{a}$ is given by $\overline{\mathfrak{a}} := \{\overline{\alpha} \;;\; \alpha \in \mathfrak{a}\}$. We now give the formulae (see [17], [19] or [10]) for the product of two primitive ideals, $\mathfrak{a}_i = [\,Q_i\,,\, P_i + \sqrt{D}\,]$, for $i = 1, 2$, given in adapted form with $\operatorname{sgn}(Q_1) = \operatorname{sgn}(Q_2) = 1$. To find a primitive 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 compute

$$\left\{ \begin{array}{l} S = \gcd(\,Q_1,\, Q_2,\, P_1 + P_2\,)\ , \\ Q = \frac{Q_1 Q_2}{S^{\,2}}\ , \\ P = \left(P_1 + \frac{Q_1}{S}\left[U(P2 - P_1) + W\left(\dfrac{D - P_1^2}{Q_1}\right)\right]\right)\ (\mathrm{mod}\ Q) \end{array} \right\} \tag{3.4}$$

where U, V, $W \in k[x]$ are such that $S = UQ_1 + VQ_2 + W(\,P_1 + P_2\,)$.

A primitive ideal $\mathfrak{a}$ is called *reduced*, if there exists for $\mathfrak{a}$ a $k[x]$-base of the form $\{\,Q,\, P + \sqrt{D}\,\}$ such that $\left|P - \sqrt{D}\right| < |Q| < \left|P + \sqrt{D}\right|$. If we let $\operatorname{sgn}(Q) = 1$, 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 (3.1). We have that $Q_0\theta_i$, $Q_0\overline{\theta_i} \in \mathfrak{O}$ and that

$$(3.5) \qquad (\, Q_0\theta_i \,)\, \mathfrak{a}_i \;=\; (\, Q_{i-1} \,)\, \mathfrak{a}_1.$$

It follows that

(3.6)

$$\deg\left(\overline{\theta}_i\right) = \deg(\, Q_{i-1} \,) - \deg(\, Q_0 \,) + \sum_{j=1}^{i-1} \deg(\, a_j \,) \qquad (\, i \in \mathbb{N} \,) \quad .$$

Properties of reduced ideals are summarized in the following Lemma (see [17] or [19]):

LEMMA 3.2. *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* $i > \max\{1, \frac{1}{2}\deg(Q) - \frac{1}{4}\deg(D) + 2\}$.
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* $k[x]$*-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* $k[x]$*-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 3.2 a). By developing the continued fraction expansion of $\alpha = \sqrt{D}$ with the formulae in (3.1), 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 [17], or [19]). More generally, we have

$$(3.7) \qquad \mathfrak{r}_{\lambda m+i} = \mathfrak{r}_i \quad (i \in \mathbb{N},\, \lambda \in \mathbb{N}_0) \quad .$$

It follows from Lemma 3.2 e) that the sequence $(\mathfrak{r}_i)_{i\in\mathbb{N}}$ contains all reduced principal ideals. By (3.5), we get $\mathfrak{r}_i = (\,\overline{\theta}_i\,)$ for $i \in \mathbb{N}$. If $\mathfrak{r}_i = [\, Q_{i-1},\, P_{i-1} + \sqrt{D}\,]$, then its conjugate ideal is given by $\overline{\mathfrak{r}}_i = [\, Q_{i-1},\, P_{i-1} - \sqrt{D}\,]$. From [17] or [19], we conclude that

$$(3.8) \qquad \overline{\mathfrak{r}}_i \;=\; \mathfrak{r}_{m-i+2} \quad (\, i = 1, 2, \ldots, m+1 \,) \quad .$$

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 3.1, we get for the regulator: $R = \delta_{m+1}$, or, more generally,

$$\delta_{\lambda m+i} = \lambda R + \delta_i \quad (i \in \mathbb{N},\, \lambda \in \mathbb{N}_0) \quad . \tag{3.9}$$

By Lemma 3.2 d), (3.2) and (3.3), we have $\delta_1 = 0$ and

$$\delta_i = \frac{1}{2}\deg(D) + \sum_{j=1}^{i-2} \deg(a_j) \qquad (i \geq 2). \tag{3.10}$$

Let i, j be arbitrary, positive integers. By using the formulae in (3.4), we are able to find a polynomial $S \in k[x]$ and a primitive ideal $\mathfrak{c}$ such that $\mathfrak{r}_i\mathfrak{r}_j = (S)\mathfrak{c}$. We apply the continued fraction algorithm to $\mathfrak{c}_1 = \mathfrak{c} = [Q',\, P' + \sqrt{D}]$. We denote by P_i', Q_i' and θ_i' the quantities appearing in the continued fraction expansion of $\alpha' = (P' + \sqrt{D})/Q'$ as defined in (3.1) and (3.2). By Lemma 3.2 b), it is guaranteed that, after a finite number of steps, we obtain a reduced ideal equivalent to $\mathfrak{c}_1 = \mathfrak{c}$. Let l be minimal such that $\mathfrak{c}_l$ is reduced. From Lemma 3.2 e), we deduce that $\mathfrak{c}_l = \mathfrak{r}_k$ for a $k \in \mathbb{N}$. Therefore, we define an operation $*$ (*Giant step*) by setting $\mathfrak{r}_i * \mathfrak{r}_j = \mathfrak{r}_k$.

LEMMA 3.3. *In above situation, we have*

$$\delta_k = \delta_i + \delta_j + f \quad ,$$

where $f = \deg(\overline{\theta_l'}) - \deg(S) \in \mathbb{Z}$ *and* $2 - \deg(D) \leq f \leq 0$.
(see [17], Theorem II.5.1, or [19], [10])

As in [10], we define

DEFINITION 3.4. *The* discrete logarithm problem *(DLP)* for real quadratic congruence function fields *is given as follows: For any reduced principal ideal* $\mathfrak{r}$, *find* $\delta(\mathfrak{r})$, $0 \leq \delta(\mathfrak{r}) < R$.

4. Elliptic Congruence Function Fields

Here, we apply the results of the previous section to real quadratic congruence function fields of genus 1. These fields are called *elliptic congruence function fields*.

Let $K = k(x)(\sqrt{D})$, where $\deg(D) = 4$, $g = 1$, and $\operatorname{sgn}(D)$ a square in k^*. Let m be the quasi-period of the continued fraction expansion of $\alpha = \sqrt{D}$. We now consider the sequence of reduced principal ideals $(\mathfrak{r}_i)_{i\in\mathbb{N}}$, starting at $\mathfrak{r}_1 = [1, \sqrt{D}]$. Then,

$$\mathfrak{r}_i = [Q_{i-1},\, P_{i-1} + \sqrt{D}] = [E_{i-1},\, F_{i-1} + \sqrt{D}] \quad ,$$

where the first $k[x]$-base is its reduced base, and the second $k[x]$-base its adapted base, i.e. $E_{i-1} = Q_{i-1}/\mathrm{sgn}(Q_{i-1})$, $\mathrm{sgn}(E_{i-1}) = 1$, and $F_{i-1} \equiv P_{i-1} \bmod E_{i-1}$. From Lemma 3.2 d), we derive that $\deg(Q_{i-1}) = 0$ or 1. Obviously, if $\deg(Q_{i-1}) = 0$, then, by Remark 3.1 and (3.7), we know that $i = \lambda m + 1$, and that $\mathfrak{r}_i = [\,1, \sqrt{D}\,] = \mathfrak{r}_1$. Let i be such that $\deg(Q_{i-1}) = 1$; thus, the adapted base of $\mathfrak{r}_i$ is given by

$$\mathfrak{r}_i \;=\; [\,x \,+\, e_{i-1},\, f_{i-1} + \sqrt{D}\,] \quad ,$$

where $e_{i-1}, f_{i-1} \in k$. This means that $E_{i-1} = x + e_{i-1}$ is a monic polynomial of degree 1, and $F_{i-1} = f_{i-1}$ is a constant polynomial.

Proposition 4.1. *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 $\mathfrak{r}_i$:*

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

where $e_{i-1}, f_{i-1} \in k$.

From the following theorem, we can conclude that the distance is equal to the index in one round of the continued fraction expansion of $\alpha = \sqrt{D}$. There is no analogue for this result in real quadratic number field. Furthermore, this theorem is one important step to prove the equivalence of the DLP for real quadratic congruence function fields of genus 1 and that for elliptic curves.

Theorem 4.2. *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*

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

Proof. By Lemma 3.2 d) and the above remarks, we conclude that $\deg(a_j) = \deg(\sqrt{D}) - \deg(Q_j) = 2 - 1 = 1$ for $j = 1, \ldots, m-1$. By inserting this in (3.10), we see that for $i = 2, \ldots, m+1$:

$$\delta_i \;=\; 2 \,+\, \sum_{j=1}^{i-2} \deg(a_j) \;=\; 2 \,+\, i \,-\, 2 \;=\; i \quad .$$

Corollary 4.3. *In the situation of Theorem 4.2, we get for the regulator R of K/k with respect to $\mathfrak{O}$ that*

$$R \;=\; m \,+\, 1 \quad .$$

Proof. It follows easily from Theorem 4.2, since $R = \delta_{m+1}$.

Corollary 4.4. *In the situation of Theorem 4.2, let $i \geq 2$ be such that $i = \lambda m + i_0$, where $\lambda \in \mathbb{N}_0$ and $2 \leq i_0 < m$. Then,*

$$\delta_i = i + \lambda \quad .$$

Proof. By (3.9), we know that $\delta_{\lambda m + i_0} = \lambda R + \delta_{i_0}$. Thus, by Theorem 4.2 and Corollary 4.3, we have for $i_0 \geq 2$ that

$$\delta_i = \delta_{\lambda m + i_0} = \lambda (m + 1) + i_0 = i + \lambda \quad .$$

Corollary 4.5. *If* $\deg(D) = 4$*, then the discrete logarithm problem (DLP) can be formulated as follows: given any reduced principal ideal $\mathfrak{r} = \mathfrak{r}_i$, where $1 \leq i \leq m$; find i.*

Proof. This is clear, since, by Theorem 4.2, $\delta(\mathfrak{r}) = \delta(\mathfrak{r}_i) = i$ for $2 \leq i \leq m$.

Next, we will show that the set $\{ \mathfrak{r}_1, \mathfrak{r}_2, \ldots, \mathfrak{r}_m \}$ is "almost" a group under the Giant step operation.

For any $i, j \in \mathbb{N}$, we proceed as in the previous section. If $\mathfrak{r}_i = \mathfrak{r}_1 = (1)$, then $\mathfrak{r}_i * \mathfrak{r}_j = \mathfrak{r}_j$ and $\delta(\mathfrak{r}_i * \mathfrak{r}_j) = \delta_j = \delta_i + \delta_j$. If $\mathfrak{r}_j = \mathfrak{r}_1 = (1)$, then $\mathfrak{r}_i * \mathfrak{r}_j = \mathfrak{r}_i$ and $\delta(\mathfrak{r}_i * \mathfrak{r}_j) = \delta_i = \delta_i + \delta_j$. Now, let $\mathfrak{r}_i, \mathfrak{r}_j \neq \mathfrak{r}_1$ be given in adapted form. Then $\mathfrak{r}_i = [x + e_{i-1}, f_{i-1} + \sqrt{D}]$ and $\mathfrak{r}_j = [x + e_{j-1}, f_{j-1} + \sqrt{D}]$ with $e_{i-1}, f_{i-1}, e_{j-1}, f_{j-1} \in k$. First, we compute S, Q' $P' \in k[x]$ such that $\mathfrak{r}_i \mathfrak{r}_j = (S) \mathfrak{c} = (S)[Q', P' + \sqrt{D}]$ by making use of the formulae in (3.4). Then, we set $\mathfrak{c}_1 = \mathfrak{c}$, and, with the continued fraction algorithm, we obtain $\mathfrak{c}_l = \mathfrak{r}_k$ and $\mathfrak{r}_i * \mathfrak{r}_j = \mathfrak{r}_k$, where $\delta_k = \delta_i + \delta_j + f$ and $f = \deg(\overline{\theta'_l}) - \deg(S)$. We distinguish between three cases.

case 1: Let $e_{i-1} \neq e_{j-1}$. Then, by (3.4), we get

$$\begin{aligned} S &= 1 = \gcd (x + e_{i-1}, x + e_{j-1}, f_{i-1} + f_{j-1}) \quad , \\ Q' &= (x + e_{i-1}) (x + e_{j-1}) \quad , \\ P' &= f_{i-1} + (x + e_{i-1}) \frac{f_{j-1} - f_{i-1}}{e_{i-1} - e_{j-1}} \quad , \end{aligned}$$

where $U = 1/(e_{i-1} - e_{j-1})$, $V = -U$ and $W = 0$. It is easy to see that $\deg(Q'_1) < \deg(Q') = 2$. Thus, by Lemma 3.2 a), $\mathfrak{c}_2 = [Q'_1, P'_1 + \sqrt{D}]$ is reduced, i.e. $l = 2$ and $\mathfrak{r}_i * \mathfrak{r}_j = \mathfrak{c}_2$. Also, by Lemma 3.2 d), $\deg(a'_1) + \deg(Q'_1) = 2$. It follows from (3.2) and (3.3) that

$$f = \deg(\overline{\theta'_2}) - 0 = \deg(Q'_1) - \deg(Q') + \deg(a'_1) = 2 - 2 = 0 \quad .$$

This means that

$$\delta_k = \delta_i + \delta_j \quad .$$

case 2: Let $e_{i-1} = e_{j-1}$ and $f_{i-1} + f_{j-1} \neq 0$. Then, $S = 1$, $Q' = (x + e_{i-1})^2$

and $P' \equiv (f_{i-1}f_{j-1}+D)/(f_{i-1}+f_{j-1}) \bmod Q'$. We proceed as in case 1, and obtain $\mathfrak{r}_i * \mathfrak{r}_j = \mathfrak{c}_2 = \mathfrak{r}_k$, $f=0$, and

$$\delta_k \;=\; \delta_i \;+\; \delta_j \quad .$$

case 3: Let $e_{i-1} = e_{j-1}$ and $f_{i-1}+f_{j-1} = 0$. This is equivalent to $\mathfrak{r}_j = \overline{\mathfrak{r}}_i$. We have $S = \gcd(x+e_{i-1}, 0) = x + e_{i-1}$, $\deg(S) = 1$, $Q' = 1$ $P' = 0$, $\mathfrak{r}_i * \mathfrak{r}_j = \mathfrak{c}_1 = [1, \sqrt{D}] = \mathfrak{r}_k$, and

$$f \;=\; \deg(\,\overline{\theta_1'}\,) - \deg(S) \;=\; -1 \quad .$$

Thus,

$$\delta_k \;=\; \delta_i \;+\; \delta_j \;-\; 1 \quad .$$

Theorem 4.6. *In the continued fraction expansion of $\alpha = \sqrt{D}$, we have for the distances $\delta_i = \delta(\mathfrak{r}_i)$, $\delta_j = \delta(\mathfrak{r}_j)$, and $\delta_k = \delta(\mathfrak{r}_k) = \delta(\mathfrak{r}_i * \mathfrak{r}_j)$, that*

$$\delta_k \;=\; \begin{cases} \delta_i \;+\; \delta_j \;-\; 1 \quad , & \textit{if} \quad \mathfrak{r}_j = \overline{\mathfrak{r}}_i \text{ and } m \not| j-1 \\[2ex] \delta_i \;+\; \delta_j \quad , & \textit{otherwise.} \end{cases}$$

Remark 4.7. *For $1 \le i \le j \le m+1$, we see from (3.8), that $\mathfrak{r}_j = \overline{\mathfrak{r}}_i$, if and only if $j = m-i+2$. Let $\mathfrak{r}_j = \overline{\mathfrak{r}}_i$. Then $i+j = m+2$. For $m \not| j-1$ we have that*

$$\delta(\mathfrak{r}_i * \mathfrak{r}_{m-i+2}) = m+1 = R = \delta_i + \delta_{m-i+2} - 1,$$

and for $j = m+1$, i.e. $i = 1$, we have that

$$\delta(\mathfrak{r}_1 * \mathfrak{r}_{m+1}) = m+1 = R = \delta_i + \delta_{m-i+2} \;.$$

We conclude that if $2 \le i \le j \le m+1$ and $i+j \le m+1$, then $\mathfrak{r}_j \ne \overline{\mathfrak{r}}_i$. For $1 \le i \le m+1$, we have, by (3.7), that $\mathfrak{r}_j = \overline{\mathfrak{r}}_i$, if and only if $j = \lambda m - i + 2$ ($\lambda \in \mathbb{N}$).

The following Theorem shows that the set of reduced principals ideals has “almost” a group structure, and, especially, there exists “almost” an associative law. However, we are not able to generalize this for arbitrary i and j.

Theorem 4.8. *In the continued fraction expansion of $\alpha = \sqrt{D}$, we have for reduced, principal ideals $\mathfrak{r}_i$, $\mathfrak{r}_j$ with $2 \le i, j \le m+1$ and $i+j \le m+1$ that*

$$\mathfrak{r}_i * \mathfrak{r}_j \;=\; \mathfrak{r}_{i+j} \quad ,$$

and $\delta(\mathfrak{r}_i * \mathfrak{r}_j) = i + j$.

Proof. From Remark 4.7 we derive that $\mathfrak{r}_j \neq \overline{\mathfrak{r}}_i$. Since $i + j \leq m + 1$, we know from Theorem 4.6 and Theorem 4.2 that

$$\delta(\mathfrak{r}_i * \mathfrak{r}_j) = \delta_i + \delta_j = i + j = \delta_{i+j} \quad .$$

Also, we have that $\delta_{i+j} = \delta(\mathfrak{r}_i * \mathfrak{r}_j) = \delta_k$. Thus, $k = i + j$, and the result follows.

REMARK 4.9. *For $2 \leq i \leq m + 1$, we have that*

$$\mathfrak{r}_i * \mathfrak{r}_{m-i+2} = \mathfrak{r}_1 = \mathfrak{r}_{m+1} = \mathfrak{r}_i * \mathfrak{r}_{m-i+1} \quad .$$

For example, let $i = 2$. We conclude that there exist two elements $\mathfrak{r}$ such that $\mathfrak{r}_2 * \mathfrak{r} = \mathfrak{r}_1 = (1)$, namely $\mathfrak{r} = \mathfrak{r}_{m-1}$ and $\mathfrak{r} = \mathfrak{r}_m$. Now, we will see, why there is no group structure.

THEOREM 4.10. *In the continued fraction expansion of $\alpha = \sqrt{D}$, let $i, j \in \mathbb{N}$ with $2 \leq i, j \leq m+1$ such that $i + j = m + i_0$, where $2 \leq i_0 \leq m$. Then,*

$$\mathfrak{r}_i * \mathfrak{r}_j = \mathfrak{r}_{i+j-1} \quad ,$$

and $\delta(\mathfrak{r}_i * \mathfrak{r}_j) = \delta_{i+j-1}$.

Proof. For $i_0 = 2$ the assertion follows from Remark 4.7. Let $i_0 \geq 3$. First, we see from Remark 4.7 that $\mathfrak{r}_j \neq \overline{\mathfrak{r}}_i$. Thus, by Theorem 4.6, $\delta_k = \delta(\mathfrak{r}_i * \mathfrak{r}_j) = \delta_i + \delta_j$. Since $2 \leq i, j \leq m+1$, we have, from Theorem 4.2, that $\delta_k = i+j = m+i_0$. We apply Corollary 4.4 to obtain $\delta_k = \delta_{m+i_0-1} = \delta_{i+j-1}$ and conclude that $k = i + j - 1$.

For general i and j, we develop the corresponding rules.

THEOREM 4.11. *In the continued fraction expansion of $\alpha = \sqrt{D}$, let $i = \lambda m + i_1$ and $j = \mu m + j_1$ be such that $2 \leq i_1, j_1 \leq m$ and $\lambda, \mu \in \mathbb{N}_0$. Then*

$$\mathfrak{r}_i * \mathfrak{r}_j = \begin{cases} \mathfrak{r}_{i+j} & , \ \text{if} \quad i_1 + j_1 \leq m + 1 \\ \mathfrak{r}_{i+j-1} & , \ \text{if} \quad i_1 + j_1 \geq m + 2 \end{cases}$$

Proof. By (3.7), we get $\mathfrak{r}_i * \mathfrak{r}_j = \mathfrak{r}_{i_1} * \mathfrak{r}_{j_1}$ with $2 \leq i_1, j_1 \leq m$. Thus, the result follows from Theorem 4.8 and Theorem 4.10.

5. The Quartic Model of an Elliptic Curve

In this section, we develop the quartic model of an elliptic curve E over a finite field k and show the connection between E and the corresponding real quadratic congruence function field of genus 1. We follow the notation of [2].

Let E be an elliptic curve over the finite field $k = \mathbb{F}_q$ of odd characteristic. We may, and will, assume E to be given in *short Weierstrass normal form*

$$E : w^2 = v^3 + Av + B \quad (A, B \in k) \quad , \tag{5.1}$$

where $\Delta = -4A^3 - 27B^2 \neq 0$. Let $K = k(v, w)$. We consider the additive *group of all k-rational points on E*

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

with the *point at infinity*

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

as the identity with respect to the usual group law on E.

Let $\mathcal{P} = (a, b) \neq \mathcal{O}$ be any k-rational point on E, i.e. $\mathcal{P} \in E(k) \setminus \{\mathcal{O}\}$. We define

$$(5.2)\ x := \frac{w+b}{v-a} \quad , \quad y := 2v + a - \left(\frac{w+b}{v-a}\right)^2 = 2v + a - x^2 \quad ,$$

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

$$(5.3) \qquad E_{\mathcal{P}} : y^2 = x^4 - 6ax^2 - 8bx + c =: D$$

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

Conversely, let $K = k(x)(\sqrt{D})$ be a real quadratic congruence function field of genus 1. We also require that the characteristic is different from 3. Then D is a squarefree polynomial of degree 4 where $\mathrm{sgn}(D)$ is a square in k^*. Without loss of generality, we assume D to be of the form in (5.3), i.e.

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

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

$$(5.4) \quad v := \frac{1}{2}(x^2 + y - a) \quad , \quad w := \frac{1}{2}(x^3 + xy - 3ax - 2b) \quad ,$$

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 (5.1) and a k-rational point $\mathcal{P} := (a, b) \in E(k) \setminus \{\mathcal{O}\}$ on E. This means that (5.2) and (5.4) provide a birational equivalence between E and $E_{\mathcal{P}}$. Again, the function fields are equal, i.e. $K = k(x)(\sqrt{D}) = k(v, w)$.

In this situation, we know that the divisor class number h, and the genus g of K are absolute invariants of K, whereas the ideal class number h', and the regulator R are relative invariants with respect to the ring of integers

$\mathfrak{O}$. Furthermore, there is a bijection of sets between $E(k)$ and the zero class group $\mathcal{C}_0$ (see for example [15]). In particular, it follows that

$$h = \#E(k) \quad . \tag{5.5}$$

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 (5.2) and $v_{\mathcal{Q}}$ be the value $v(\mathcal{Q})$ under the transformation (5.4). The conjugation in $K = k(x)(y)$ yields a bi-regular k-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 $\overline{\mathcal{O}} = \mathcal{P}$, $\overline{\mathcal{P}} = \mathcal{O}$.

DEFINITION 5.1. *We define the discrete logarithm problem (DLP) for elliptic curves over finite fields 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.*

6. Continued Fractions and Orders of Points

In the notation of the previous section, we 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 k-rational point on E such that $\mathcal{Q} \neq \mathcal{P}$ and that the characteristic of k is different from 2 and 3. Note that we always have $\mathfrak{O} = \mathfrak{O}_{\mathcal{P}}$ and $D = D_{\mathcal{P}}$. We now draw a connection between the addition on E and the continued fraction expansion of $\alpha = \sqrt{D}$. As in [2], we define:

DEFINITION 6.1. *Let $\mathcal{Q} \in E(k)$ be such that $\mathcal{Q} \neq \mathcal{P}$. We set*

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

By (5.3), (5.4) and the definition of $\overline{\mathcal{Q}}$, we get for $\mathcal{Q} \neq \mathcal{O}$ that

$$f_{\mathcal{Q}} = \frac{x^2 - x_{\mathcal{Q}}^2 + y_{\mathcal{Q}} + \sqrt{D}}{2(x - x_{\mathcal{Q}})} \quad , \tag{6.1}$$

and

$$f_{\mathcal{O}} = \frac{1}{2}\left(x^2 - 3a + \sqrt{D}\right) \quad . \tag{6.2}$$

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

We develop the continued fraction expansion of $\sqrt{D}$, and obtain a sequence of elements $\alpha_0 = \sqrt{D}$, α_1, α_2, ..., where, by (3.1), we have written $\alpha_{i-1} = (P_{i-1} + \sqrt{D})/Q_{i-1}$ $(i \geq 2)$ with $P_{i-1}, Q_{i-1} \in k[x]$. The continued fraction expansion of $\sqrt{D}$ is periodic and quasi-periodic with quasi-period $m = m_{\mathcal{P}}$. As in Section 3, 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 $\mathfrak{r}_i = [\,Q_{i-1}, P_{i-1} + \sqrt{D}\,]$.

If we explicitly refer to the continued fraction expansion of an element $\beta \in k(x)(\sqrt{D})$, we write $\alpha_i(\beta)$ $(i \geq 1)$ for the partial remainders. Note that $\alpha_i(\sqrt{D}) = \alpha_i$ $(i \geq 1)$.

Lemma 6.2. *In the continued fraction expansions of $f_{\mathcal{O}}$ and $\sqrt{D}$, we have that*

$$\alpha_i(f_{\mathcal{O}}) = 2^{-(-1)^i}\alpha_i \quad (\, i \geq 1\,) \quad .$$

In particular, the continued fraction expansions of $f_{\mathcal{O}}$ and $\sqrt{D}$ have the same quasi-period m and the same period.

Proof. By (5.2) and (6.2), we see that $2f_{\mathcal{O}} - \sqrt{D} = x^2 - 3a \in k[x]$. Thus, the continued fraction expansion of $\sqrt{D}$ differs from that of $2f_{\mathcal{O}}$ only in the first term, i.e.

$$\alpha_i(2f_{\mathcal{O}}) = \alpha_i(\sqrt{D}) = \alpha_i \quad (\, i \geq 1\,) \quad .$$

Then, by Remark 2.1, we follow that

$$\alpha_i(f_{\mathcal{O}}) = \left(\frac{1}{2}\right)^{(-1)^i} \alpha_i(2f_{\mathcal{O}}) = 2^{-(-1)^i}\alpha_i \quad (\, i \geq 1\,) \quad .$$

The proof of this lemma is the corrected proof of Corollary 4.4 of [2]. We now state an important result which is due to Adams and Razar [2], Theorem 4.2.

Theorem 6.3. *(Adams & Razar) Let E be an elliptic curve over a finite field k with characteristic different from 2, and let $\mathcal{P} \in E(k) \setminus \{\mathcal{O}\}$ with ord$(\mathcal{P}) \neq 2$. Then $\mathcal{P}$ on E has finite order μ, and the continued fraction expansion of $f_{\mathcal{O}}$ is pure quasi-periodic with quasi-period $m(f_{\mathcal{O}})$. Furthermore,*

$$\mu = m(f_{\mathcal{O}}) + 1 \,.$$

Theorem 6.4. *Let E be an elliptic curve over a finite field k with characteristic different from 2, 3. Let $\mathcal{P} \in E(k)$ be such that $\mathcal{P} \neq \mathcal{O}$, and let ord$(\mathcal{P}) \neq 2$. Then,*

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

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

Proof. From Theorem 6.3 we derive that the continued fraction expansion of $f_{\mathcal{O}}$ is pure quasi-periodic with quasi-period $m(f_{\mathcal{O}})$, and that

$$\mathrm{ord}(\mathcal{P}) \;=\; m(f_{\mathcal{O}}) \,+\, 1\ .$$

By Lemma 6.2, we know that $m = m(f_{\mathcal{O}})$. Thus,

$$\mathrm{ord}(\mathcal{P}) \;=\; m \,+\, 1\ .$$

The second equality follows immediately from Corollary 4.3.

This means that we have a connection between the order of the subgroup of $E(k)$ 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 7) than Theorem 6.4.

7. 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 $\mathrm{ord}(\mathcal{P}) \neq 2$, $\mathrm{char}(k) \neq 2, 3$, and that $f_{i\,\mathcal{P}}$ is only defined for $i \neq 1$.

THEOREM 7.1. *(Adams & Razar) Let E be an elliptic curve over a finite field k with characteristic different from 2, and let $\mathcal{P} \in E(k) \setminus \{\mathcal{O}\}$ with ord($\mathcal{P}$) $\neq 2$. For all $\nu \in \mathbb{N}$ with $1 \leq \nu \leq$ ord($\mathcal{P}$) $- 1$ there exist $\rho_\nu \in k^*$ such that* [1]

$$\alpha_\nu(f_{\mathcal{O}}) \;=\; \rho_\nu \cdot f_{(\nu+1)\mathcal{P}}\ .$$

COROLLARY 7.2. *If $\mathcal{P}$ is a point on E with ord($\mathcal{P}$) $\neq 2$, then we have, in the continued fraction expansion of $\alpha_0 = \sqrt{D}$, that*

$$f_{i\,\mathcal{P}} \;=\; c_i \cdot \alpha_{i-1} \quad (2 \,\leq\, i \,\leq\, m)\ ,$$

where $c_i \in k^*$. More general, we have that

$$f_{i\,\mathcal{P}} \;=\; c_{\lambda m+i} \cdot \alpha_{\lambda m+i-1} \quad (\,\lambda \in \mathbb{N}_0\,,\, 2 \,\leq\, i \,\leq\, m\,)\ ,$$

where $c_{\lambda m+i} \in k^*$.

Proof. We see from Theorem 7.1 by changing indices $i := \nu + 1$ that

$$f_{i\,\mathcal{P}} \;=\; \rho_{i-1}^{-1} \cdot \alpha_{i-1}(f_{\mathcal{O}}) \;=\; \underbrace{\rho_{i-1}^{-1} \cdot 2^{-(-1)^{i-1}}}_{=:c_i}\alpha_{i-1}\ ,$$

by Lemma 6.2.

[1] We mention here that sometimes in the literature the notation $\varphi_\nu(\alpha) := \alpha_\nu$ is used to express the ν-fold composition of φ with itself, where $\varphi(\alpha) = 1/(\alpha - \lfloor\alpha\rfloor)$.

Let i be arbitrary such that $2 \le i \le m$. We denote the coordinates of $i\,\mathcal{P}$ on $E_{\mathcal{P}}$ by

$$i\,\mathcal{P} \;=\; (\, x_i \,,\, y_i \,) \quad , \tag{7.1}$$

where $x_i,\, y_i \in k$. Note that $i\,\mathcal{P} \neq \mathcal{O},\, \mathcal{P}$. From Corollary 7.2, we know that $f_{i\,\mathcal{P}} = c_i \cdot \alpha_{i-1}$ with $c_i \in k^*$. By (6.1) and (3.1), this relation is equivalent to

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

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

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

Thus,

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

The second equality follows by an easy ideal operation. In particular, the first $k[x]$-base is the reduced $k[x]$-base of $\mathfrak{r}_i$. Since $x_i,\, y_i \in k$, the $k[x]$-base $\{x - x_i,\, y_i + \sqrt{D}\}$ is the adapted $k[x]$-base of $\mathfrak{r}_i$ (see Proposition 4.1). We notice that it is easy to compute the ideal $\mathfrak{r}_i$ from x_i and y_i, and, conversely, to compute $i\,\mathcal{P}$ from the adapted $k[x]$-base of $\mathfrak{r}_i$.

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 7.3. *Let E be an elliptic curve over a finite field k with characteristic different from 2, 3, and let $\mathcal{P} \in E(k)$ be such that $\mathcal{P} \neq \mathcal{O}$, and ord($\mathcal{P}$) $\neq 2$. Then, there is a one-to-one correspondence between the sets $\{i\,\mathcal{P} \,:\, 2 \le i \le m+1\}$ and $\{\mathfrak{r}_1,\, \ldots,\, \mathfrak{r}_m\}$ as follows: Let $\mathcal{Q} \in \{i\,\mathcal{P} \,:\, 2 \le i \le m+1\}$. Then, $\mathcal{Q} = l\,\mathcal{P}$ for a l such that $2 \le l \le m+1$.*

$$\mathcal{Q} \;=\; l\,\mathcal{P} \;\longmapsto\; \mathfrak{r}_{\mathcal{Q}} \;=\; \mathfrak{r}_l \;=\; \begin{cases} [\,1,\, \sqrt{D}\,] & ,\ \textit{if}\ \mathcal{Q} \,=\, \mathcal{O} \\[2ex] [\, x \,-\, x_{\mathcal{Q}} \,,\, y_{\mathcal{Q}} \,+\, \sqrt{D}\,] & ,\ \textit{if}\ \mathcal{Q} \,\neq\, \mathcal{O}\,. \end{cases}$$

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 $1 \le l \le m$. Let $\mathfrak{r}$ be given in adapted form with respect to Proposition 4.1.

$$\mathfrak{r} \;=\; \mathfrak{r}_l \;\longmapsto\; \mathcal{Q} \;=\; l\,\mathcal{P} \;=\; \begin{cases} \mathcal{O} & ,\ \textit{if}\ \mathfrak{r} \,=\, [\,1,\, \sqrt{D}\,] \\[2ex] (\,-\,e\,,\, f\,) & ,\ \textit{if}\ \mathfrak{r} \,=\, [\, x \,+\, e\,,\, f \,+\, \sqrt{D}\,] \neq [\,1,\, \sqrt{D}\,] \end{cases}$$

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

We illustrate the meaning of Theorem 7.3. For $i = 2, \ldots, m+1$, we denote the point $i\mathcal{P}$ on E, $E_{\mathcal{P}}$, respectively, by (v_i, w_i), (x_i, y_i).

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

We now state the main result concerning the equivalence between the DLP for elliptic curves and the DLP for real quadratic congruence function fields of genus 1.

THEOREM 7.4. *The discrete logarithm problem for real quadratic congruence function fields of genus* 1 *with characteristic different from* 2, 3 *can be solved in polynomial time if and only if the discrete logarithm problem for elliptic curves over finite fields can be solved in polynomial time.*

Proof. Here, we use Theorem 7.3 and Theorem 4.2. 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 given, as in (5.1), in short Weierstrass normal form

$$E:\ w^2 = v^3 + Av + B \quad (A, B \in k) \quad ,$$

where $\Delta = -4A^3 - 27B^2 \neq 0$. Let $\mathcal{P} = (a, b) \in E(k)$ 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 (5.2), we obtain the curve

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

E and $E_{\mathcal{P}}$ are birationally equivalent, and the field $k(x)(\sqrt{D})$ is a real quadratic congruence function field of genus 1 with respect to $\mathfrak{O} = k[x][\sqrt{D}]$. Let m be the quasi-period of the continued fraction expansion of $\sqrt{D}$, and let R be the regulator of $k(x)(\sqrt{D})$ 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 $\mathcal{Q} \in E(k)$ such that $\mathcal{Q} = l \cdot \mathcal{P}$, where $l \in \mathbb{N}$, $2 \leq l \leq \mathrm{ord}(\mathcal{P})$. By Theorem 6.4, we know that $\mathrm{ord}(\mathcal{P}) = m+1 = R$. If $l = m+1 = R$, then $\mathcal{Q} = \mathcal{O}$, and, by Theorem 7.3, 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 $R = \delta(\mathfrak{r}_{m+1})$ (see (3.7) and (3.9)). 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 7.3 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 5.2, $\mathfrak{r}_{\mathcal{Q}}$ can be computed from $\mathcal{Q}$ in polynomial time. From Theorem 4.2, 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 elliptic curves over finite fields can be solved in polynomial time. Let $K = k(x)(\sqrt{D})$ be a real quadratic congruence function field of genus 1, where D is a squarefree polynomial of degree 4, and $\mathfrak{O} = k[x][\sqrt{D}]$. Without loss of generality (see Section 5), we assume D to be of the form

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

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

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

The birational transformation in 5.4 yields an elliptic curve E in short Weierstrass normal form

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

and a point $\mathcal{P} := (a, b) \in E(k) \setminus \{\mathcal{O}\}$, 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 $k(x)(\sqrt{D})$ 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, by (3.7), $\mathfrak{r}_1 = \mathfrak{r}_{m+1}$, and, by Theorem 6.4, $\delta(\mathfrak{r}) = \delta(\mathfrak{r}_{m+1}) = R = \mathrm{ord}(\mathcal{P})$. 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 $k[x]$-base of $\mathfrak{r}$ in polynomial time (see [17]), and obtain $\mathfrak{r} = [\,x + e,\, f + \sqrt{D}\,]$, where $e, f \in k$. From Theorem 7.3, we conclude that $\mathfrak{r}$ corresponds to the point $\mathcal{Q} = (-e, f)$ on $E_{\mathcal{P}}$. By (5.4), the coordinates of $\mathcal{Q}$ on E can be computed in polynomial time. Furthermore, we know that $\mathcal{Q} = l\mathcal{P}$. From Theorem 4.2, we get $l = \delta_l$. Thus, by assumption, $\delta(\mathfrak{r}) = \delta(\mathfrak{r}_l) = l$ can be computed in polynomial time.

Note that Theorem 4.2 is also very important for the proof of this theorem. For real quadratic congruence function fields of higher genus, there exists no direct relation between $\delta_i = \delta(\mathfrak{r}_i)$ and i. We state the equivalence in terms of polynomial time algorithms, but the proof of Theorem 7.4 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, and the DLP for real quadratic congruence function fields is at least as difficult as the DLP for elliptic curves. Known methods for solving the DLP for elliptic curves, except supersingular elliptic curves, are of exponential complexity. Note that we "shift" the DLP for a group to the DLP in a non-group.

Corollary 7.5. *The time needed to solve the discrete logarithm problem for real quadratic congruence function fields of genus* 1 *with characteristic different from* 2, 3 *is polynomially equivalent to the time needed to solve the discrete logarithm problem for elliptic curves over finite fields.*

References

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

[2] W. W. Adams & M. J. Razar, Multiples of points on elliptic curves and continued fractions. *Proc. London Math. Soc.* **41**, 1980, 481-498.

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

[4] H. Cohen, *A Course in Computation Algebraic Number Theory.* Springer, Berlin 1994.

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

[6] W. Diffie & M. E. Hellman, New directions in cryptography. *IEEE Trans. Inform. Theory* **22**, 6, 644-654, 1976.

[7] E. Friedman & L. C. Washington, On the distribution of divisor class groups of curves over finite fields. *Theorie des Nombres, Proc. Int. Number Theory Conf. Laval*, 1987, Walter de Gruyter, Berlin and New York, 227-239, 1989.

[8] A. Stein, V. Müller, & C. Thiel *Computing discrete logarithms in real quadratic congruence function fields of large genus.* Submitted.

[9] R. Scheidler, J. A. Buchmann & H. C. Williams, A key exchange protocol using real quadratic fields. *J. Cryptology* **7**, 171-199, 1994.

[10] R. Scheidler, A. Stein, & H. C. Williams, Key-exchange in real quadratic congruence function fields. *Designs, Codes and Cryptography* **7**, (1996), no. 1/2, 153-174.

[11] F. K. Schmidt, Analytische Zahlentheorie in Körpern der Charakteristik p. *Math. Zeitschr.* **33** (1931), 1-32.

[12] R. J. Schoof Quadratic fields and factorization. *Computational Methods in Number Theory* (H. W. Lenstra and R. Tijdemans, eds.,). Math. Centrum Tracts **155**, 235-286, Part II, Amsterdam 1983.

[13] D. Shanks, The Infrastructure of a Real Quadratic Field and its Applications. *Proc. 1972 Number Theory Conf.*, Boulder, Colorado, (1972), 217-224.

[14] D. Shanks, On Gauss's Class Number Problems. *Math. Comp.* **23** (1969), 151-163.

[15] J. H. Silverman, *The Arithmetic of Elliptic Curves.* Springer, New York, 1986.

[16] A. Stein & H. G. Zimmer, 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.

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

[18] A. Stein, Elliptic Congruence Function Fields. Proc. of ANTS II, Bordeaux, 1996, Lecture Notes in Computer Science **1122**, Springer (1996), 375-384.

[19] A. Stein & H. C. Williams, Baby step Giant step in Real Quadratic Function Fields. Unpublished Manuscript.

[20] H. Stichtenoth, *Algebraic Function Fields and Codes.* Springer Verlag, Berlin (1993).

[21] B. Weis & H. G. Zimmer, Artin's Theorie der quadratischen Kongruenzfunktionenkörper und ihre Anwendung auf die Berechnung der Einheiten- und Klassengruppen. *Mitt. Math. Ges. Hamburg*, Sond. **XII** (1991), no. 2.

[22] H. C. Williams & M. C. Wunderlich, On the Parallel Generation of the Residues for the Continued Fraction Algorithm. *Math. Comp.* **48** (1987), 405–423.

Andreas Stein
FB 9-Mathematik
Universität des Saarlandes
66041 Saarbrücken
Germany
e-mail: andreas@math.uni-sb.de