Theta null points of canonical lifts II [*]

Robert Carls

School of Mathematics and Statistics
University of Sydney
NSW 2006 Australia

tel: +61293515775
fax: +61293514534
email: carls@maths.usyd.edu.au

May 13, 2005

Abstract

In this article we compute equations satisfied by the theta null point of a canonical lift in the case of residue field characteristic 2.

1 Introduction

The present article follows up [1]. Theorem 2.1, our main result, states equations satisfied by the canonical theta null point of the canonical lift of an ordinary abelian variety over a perfect field of characteristic 2. The canonical theta null point is given in terms of the canonical theta structure whose existence is proven in the first part of this article (see [1, Cor. 2.2]).

According to the theory of complex multiplication solutions of the equations stated in Theorem 2.1 generate class fields. This is verified for some examples in Appendix A. We expect that solving our equations gives a 2-adic CM method similar to the one described in [2].

In Section 2 we show how our equations are related to the generalised *Arithmetic Geometric Mean* (AGM) formulas that Jean-François Mestre proposed in [6, §1.3]. Mestre derived his formulas from a transformation formula for complex analytic theta functions describing their behaviour under the doubling of the period matrix. (For the transformation formula see [3, Ch. IV, Th. 2] or [4, Ch. 7 §1].) Our formulas are computed by purely algebraic means using the *Multiplication Formula* and the *Isogeny Theorem* for algebraic theta functions

[*] This work was partially supported by the Australian Research Council grant DP0453134 and by the Spinoza grant of H.W. Lenstra.

stated in [8, §1-3]. The theory of algebraic theta functions was developed by David Mumford. We give a short overview of his ideas in Section 3.

In the year 2000 Mestre came up with a point counting algorithm for ordinary hyperelliptic curves over a finite field of characteristic 2 based on his formulas for a generalised AGM. For an exposition of his algorithm see [14, Ch. III] and [5]. One of the aims of this article is to broaden the understanding of Mestre's algorithm in order to generalise it to arbitrary residue field characteristic.

2 The main result

For general remarks about the notation see [1, §3]. Let R be a complete noetherian local ring with perfect residue field k of characteristic 2. Assume that R admits a lift σ of the 2-th power Frobenius automorphism of k. Let A be an abelian scheme over R of relative dimension g having ordinary reduction. Let $\mathcal{L}$ be an ample symmetric line bundle of degree 1 on A. Assume that $j \geq 1$ and that we are given an isomorphism

$$(\mathbb{Z}/2^j\mathbb{Z})_R^g \xrightarrow{\sim} A[2^j]^{\mathrm{et}} \tag{1}$$

where $A[2^j]^{\mathrm{et}}$ denotes the maximal étale quotient of $A[2^j]$. Suppose that A is a canonical lift. By [1, Cor. 2.2] there exists a canonical theta structure of type $(\mathbb{Z}/2^j\mathbb{Z})_R^g$ for the pair $(A, \mathcal{L}^{\otimes 2^j})$ depending on the isomorphism (1). Let $[x_u]_{u \in (\mathbb{Z}/2^j\mathbb{Z})_R^g}$ denote the theta null point of A with respect to the canonical theta structure. For the definition of the theta null point see Section 3.1.

Theorem 2.1 *There exists a square $\omega \in R^*$ such that*

$$x_u^2 = \omega \cdot \sum_{v \in (\mathbb{Z}/2\mathbb{Z})_R^g} \sigma(x_{v+u}) \cdot \sigma(x_v), \quad u \in (\mathbb{Z}/2^j\mathbb{Z})_R^g.$$

Theorem 2.1 will be proven in Section 4.1. In Appendix A we demonstrate the use of Theorem 2.1 by computing theta null points for small values of j and g. The formulas of Theorem 2.1 are related to Mestre's generalised AGM formulas in the following way. Take $j = 1$ and set $a_u^{(n+1)} = x_u^2$ and $a_u^{(n)} = \sigma(x_u)^2$. Then by Theorem 2.1 one has

$$a_u^{(n+1)} = \omega \cdot \sum_{v \in (\mathbb{Z}/2\mathbb{Z})_R^g} \sqrt{a_{v+u}^{(n)} \cdot a_v^{(n)}}, \quad u \in (\mathbb{Z}/2\mathbb{Z})_R^g.$$

These are up to a scalar the formulas that Mestre proposed for a generalised arithmetic geometric mean (see [6, §1.3]).

3 Algebraic theta functions

In this section we present the theoretical background which is necessary in order to understand the proof of Theorem 2.1. The theory of algebraic theta functions was developed by David Mumford in [8], [9] and [10]. For a detailed account to theta functions we refer to [11], [12] and [13].

3.1 Theta null points

Assume that we are given an abelian scheme A of relative dimension g over a ring R and an ample line bundle $\mathcal{L}$ on A. Let K be a finite constant commutative R-group of rank d. Assume that we are given a theta structure $\Theta : G(K) \xrightarrow{\sim} G(\mathcal{L})$. For our notation and the definition of a theta structure see [1, §4].

Theorem 3.1 *There exists a morphism*

$$A \to \mathbb{P}_R^{(K)} \tag{2}$$

which is uniquely determined by the theta structure Θ. If $\mathcal{L}$ is very ample then the morphism (2) *is a closed immersion.*

Later on in this section we will give a proof of Theorem 3.1. In the above theorem $\mathbb{P}_R^{(K)}$ denotes the homogeneous spectrum of the polynomial ring $R[\{x_u | u \in K\}]$. In the case that $R = \mathbb{Z}$ we simply write $\mathbb{P}^{(K)}$. Ordering the points of K determines an isomorphism $\mathbb{P}^{(K)} \xrightarrow{\sim} \mathbb{P}^{d-1}$ where d is the rank of K.

Definition 3.2 *The image of the zero section 0_A of A under the morphism* (2)*, denoted by $\Theta(0_A)$, is called the* theta null point *of A with respect to the theta structure Θ.*

We set $V(K) = \underline{\mathrm{Hom}}(K, \mathcal{O}_R)$ where the latter is defined to be the functor giving the functions on K. Note that $V(K)$ is a locally free $\mathcal{O}_R$-module of rank d. Now consider the representation of $G(K)$ on $V(K)$ given by

$$\big((\alpha, x, l), f\big) \mapsto \big[y \mapsto \alpha \cdot l(y) \cdot f(x+y)\big].$$

We define an action $G(\mathcal{L}) \times \pi_* \mathcal{L} \to \pi_* \mathcal{L}$ by setting

$$\big((x, \psi), s\big) \mapsto T_{-x}^*(\psi(s)).$$

By the existence of the theta structure Θ the line bundle $\mathcal{L}$ has degree d. Hence $\pi_* \mathcal{L}$ is locally free of rank d. The group $G(K)$ acts on $\pi_* \mathcal{L}$ by means of the theta structure Θ.

Lemma 3.3 *There exists an isomorphism of $G(K)$-modules*

$$\pi_* \mathcal{L} \xrightarrow{\beta} V(K)$$

uniquely determined by the theta structure Θ up to multiplication by a unit in R.

Proof. Up to isomorphism there exists only one irreducible representation of $G(K)$ such that the subgroup $\mathbb{G}_{m,R}$ acts by scalar multiplications. Every finite locally free $G(K)$-module having the latter property is a direct sum of copies of the unique irreducible one. For a proof over a field see [8, Th. 2]. The case of an arbitrary base ring is discussed in [7, Ch. V]. The $G(K)$-module $V(K)$ is irreducible. Hence a $G(K)$-module is irreducible if and only if it has rank d. We conclude that $\pi_*\mathcal{L}$ is an irreducible $G(K)$-module. This proves the existence of the isomorphism β.

In the following we will prove the uniqueness of β. Let β_1 and β_2 be $G(K)$-isomorphisms $\pi_*\mathcal{L} \xrightarrow{\sim} V(K)$. Then $\gamma = \beta_2 \circ \beta_1^{-1}$ is a $G(K)$-automorphism of $V(K)$. We claim that γ is given by a scalar multiplication. We can check this on geometric fibres. For the following we assume that R is an algebraically closed field. A decomposition of $V(K)$ into eigenspaces of γ is $G(K)$-invariant by the $G(K)$-linearity of γ. Our claim now follows from the irreducibility of $V(K)$. This finishes the proof of the lemma. □

Proof of Theorem 3.1: We claim that there exists a canonical basis of $\pi_*\mathcal{L}$ which is uniquely determined up to scalars. Let β be as in Lemma 3.3. The module $V(K)$ has a canonical basis given by the functions

$$\delta_z(x) = \begin{cases} 1, & x = z \\ 0, & x \neq z \end{cases}$$

where $z \in K$. The canonical basis of $\pi_*\mathcal{L}$ is given by the image of the basis $(\delta_z)_{z\in K}$ under β^{-1}. By general theory the latter basis determines a morphism $A \to \mathbb{P}_R^{(K)}$. By uniqueness the latter morphism does not depend on the choice of β. This completes the proof of Theorem 3.1. □

In the following we will explain how to evaluate sections of $\pi_*\mathcal{L}$ at torsion points contained in $H(\mathcal{L}) = \mathrm{Ker}(\varphi_\mathcal{L})$ where $\varphi_\mathcal{L} : A \to \mathrm{Pic}^0_{A/R}$ is defined by $x \mapsto \langle T_x^*\mathcal{L} \otimes \mathcal{L}^{-1}\rangle$ (compare [1, §4.1]). Assume we are given an isomorphism β as in Lemma 3.3 and a rigidification of $\mathcal{L}$, i.e. an isomorphism $\epsilon : 0_A^*\mathcal{L} \xrightarrow{\sim} \mathcal{O}_R$ where 0_A denotes the zero section of A. We indicate the application of the composed morphism

$$\pi_*\mathcal{L} = 0_A^*\pi^*\pi_*\mathcal{L} \xrightarrow{can} 0_A^*\mathcal{L} \xrightarrow{\epsilon} \mathcal{O}_R$$

by $(\cdot)_0$. The latter morphism allows us to evaluate sections of $\pi_*\mathcal{L}$ at zero. Let $(x,l) \in K \times K^D$ and let s be a section of $\pi_*\mathcal{L}$. Let $g = \Theta(1,x,l) \in G(\mathcal{L})$. We set

$$\Theta[s](x,l) = \left(g^{-1}s\right)_0.$$

Lemma 3.4 *There exists a unique function $q_\mathcal{L} \in V(K)$ such that*

$$\Theta[s](0,0) = \sum_{x\in K} \beta(s)(x) \cdot q_\mathcal{L}(x).$$

Proof. Consider the morphism

$$\kappa : \pi_*\mathcal{L} \to \underline{\mathrm{Hom}}(K \times K^D, \mathcal{O}_R), \quad s \mapsto \Theta[s].$$

The morphism κ is injective because its kernel is a $G(K)$-submodule of $\pi_*\mathcal{L}$. The latter module is irreducible. This implies the lemma. □

We remark that the composition of the morphism κ, as defined in the proof of Lemma 3.4, with the restriction to $V(K)$ does not preserve the $G(K)$-action. Note that by Lemma 3.4 the theta null point with respect to Θ is given by $[q_\mathcal{L}(x)]_{x\in K}$.

3.2 The Isogeny Theorem

In the following we use the notation of Section 3.1 and [1, §4]. Let $I : A \to A'$ be an isogeny of abelian schemes over a ring R. Assume that we are given ample line bundles $\mathcal{L}$ and $\mathcal{L}'$ on A and A', respectively. Suppose we are given theta structures $\Theta_A : G(K_A) \xrightarrow{\sim} G(\mathcal{L})$ and $\Theta_{A'} : G(K_{A'}) \xrightarrow{\sim} G(\mathcal{L}')$ where K_A and $K_{A'}$ are finite constant groups. Let $\alpha : I^*\mathcal{L}' \xrightarrow{\sim} \mathcal{L}$ be an isomorphism of $\mathcal{O}_A$-modules. The existence of α implies that $\mathrm{Ker}(I)$ is contained in $H(\mathcal{L})$. By [1, Prop. 4.2] the morphism α induces a section $\mathrm{Ker}(I) \to G(\mathcal{L})$ of the natural projection $G(\mathcal{L}) \to H(\mathcal{L})$. Let $\widetilde{K}$ denote the image of $\mathrm{Ker}(I)$ in $G(\mathcal{L})$. Assume that

(†) *the image of $\widetilde{K}$ under Θ_A^{-1} is of the form $\{1\} \times Z_1 \times Z_2$ with subgroups $Z_1 \le K_A$ and $Z_2 \le K_A^D$.*

By abuse of notation we define

$$Z_1^\perp = \{ \ x \in K_A \ \mid \ (\forall l \in Z_2) \ l(x) = 1 \ \}$$

and

$$Z_2^\perp = \{ \ l \in K_A^D \ \mid \ (\forall x \in Z_1) \ l(x) = 1 \ \}.$$

Note that $Z_1^\perp \times Z_2^\perp$ is the subgroup of points of $K_A \times K_A^D$ being orthogonal to $Z_1 \times Z_2$. Assume that we are given a surjective morphism of groups $\sigma : Z_1^\perp \to K_{A'}$ having kernel Z_1.

Proposition 3.5 *The theta structure Θ_A induces a theta structure $\Theta_A(\sigma)$ of type $K_{A'}$ for the pair $(A', \mathcal{L}')$ depending on the morphism σ.*

Proof. Let $G(\mathcal{L})^*$ denote the centraliser of $\widetilde{K}$ in $G(\mathcal{L})$. By [8] Proposition 2 there exists a natural isomorphism of groups

$$G(\mathcal{L})^*/\widetilde{K} \xrightarrow{\sim} G(\mathcal{L}'). \tag{3}$$

It is easily checked that the image of $G(\mathcal{L})^*$ under Θ_A^{-1} equals $\mathbb{G}_{m,R} \times Z_1^\perp \times Z_2^\perp$. The isomorphism (3) composed with the isomorphism

$$\mathbb{G}_{m,R} \times Z_1^\perp/Z_1 \times Z_2^\perp/Z_2 \xrightarrow{\sim} G(\mathcal{L})^*/\tilde{K}$$

induced by Θ_A establishes an isomorphism

$$\mathbb{G}_{m,R} \times Z_1^\perp/Z_1 \times Z_2^\perp/Z_2 \xrightarrow{\sim} G(\mathcal{L}'). \tag{4}$$

We claim that there exists a natural isomorphism

$$Z_2^\perp/Z_2 \xrightarrow{\sim} (Z_1^\perp/Z_1)^D. \tag{5}$$

To see this one has to apply the Snake Lemma to the following commutative diagram of exact sequences

$$\begin{tikzcd}
0 \arrow[r] & Z_1 \arrow[r] \arrow[d] & K_A \arrow[r] \arrow[d, "\mathrm{id}"] & (Z_2^\perp)^D \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & Z_1^\perp \arrow[r] & K_A \arrow[r, "e"] & Z_2^D \arrow[r] & 0.
\end{tikzcd}$$

Here the upper exact sequence is obtained by dualising the exact sequence

$$0 \to Z_2^\perp \to K_A^D \xrightarrow{res} K_1^D \to 0$$

and e denotes the map $x \mapsto \mathrm{e}(K_A)\big((x,1),(0,\cdot)\big)$ defined in terms of the commutator pairing e. The left hand vertical morphism is the natural inclusion. The morphism σ induces an isomorphism $\sigma_1 : K_{A'} \xrightarrow{\sim} Z_1^\perp/Z_1$. Let $\sigma_2 : K_{A'}^D \xrightarrow{\sim} Z_2^\perp/Z_2$ denote the inverse of the isomorphism that one gets by composing σ_1^D with (5). Composing the isomorphism (4) with the isomorphism $\mathrm{id} \times \sigma_1 \times \sigma_2$ we get a theta structure $\Theta(\sigma) : G(K_{A'}) \xrightarrow{\sim} G(\mathcal{L}')$. This proves the proposition. □

Note that $\Theta_A(\sigma)$ does not depend on the choice of α.

Definition 3.6 *We say that Θ_A and $\Theta_{A'}$ are I-compatible if there exists α as above, assumption (†) holds and there exists a morphism σ as above such that $\Theta_{A'} = \Theta_A(\sigma)$.*

Let π_A and $\pi_{A'}$ denote the structure maps of A and A', respectively. Since I is faithfully flat the natural morphism $\mathcal{L}' \xrightarrow{\tau} I_* I^* \mathcal{L}'$ is injective. As a consequence there exists an injective morphism $\iota : \pi'_* \mathcal{L}' \to \pi_* \mathcal{L}$ of $\mathcal{O}_R$-modules given by the composition

$$\pi'_* \mathcal{L}' \xrightarrow{\pi'_* \tau} \pi'_* I_* I^* \mathcal{L}' = \pi_* I^* \mathcal{L}' \xrightarrow{\pi_* \alpha} \pi_* \mathcal{L}.$$

The morphism ι identifies the sections of $\pi'_* \mathcal{L}'$ with those sections of $\pi_* \mathcal{L}$ which are invariant under the translations with points in the kernel of I. By Lemma 3.3 we can choose $G(K_A)$- and $G(K_{A'})$-isomorphisms $\beta_A : \pi_* \mathcal{L} \xrightarrow{\sim} V(K_A)$ and $\beta_{A'} : \pi'_* \mathcal{L}' \xrightarrow{\sim} V(K_{A'})$. We define $V_I : V(K_{A'}) \to V(K_A)$ by setting $V_I = \beta_A \circ \iota \circ \beta_{A'}^{-1}$.

Theorem 3.7 (Isogeny Theorem) *Suppose Θ_A and $\Theta_{A'}$ are I-compatible. In particular we are given a morphism σ as above such that $\Theta_{A'} = \Theta_A(\sigma)$. There exists a $\lambda \in R^*$ such that for all $f \in V(K_{A'})$ we have*

$$V_I(f)(x) = \begin{cases} 0 & , \quad x \notin Z_1^\perp \\ \lambda \cdot f\big(\sigma(x)\big), & \quad x \in Z_1^\perp \end{cases}$$

where $x \in K_A$.

For a proof of Theorem 3.7 in the case where R is a field see [8, §1, Th.4].

3.3 The Multiplication Formula

Let $A \xrightarrow{\pi} \mathrm{Spec}(R)$ be an abelian scheme and $\mathcal{L}$ an ample symmetric line bundle on A. Suppose $n \geq 2$. We set $\mathcal{L}_n = \mathcal{L}^{\otimes n}$. Assume we are given theta structures $\Theta : G(K) \xrightarrow{\sim} G(\mathcal{L})$ and $\Theta_n : G(K_n) \xrightarrow{\sim} G(\mathcal{L}_n)$. We define a morphism of groups $\epsilon_n : G(\mathcal{L}) \to G(\mathcal{L}_n)$ by setting

$$(x, \psi) \mapsto (x, \psi^{\otimes n}).$$

Note that there is a natural inclusion $H(\mathcal{L}) \hookrightarrow H(\mathcal{L}_n)$ (notation as in [1, §4]) and the multiplication-by-n on $H(\mathcal{L}_n)$ induces an epimorphism $H(\mathcal{L}_n) \to H(\mathcal{L})$.

On $\mathbb{G}_{m,R}$ the morphism ϵ_n equals the n-th powering morphism.

Next we will define a morphism of groups $\eta_n : G(\mathcal{L}_n) \to G(\mathcal{L})$ using the symmetry of $\mathcal{L}$. Assume we are given $(x, \psi) \in G(\mathcal{L}_n)$. Since $\mathcal{L}$ is symmetric there exists an isomorphism $\gamma : \mathcal{L}^{\otimes n^2} \xrightarrow{\sim} [n]^*\mathcal{L}$. Consider the composed isomorphism

$$[n]^*\mathcal{L} \xrightarrow{\gamma^{-1}} \mathcal{L}^{\otimes n^2} = \mathcal{L}_n^{\otimes n} \xrightarrow{\psi^{\otimes n}} T_x^*\mathcal{L}_n^{\otimes n} = T_x^*\mathcal{L}^{\otimes n^2} \xrightarrow{T_x^*\gamma} T_x^*[n]^*\mathcal{L} = [n]^*T_{nx}^*\mathcal{L}. \qquad (6)$$

Since nx is a point of $H(\mathcal{L})$ there exists an isomorphism $\rho : \mathcal{L} \xrightarrow{\sim} T_{nx}^*\mathcal{L}$ inducing the isomorphism (6). Since $[n]$ is faithfully flat the morphism ρ is uniquely determined. We set $\eta_n(x, \psi) = (nx, \rho)$. One can check that this is independent of the choice of γ. The map η_n restricted to $\mathbb{G}_{m,R}$ equals the n-th powering morphism.

We denote the Lagrangian structures induced by Θ and Θ_n by δ and δ_n, respectively. Suppose that $K \leq K_n$ and $K = \{nx | x \in K_n\}$. Also we assume that δ_n restricted to $K \times K^D$ equals δ. As a consequence the multiplication-by-n morphism on $K_n \times K_n^D$ induces an epimorphism $K_n \times K_n^D \to K \times K^D$, $(x, l) \mapsto (nx, l^n)$. We define morphisms $E_n : G(K) \to G(K_n)$ and $H_n : G(K_n) \to G(K)$ by setting $(\alpha, x, l) \mapsto (\alpha^n, x, l)$ and $(\alpha, x, l) \mapsto (\alpha^n, nx, l^n)$, respectively. Here we consider points of $K \times K^D$ as points of $K_n \times K_n^D$ via the natural inclusion.

Definition 3.8 *We say that the theta structures Θ_n and Θ are n-compatible if*

1. $K \leq K_n$ *and* $K = \{nx | x \in K_n\}$,
2. δ_n *restricted to* $K \times K^D$ *equals* δ,
3. $\Theta_n \circ E_n = \epsilon_n \circ \Theta$ *and* $\Theta \circ H_n = \eta_n \circ \Theta_n$.

Now assume that $n = 2$. Choose $\beta : \pi_*\mathcal{L} \xrightarrow{\sim} V(K)$ and $\beta_2 : \pi_*\mathcal{L}_2 \xrightarrow{\sim} V(K_2)$ as in Lemma 3.3.

Definition 3.9 *Let s and s' be sections of $\pi_*\mathcal{L}$. Set $f = \beta(s)$ and $f' = \beta(s')$. We define*

$$f \star f' = \beta_2(s \otimes s').$$

Theorem 3.10 (Multiplication Formula) *Suppose Θ and Θ_2 are 2-compatible theta structures. Then for all $f, f' \in V(K)$ we have*

$$(f \star f')(x) = \sum_{y \in x+K} f(x+y) \cdot f'(x-y) \cdot q_{\mathcal{L}_2}(y)$$

where $x \in K_2$.

Note that in order to obtain the formulas of Theorem 3.10 one has to normalise β and β_2 in a suitable way. For a proof of Theorem 3.10 over a field see [8, §3].

4 The proofs

In this section we will prove Theorem 2.1. Let R denote a complete noetherian local ring with perfect residue field k of characteristic $p > 0$. Assume that R admits a lift of the p-th power Frobenius automorphism of k. Let $A \xrightarrow{\pi} \mathrm{Spec}(R)$ be an abelian scheme of relative dimension g having ordinary reduction and let $\mathcal{L}$ be an ample symmetric line bundle of degree 1 on A. Let $F : A \to A^{(p)}$ denote the unique lift of the relative p-Frobenius. We denote the structure map of $A^{(p)}$ by $\pi^{(p)}$. By [1, Th. 5.1] there exists an ample symmetric line bundle $\mathcal{L}^{(p)}$ of degree 1 on $A^{(p)}$ and an isomorphism $F^*\mathcal{L}^{(p)} \xrightarrow{\sim} \mathcal{L}^{\otimes p}$. For $i \geq 0$ we set

$$\mathcal{L}_i = \mathcal{L}^{\otimes p^i}, \quad \mathcal{M}_i = \left(\mathcal{L}^{(p)}\right)^{\otimes p^i} \quad \text{and} \quad K_i = (\mathbb{Z}/p^i\mathbb{Z})^g_R.$$

Let $r \geq 1$ and assume that we are given an isomorphism

$$K_r \xrightarrow{\sim} A[p^r]^{\mathrm{et}}. \tag{7}$$

The lift of the relative p-Frobenius $F : A \to A^{(p)}$ induces an isomorphism $F[p^r]^{\mathrm{et}} : A[p^r]^{\mathrm{et}} \xrightarrow{\sim} A^{(p)}[p^r]^{\mathrm{et}}$. Composing $F[p^r]^{\mathrm{et}}$ with the isomorphism (7) we get an isomorphism

$$K_r \xrightarrow{\sim} A^{(p)}[p^r]^{\mathrm{et}}. \tag{8}$$

Now assume that A is a canonical lift. As a consequence $A^{(p)}$ is a canonical lift. By [1, Cor. 2.2] there exist for all $0 \leq j \leq r$ canonical theta structures $\Theta_j : G(K_j) \xrightarrow{\sim} G(\mathcal{L}_j)$ and $\Sigma_j : G(K_j) \xrightarrow{\sim} G(\mathcal{M}_j)$ depending on the isomorphisms (7) and (8).

Lemma 4.1 *For $0 \leq j < r$ the theta structures Θ_{j+1} and Σ_{j+1} are p-compatible to Θ_j and Σ_j, respectively.*

For the notion of p-compatibility see Definition 3.8.

Proof. We use the notation of Section 3.3. We prove the claim for the theta structures Θ_j where $0 \leq j \leq r$. For trivial reasons the theta structure Θ_1 is compatible with the theta structure Θ_0. Now let $j \geq 1$. Obviously the theta structures Θ_{j+1} and Θ_j satisfy the conditions *1.* and *2.* of Definition 3.8. We claim that

$$\Theta_{j+1} \circ E_p = \epsilon_p \circ \Theta_j \tag{9}$$

(notation as in Section 3.3). We verify equation (9) for points lying over K_j. Since the proof for points lying over K_j^D is analogous we do not present it here. By $V_j : A \to A_j$ we denote the j-fold application of the lift of the p-Verschiebung. Let $V = V_1$. Note that we have $A_j = A/K_j$ where we consider K_j as a subgroup of A via the Lagrangian level structure induced by Θ_j. Let $v_{j+1} : K_{j+1} \to G(\mathcal{L}_{j+1})$ and $v_j : K_j \to G(\mathcal{L}_j)$ be the sections of theta exact sequences over K_{j+1} and K_j induced by the canonical theta structure. By [1, Prop. 4.2] the sections v_{j+1} and v_j correspond to line bundles $\mathcal{L}^{(j+1)}$ and $\mathcal{L}^{(j)}$ on A_{j+1} and A_j together with isomorphisms $\beta_{j+1} : V_{j+1}^* \mathcal{L}^{(j+1)} \xrightarrow{\sim} \mathcal{L}_{j+1}$ and $\beta_j : V_j^* \mathcal{L}^{(j)} \xrightarrow{\sim} \mathcal{L}_j$. Let x be a point of K_j. We have $v_{j+1}(x) = (x, T_x^* \beta_{j+1} \circ \beta_{j+1}^{-1})$ and $v_j(x) = (x, T_x^* \beta_j \circ \beta_j^{-1})$. By the definition of the canonical theta structure there exists an isomorphism $\beta : V^* \mathcal{L}^{(j+1)} \xrightarrow{\sim} (\mathcal{L}^{(j)})^{\otimes p}$. Consider the isomorphism κ given by the composition

$$V_{j+1}^* \mathcal{L}^{(j+1)} = V_j^* V^* \mathcal{L}^{(j+1)} \xrightarrow{V_j^* \beta} V_j^* (\mathcal{L}^{(j)})^{\otimes p} \xrightarrow{\beta_j^{\otimes p}} \mathcal{L}_j^{\otimes p} = \mathcal{L}_{j+1}.$$

Since x lies in the kernel of V_j we have $V_j \circ T_x = V_j$ and hence $T_x^* V_j^* \beta = V_j^* \beta$. It follows that

$$\begin{aligned} \epsilon_p(v_j(x)) &= \big(x, (T_x^* \beta_j \circ \beta_j^{-1})^{\otimes p}\big) = \big(x, T_x^* \beta_j^{\otimes p} \circ \beta_j^{\otimes -p}\big) \\ &= \big(x, T_x^* \kappa \circ \kappa^{-1}\big) = \big(x, T_x^* \beta_{j+1} \circ \beta_{j+1}^{-1}\big) = v_{j+1}(x). \end{aligned}$$

The latter equality follows from the fact that β_{j+1} and κ differ by a unit. Next we will verify that

$$\Theta_j \circ H_p = \eta_p \circ \Theta_{j+1}$$

for points of $G(K_{j+1})$ lying over K_{j+1}. The proof for points lying over K_{j+1}^D is analogous. Consider a point $(1, x, 1)$ in $G(K_{j+1})$. We have $\Theta_j(H_p(1, x, 1)) = v_j(px) = (px, \tau_j)$ and $\Theta_{j+1}(1, x, 1) = v_{j+1}(x) = (x, \tau_{j+1})$ where $\tau_{j+1} = T_x^* \beta_{j+1} \circ \beta_{j+1}^{-1}$ and $\tau_j = T_{px}^* \beta_j \circ \beta_j^{-1}$. Choose an isomorphism $\gamma : \mathcal{L}_j^{\otimes p^2} \xrightarrow{\sim} [p]^* \mathcal{L}_j$. Consider the composed isomorphism

$$[p]^* \mathcal{L}_j \xrightarrow{\gamma^{-1}} \mathcal{L}_j^{\otimes p^2} = \mathcal{L}_{j+1}^{\otimes p} \xrightarrow{\tau_{j+1}^{\otimes p}} (T_x^* \mathcal{L}_{j+1})^{\otimes p} = T_x^* \mathcal{L}_j^{\otimes p^2} \xrightarrow{T_x^* \gamma} T_x^* [p]^* \mathcal{L}_j = [p]^* T_{px}^* \mathcal{L}_j.$$

We claim that the latter isomorphism is induced by τ_j. By the definition of the canonical theta structure there exists an isomorphism $\xi : F^* \mathcal{L}^{(j)} \xrightarrow{\sim} (\mathcal{L}^{(j+1)})^{\otimes p}$ where F denotes the lift of the relative p-Frobenius. The composed isomorphism

$$V_{j+1}^* (\mathcal{L}^{(j+1)})^{\otimes p} \xrightarrow{V_{j+1}^* \xi^{-1}} V_{j+1}^* F^* \mathcal{L}^{(j)} = V_j^* [p]^* \mathcal{L}^{(j)} = [p]^* V_j^* \mathcal{L}^{(j)} \xrightarrow{[p]^* \beta_j} [p]^* \mathcal{L}_j.$$

differs from $\gamma \circ \beta_{j+1}^{\otimes p}$ by a unit. We conclude that

$$\begin{aligned} T_x^* \gamma \circ \tau_{j+1}^{\otimes p} \circ \gamma^{-1} &= T_x^* (\gamma \circ \beta_{j+1}^{\otimes p}) \circ (\gamma \circ \beta_{j+1}^{\otimes p})^{-1} \\ &= T_x^* \big([p]^* \beta_j \circ V_{j+1}^* \xi^{-1}\big) \circ \big([p]^* \beta_j \circ V_{j+1}^* \xi^{-1}\big)^{-1} = T_x^* [p]^* \beta_j \circ [p]^* \beta_j^{-1} \\ &= [p]^* T_{px}^* \beta_j \circ [p]^* \beta_j^{-1} = [p]^* (T_{px}^* \beta_j \circ \beta_j^{-1}) = [p]^* \tau_j. \end{aligned}$$

Note that $T_x^* V_{j+1}^* \xi^{-1} = V_{j+1}^* \xi^{-1}$ since x is in the kernel of V_{j+1}. This completes the proof of the lemma. □

Lemma 4.2 *For all $0 \leq j < r$ the theta structures Θ_{j+1} and Σ_j are F-compatible.*

For the meaning of F-compatibility see Definition 3.6.

Proof. For the notation see Section 3.2. By [1, Th. 5.1] there exists an isomorphism $\gamma_{j+1} : F^*\mathcal{M}_j \xrightarrow{\sim} \mathcal{L}_{j+1}$. Obviously assumption (†) holds with $Z_1 = 0$ and $Z_2 = K_1^D$. It follows that $Z_2^\perp = K_{j+1}^D$. By duality we conclude that $Z_1^\perp$ coincides with the image of K_j in K_{j+1}. Take σ to be the identity. We claim that $\Sigma_j = \Theta_{j+1}(\sigma)$. Checking the claim amounts to prove the commutativity of the diagram

$$\begin{tikzcd}
G(\mathcal{L}_{j+1})/\tilde{K} \arrow[d, "\mathrm{can}"] & \mathbb{G}_{m,R} \times Z_1^\perp/Z_1 \times Z_2^\perp/Z_2 \arrow[l] \\
G(\mathcal{M}_j) & \mathbb{G}_{m,R} \times K_j \times K_j^D \arrow[l, "\Sigma_j"'] \arrow[u, "\mathrm{id}\times\sigma_1\times\sigma_2"']
\end{tikzcd}$$

where the upper horizontal arrow is induced by Θ_{j+1} and the morphisms σ_1 and σ_2 are as in the proof of Proposition 3.5. In the following we verify the commutativity of the above diagram for points of the form $(1, x, 1) \in \mathbb{G}_{m,R} \times K_j \times K_j^D$. An analogous proof exists for points of the form $(1, 0, l)$. Via the morphisms σ_1 and σ_2 we can consider $(1, x, 1)$ as a point of $G(K_{j+1})$. By definition its image under Θ_{j+1} is given by $v(x)$ where $v : K_{j+1} \to G(\mathcal{L}_{j+1})$ is the section of the theta exact sequence over K_{j+1} induced by the isomorphism $\alpha_{j+1} : V_{j+1}^*\mathcal{L}^{(j+1)} \xrightarrow{\sim} \mathcal{L}_{j+1}$ (notation as in the proof of Lemma 4.1). We have $v(x) = (y, T_y^*\alpha_{j+1} \circ \alpha_{j+1}^{-1})$ where $y \in H(\mathcal{L}_{j+1})$ is uniquely determined by the condition $F(y) = x$. On the other hand we have $\Sigma_j(1, x, 1) = w(x)$ where $w : K_j \to G(\mathcal{M}_j)$ is the section of the theta exact sequence over K_j induced by the canonical theta structure. The section w corresponds to a line bundle $\mathcal{L}^{(j-1)}$ on $A^{(j-1)}$ and an isomorphism $\beta_j : V_j^*\mathcal{L}^{(j-1)} \xrightarrow{\sim} \mathcal{M}_j$ where we set $A^{(0)} = A$ and $A^{(j)} = A/K_j$ for $j \geq 1$ (compare proof of Lemma 4.1). We have $w(x) = (x, T_x^*\beta_j \circ \beta_j^{-1})$. There exist isomorphisms

$$\xi_1 : F^*\mathcal{L}^{(j-1)} \xrightarrow{\sim} (\mathcal{L}^{(j)})^{\otimes p} \quad \text{and} \quad \xi_2 : V^*\mathcal{L}^{(j+1)} \xrightarrow{\sim} (\mathcal{L}^{(j)})^{\otimes p}.$$

Let $\xi = \xi_1^{-1} \circ \xi_2$. The isomorphism $V_j^*\xi$ induces an isomorphism

$$V_{j+1}\mathcal{L}^{(j+1)} = V_j^*V^*\mathcal{L}^{(j+1)} \xrightarrow{V_j^*\xi} V_j^*F^*\mathcal{L}^{(j-1)} = F^*V_j^*\mathcal{L}^{(j-1)}.$$

The composed isomorphism $\gamma_{j+1} \circ F^*\beta_j \circ V_j^*\xi$ differs from α_{j+1} by a unit. By the definition of the canonical isomorphism $G(\mathcal{L}_{j+1})/\tilde{K} \xrightarrow{\sim} G(\mathcal{M}_j)$ (see [8, Prop. 2]) the element in $G(\mathcal{L}_{j+1})/\tilde{K}$ corresponding to $w(x)$ is given by

$$\begin{aligned}
&\big(y, T_y^*\gamma_{j+1} \circ F^*(T_x^*\beta_j \circ \beta_j^{-1}) \circ \gamma_{j+1}^{-1}\big) \\
&\quad = \big(y, T_y^*\gamma_{j+1} \circ F^*T_x^*\beta_j \circ F^*\beta_j^{-1} \circ \gamma_{j+1}^{-1}\big) \\
&\quad = \big(y, T_y^*\gamma_{j+1} \circ T_y^*F^*\beta_j \circ F^*\beta_j^{-1} \circ \gamma_{j+1}^{-1}\big) \\
&\quad = \big(y, T_y^*(\gamma_{j+1} \circ F^*\beta_j \circ V_j^*\xi) \circ (\gamma_{j+1} \circ F^*\beta_j \circ V_j^*\xi)^{-1}\big) \\
&\quad = (y, T_y^*\alpha_{j+1} \circ \alpha_{j+1}^{-1}) = v(x).
\end{aligned}$$

This completes the proof of the lemma. □

4.1 Proof of Theorem 2.1

We use the notation introduced above. For the rest of Section 4 we assume that $p = 2$. Let 0_A and $0_{A^{(2)}}$ denote the zero sections of A and $A^{(2)}$.

Theorem 4.3 *Let $0 \leq j < r$. There exists a square $\omega \in R^*$ such that the theta null points*

$$\Theta_j(0_A) = [x_u]_{u \in K_j} \quad \text{and} \quad \Sigma_j(0_{A^{(2)}}) = [y_u]_{u \in K_j}$$

are related by the equations

$$x_u^2 = \omega \cdot \sum_{v \in K_1} y_{v+u} \cdot y_v, \quad u \in K_j.$$

Proof. We choose rigidifications $\epsilon_{\mathcal{L}_0}$ and $\epsilon_{\mathcal{M}_0}$ of the line bundle $\mathcal{L}_0$ and $\mathcal{M}_0$. The latter induce rigidifications of $\mathcal{L}_i$ and $\mathcal{M}_i$ for all $i \geq 0$. Assume that we have chosen $G(K_i)$-isomorphisms $\beta_i : \pi_* \mathcal{L}_i \xrightarrow{\sim} V(K_i)$ and $\beta_i^{(2)} : \pi_*^{(2)} \mathcal{M}_i \xrightarrow{\sim} V(K_i)$ for all $0 \leq i \leq r$ (compare Lemma 3.3). By Lemma 3.4 there exist for every $0 \leq i \leq r$ functions $q_{\mathcal{L}_i}$ and $q_{\mathcal{M}_i}$ defined on K_i with values in R giving the coordinates of the theta null point with respect to Θ_i and Σ_i. By Lemma 4.1 and Lemma 4.2 the theta structures Θ_i and Σ_i satisfy the compatibility assumptions of Theorem 3.10 and Theorem 3.7. The key ingredient in the proof of Theorem 4.3 is the following lemma.

Lemma 4.4 *Let $1 \leq j < r$. There exists an $\omega \in R^*$ such that for all $x \in K_j$ we have*

$$q_{\mathcal{L}_{j+1}}(x) = \omega \cdot q_{\mathcal{M}_j}(x).$$

Proof. Let $\mathbb{1} \in V(K_{j-1})$ be defined to be the constant function on K_{j-1} with value 1. Let $\delta_0 \in V(K_{j-1})$ be defined by

$$\delta_0(x) = \begin{cases} 1, & x = 0 \\ 0, & x \neq 0 \end{cases}$$

where $x \in K_{j-1}$. We can assume that

$$V_F(\mathbb{1} \star \delta_0) = V_F(\mathbb{1}) \star V_F(\delta_0) \tag{10}$$

where V_F is defined as in Section 3.2. First we compute the right hand side of (10). It follows by Theorem 3.7 that there exists a $\beta \in R^*$ such that for all $x \in K_j$ we have

$$V_F(\mathbb{1})(x) = \begin{cases} \beta & if \quad x \in K_{j-1} \\ 0 & if \quad x \notin K_{j-1} \end{cases} \quad \text{and} \quad V_F(\delta_0)(x) = \begin{cases} \beta & if \quad x = 0 \\ 0 & if \quad x \neq 0 \end{cases}$$

Now using Theorem 3.10 one computes

$$\big(V_F(\mathbb{1}) \star V_F(\delta_0)\big)(x) = \sum_{y \in x + K_j} V_F(\mathbb{1})(x+y) \cdot V_F(\delta_0)(x-y) \cdot q_{\mathcal{L}_{j+1}}(y)$$

$$= \begin{cases} \beta^2 \cdot q_{\mathcal{L}_{j+1}}(x) & if \quad x \in K_j \\ 0 & if \quad x \notin K_j. \end{cases}$$

for $x \in K_{j+1}$. The latter equality follows from the fact that $V_F(\mathbb{1})(x+y) \cdot V_F(\delta_0)(x-y) \neq 0$ is equivalent to $x = y$ and $2x \in K_{j-1}$. Next we compute the left hand side of equation (10). By Theorem 3.10 we have

$$(\mathbb{1} \star \delta_0)(x) = \sum_{y \in x + K_{j-1}} \mathbb{1}(x+y) \cdot \delta_0(x-y) \cdot q_{\mathcal{M}_j}(y) = q_{\mathcal{M}_j}(x)$$

for all $x \in K_j$. We conclude by Theorem 3.7 that there exists a $\gamma \in R^*$ such that

$$V_F(\mathbb{1} \star \delta_0)(x) = \begin{cases} \gamma \cdot q_{\mathcal{M}_j}(x) & if \quad x \in K_j \\ 0 & if \quad x \notin K_j. \end{cases}$$

for all $x \in K_{j+1}$. Set $\omega = \beta^{-2} \cdot \gamma$. This implies the lemma. □

Using the above lemma we can finish the proof of Theorem 4.3. The canonical basis of $V(K_j)$ is given by the functions

$$\delta_z(x) = \begin{cases} 1, & x = z \\ 0, & x \neq z \end{cases}$$

where $z \in K_j$. By Theorem 3.10 one has

$$(\delta_z \star \delta_z)(x) = \sum_{y \in x + K_j} \delta_z(x+y) \cdot \delta_z(x-y) \cdot q_{\mathcal{L}_{j+1}}(y)$$

$$= \begin{cases} \omega \cdot q_{\mathcal{M}_j}(x-z) & , \quad 2(x-z) = 0 \\ 0 & , \quad 2(x-z) \neq 0 \end{cases}$$

for all $z \in K_j$ and $x \in K_{j+1}$. The latter equality follows from Lemma 4.4 and the fact that $\delta_z(x+y) \cdot \delta_z(x-y) \neq 0$ is equivalent to $y = x - z$ and $2(x-z) = 0$. Let $\{s_u\}_{u \in K_j}$ denote the canonical R-basis of $\mathcal{L}_j$. By Lemma 3.4 we have

$$\begin{aligned} q_{\mathcal{L}_j}(u)^2 &= \Theta_j[s_u](0,0)^2 = \Theta_{j+1}[s_u \otimes s_u](0,0) \\ &= \sum_{x \in K_{j+1}} (\delta_u \star \delta_u)(x) \cdot q_{\mathcal{L}_{j+1}}(x) = \omega^2 \cdot \sum_{v \in K_1} q_{\mathcal{M}_j}(v) \cdot q_{\mathcal{M}_j}(u+v). \end{aligned}$$

The latter equality follows by the above discussion and Lemma 4.4. This finishes the proof of Theorem 4.3. □

We claim that Theorem 4.3 implies Theorem 2.1. We remark that one may have to work over a finite local étale extension of R in order to trivialise the 2-torsion of A up to the right level. However, the resulting formulas are defined over R.

Let σ denote a lift of the 2-th power Frobenius automorphism of k. Note that the pull back of $A^{(2)}$ by the morphism Spec(σ^{-1}) is the canonical lift of A_k and hence canonically isomorphic to A. Via this canonical isomorphism the pull back of the line bundle $\mathcal{M}_j$ is isomorphic to $\mathcal{L}_j$ and the theta structure Θ_j coincides with the pull back of Σ_j. We conclude that there exists a $\omega' \in R^*$ such that

$$\sigma^{-1}\big(q_{\mathcal{M}_j}(x)\big) = \omega' \cdot q_{\mathcal{L}_j}(x)$$

for all $x \in K_j$. This proves our claim and completes the proof of Theorem 2.1.

A Fields generated by theta null points

Our expectation is that the solutions of the equations of Theorem 2.1 generate Hilbert class fields of certain CM-fields. In the following we will justify our expectation by giving some examples.

A.1 Example: $g = 1$, $j = 1$

Let E be an elliptic curve over $\mathbb{Z}_q$ where $\mathbb{Z}_q$ denotes the 2-Witt vectors with values in a finite field $\mathbb{F}_q$ with $q = 2^d$. We denote the unique lift of the absolute 2-Frobenius of $\mathbb{F}_q$ to $\mathbb{Z}_q$ by σ. Assume that E has ordinary reduction $E_{\mathbb{F}_q}$ and E is a canonical lift. Let $\mathcal{L}$ denote the ample line bundle $\mathcal{O}(0_E)$. There exists a unique isomorphism $(\mathbb{Z}/2\mathbb{Z})_{\mathbb{Z}_q} \xrightarrow{\sim} E[2]^{\mathrm{et}}$. By [1, Cor. 2.2] there exists a canonical theta structure Θ of type $(\mathbb{Z}/2\mathbb{Z})_{\mathbb{Z}_q}$ for the pair $(E, \mathcal{L}^{\otimes 2})$. By Theorem 2.1 there exists a square $\omega \in \mathbb{Z}_q^*$ such that the coordinates of the theta null point $\Theta(0_E) = [x_0, x_1]$ satisfy the equations

$$x_0^2 = \omega \cdot \left(\sigma(x_0)^2 + \sigma(x_1)^2\right) \quad \text{and} \quad x_1^2 = 2\omega \cdot \sigma(x_0) \cdot \sigma(x_1). \tag{11}$$

The equations (11) imply that $x_1 \equiv 0 \bmod 2$. Hence x_0 must be a unit in $\mathbb{Z}_q$. We set $\mu = x_1/x_0$. Let $\mathbb{Q}_q$ denote the field of fractions of $\mathbb{Z}_q$.

Lemma A.1 *The curve $E_{\mathbb{Q}_q}$ can be given by the equation*

$$y^2 = x(x-1)(x-\lambda) \quad \textit{where} \quad \lambda = \left(\frac{\mu^2 - 1}{\mu^2 + 1}\right)^2.$$

Proof. We use a method described in [8, §5]. The morphism $\tau : E \rightarrow \mathbb{P}^1_{\mathbb{Z}_q}$ induced by Θ is finite locally free of rank 2 and surjective. This can be verified on fibers. The group $G(\mathcal{L}^{\otimes 2})/\mathbb{G}_{m,\mathbb{Z}_q} \cong H(\mathcal{L})$ acts on E by translation. The action of $H(\mathcal{L})$ on E extends to $\mathbb{P}^1_{\mathbb{Z}_q}$. The theta structure Θ establishes an isomorphism $(\mathbb{Z}/2\mathbb{Z})_{\mathbb{Z}_q} \times \mu_{2,\mathbb{Z}_q} \xrightarrow{\sim} H(\mathcal{L})$.

Remark A.2 *The group elements $(1,0)$ and $(0,1)$ act on $\mathbb{P}^1_{\mathbb{Z}_q}$ via the matrices*

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \textit{and} \quad \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Proof. We set

$$\delta_z(x) = \begin{cases} 1, & x = z \\ 0, & x \neq z \end{cases}$$

for $x, z \in K$. Using the definition of the action of $G(K)$ on $V(K)$ (compare Section 3.1) one computes $(1, x, 1) \circ \delta_z = \delta_{z-x}$ and $(1, 0, l) \circ \delta_z = l(z) \cdot \delta_z$. This proves the claim. □

By construction the point $\Theta(0_E) = [1, \mu]$ induces a ramification point of the morphism $\tau_{\mathbb{Q}_q} : E_{\mathbb{Q}_q} \rightarrow \mathbb{P}^1_{\mathbb{Q}_q}$. The orbit of $\Theta(0_E)$ under the group $H(\mathcal{L})$ is given by $[1, \mu]$, $[1, -\mu]$, $[\mu, 1]$ and $[-\mu, 1]$. Note that $\mu \notin \{0, \pm 1, \pm i\}$. Clearly the points in the orbit of $[1, \mu]$ give rise to ramification points of $\tau_{\mathbb{Q}_q}$. By Hurwitz's theorem there are exactly 4 ramification points of $\tau_{\mathbb{Q}_q}$. We map $[1, \mu] \mapsto [0, 1]$, $[1, -\mu] \mapsto [1, 0]$ and $[\mu, 1] \mapsto [1, 1]$ by the linear transformation

$$\begin{pmatrix} \frac{\mu^2+1}{\mu^2-1} & -\frac{\mu^2+1}{\mu(\mu^2-1)} \\ 1 & \frac{1}{\mu} \end{pmatrix}.$$

The latter transformation maps the point $[-\mu, 1]$ to $[1, \lambda]$. This completes the proof of Lemma A.1. □

Rewriting the equations (11) in terms of μ we get

$$\mu^2 \cdot \big(\sigma(\mu)^2 + 1\big) = 2\sigma(\mu). \tag{12}$$

We set $L = \mathrm{End}_{\mathbb{Z}_q}(E) \otimes \mathbb{Q}$. First we consider the case $d = 1$. In this special case equation (12) implies that

$$0 = \mu^3 + \mu - 2 = (\mu - 1) \cdot (\mu^2 + \mu + 2).$$

There exist exactly two ordinary elliptic curves over $\mathbb{F}_2$ which are twists of each other. A short calculation shows that $L = \mathbb{Q}(\sqrt{-7})$ which has class number 1. The polynomial $x^2 + x + 2$ is reducible over L. The roots $\frac{1}{2}(-1 \pm \sqrt{-7})$ both give rise to the j-invariant -15^3. The correct value for μ is uniquely determined by the condition that it reduces to zero. We remark that $\mu = 2\omega$.

Now let $d = 2$. Equation (12) implies that

$$0 = (\mu^2 + \mu + 2) \cdot (\mu^4 + 4\mu^3 + 5\mu^2 + 2\mu + 4).$$

Assume that the j-invariant of $E_{\mathbb{F}_4}$ is not equal to 1. Then $L = \mathbb{Q}(\sqrt{-15})$ which has class number 2. Over L the polynomial $x^4 + 4x^3 + 5x^2 + 2x + 4$ is reducible with irreducible factors $x^2 + 2x + \frac{1}{2}(1 \pm \sqrt{-15})$. The latter become reducible over the Hilbert class field of L.

A.2 Example: $g = 1$, $j = 2$

Let R be a complete discrete valuation ring with finite residue field $\mathbb{F}_q$ where $q = 2^d$. We denote the field of fractions of R by K. We assume that $i \in R$ with $i^2 = -1$. This implies that R is a ramified over $\mathbb{Z}_2$. Further we assume that R admits a lift σ of the 2-th power Frobenius of $\mathbb{F}_q$. Let E be an elliptic curve over R having ordinary reduction. Suppose E is a canonical lift. Let $\mathcal{L}$ denote the ample line bundle $\mathcal{O}(0_E)$. Assume we are given an isomorphism

$$(\mathbb{Z}/4\mathbb{Z})_{\mathbb{Z}_q} \xrightarrow{\sim} E[4]^{\mathrm{et}}. \tag{13}$$

By [1, Cor. 2.2] there exists a canonical theta structure Θ of type $(\mathbb{Z}/4\mathbb{Z})_{\mathbb{Z}_q}$ for the pair $(A, \mathcal{L}^{\otimes 4})$ depending on the trivialisation (13). The theta structure Θ induces a closed immersion $\tau : E_K \to \mathbb{P}^3_K$. Let $\Theta(0_E) = [x_0, x_1, x_2, x_3]$ denote the theta null point of E with respect to Θ. According to Mumford the image of τ in $\mathbb{P}^3_K$ is the intersection of the quadratic hypersurfaces

$$y_1^2 + y_3^2 = 2\lambda \cdot y_0 \cdot y_2 \quad \text{and} \quad y_0^2 + y_2^2 = 2\lambda \cdot y_1 \cdot y_3 \tag{14}$$

where $\lambda = \frac{x_1^2}{x_0 x_2}$. By symmetry the theta null point lies in the plane $y_1 = y_3$. For more details see [8, §5]. By Theorem 2.1 there exists an $\omega \in R$ such that

$$x_0^2 = \omega \cdot \big(\sigma(x_0)^2 + \sigma(x_2)^2\big) \tag{15}$$

$$x_1^2 = \omega \cdot \big(\sigma(x_1) \cdot \sigma(x_0) + \sigma(x_3) \cdot \sigma(x_2)\big) \tag{16}$$

$$x_2^2 = 2\omega \cdot \sigma(x_2) \cdot \sigma(x_0) \tag{17}$$

$$x_3^2 = \omega \cdot \big(\sigma(x_3) \cdot \sigma(x_0) + \sigma(x_1) \cdot \sigma(x_2)\big). \tag{18}$$

Now assume that $d = 1$. By the equations (15) and (17) we conclude that $4\omega^3 + \omega - 1 = 0$. Hence

$$\omega \in \left\{ \frac{1}{2}, \frac{1}{4}(-1 \pm \sqrt{-7}) \right\}.$$

Note that $\omega \neq \frac{1}{2}$. Using equation (15)-(18) one computes $\lambda = \frac{\omega}{2} \cdot (1+2\omega)^2$ where λ is as in (14). The theta null point of E is given by $[1, \omega(1+2\omega), 2\omega, \omega(1+2\omega)]$.

Acknowledgements

The results contained in this article were proven with some help of Bas Edixhoven. I want to express my gratitude to David Kohel, David Lubicz, Jean-François Mestre and Christophe Ritzenthaler for explaining me their results and commenting on my work. The examples of Appendix A were computed using the computer algebra system MAGMA.

References

[1] Robert Carls. Theta null points of canonical lifts I. unpublished, 2005.

[2] Pierrick Gaudry, Thomas Houtmann, David Kohel, Christophe Ritzenthaler, and Annegret Weng. The p-adic CM-method for genus 2. unpublished, available at http://arxiv.org/abs/math.NT/0503148, 2005.

[3] Jun-Ichi Igusa. *Theta functions.* Number 194 in Grundlehren der mathematischen Wissenschaften. Springer-Verlag, 1972.

[4] Herbert Lange and Christina Birkenhage. *Complex abelian varieties.* Number 302 in Grundlehren der mathematischen Wissenschaften. Springer-Verlag, 1992.

[5] Reynald Lercier and David Lubicz. A quasi-quadratic time algorithm for hyperelliptic curve point counting. unpublished, available at http://www.math.u-bordeaux.fr/∼lubicz, 2003.

[6] Jean-François Mestre. Algorithmes pour compter des points en petite caractéristique en genre 1 et 2. unpublished, rédigé par D. Lubicz, available at http://www.math.univ-rennes1.fr/crypto/2001-02/mestre.ps, 2002.

[7] Laurent Moret-Bailly. *Pinceaux de variétés abéliennes*, volume 129 of *Astérisque.* Société Mathématiques de France, 1985.

[8] David Mumford. On the equations defining abelian varieties I. *Inventiones Mathematicae*, 1:287–354, 1966.

[9] David Mumford. On the equations defining abelian varieties II. *Inventiones Mathematicae*, 3:75–135, 1967.

[10] David Mumford. On the equations defining abelian varieties III. *Inventiones Mathematicae*, 3:215–244, 1967.

[11] David Mumford. *Tata lectures on theta I*, volume 28 of *Progress in Mathematics.* Birkhäuser Verlag, 1983.

[12] David Mumford. *Tata lectures on theta II*, volume 43 of *Progress in Mathematics.* Birkhäuser Verlag, 1984.

[13] David Mumford. *Tata lectures on theta III*, volume 97 of *Progress in Mathematics.* Birkhäuser Verlag, 1991.

[14] Christophe Ritzenthaler. *Problèmes arithmétiques relatifs à certaines familles de courbes sur les corps finis.* PhD thesis, Université Paris 7, Denis-Diderot, France, 2003.