Higher dimensional 3-adic CM construction

Robert Carls, David Kohel, David Lubicz *

December 21, 2007

Robert Carls, David Kohel
{carls,kohel}@maths.usyd.edu.au
School of Mathematics & Statistics F07
University of Sydney NSW 2006
Australia

David Lubicz
david.lubicz@univ-rennes1.fr
CELAR
BP 7419 35174 Bruz Cedex
France

Abstract

We outline a method for the construction of genus 2 hyperelliptic curves over small degree number fields whose Jacobian has complex multiplication and good ordinary reduction at the prime 3. We prove the existence of a quasi-quadratic time algorithm for computing a canonical lift in characteristic 3 based on equations defining a higher dimensional analogue of the classical modular curve $X_0(3)$. We give a detailed description of our method in the special case of genus 2.

Keywords: CM-methods, canonical lift, theta functions, modular equations.

1 Introduction

The theory of complex multiplication yields an efficient method to produce abelian varieties over a finite field with a prescribed endomorphism ring. In the case of elliptic curves, one starts with $\mathcal{O}$ an order in an imaginary quadratic field of discriminant D. Let $h = h(D)$ be the class number of $\mathcal{O}$. It is well known [26, Ch.II] that there exist exactly h isomorphism classes of elliptic curves with complex multiplication by $\mathcal{O}$. Let j_i be their j-invariants where $i = 1, \dots h$. The usual CM-method for elliptic curves consists of computing the j_i using floating point arithmetic. One then recovers the Hilbert class polynomial

$$H_D(X) = \prod_{i=1}^{h}(X - j_i)$$

from its real approximation, using the fact that it has integer coefficients. It is usual to assess the complexity of this algorithm with respect to the size of the output. As h grows quasi-linearly with respect to D, the complexity parameter is D.

In 2002, Couveignes and Henocq [5] introduced the idea of CM construction via p-adic lifting of elliptic curves. The basis of their idea is to construct a *CM lift*, i.e. a lift of a curve over a finite field to characteristic zero such that the Jacobian of the lifted curve has complex multiplication. In the ordinary case the lifting can be done in a canonical way. In fact, one lifts a geometric invariant of the curve using modular equations. The computation of the canonical lift of an ordinary elliptic curve has drawn a considerable amount of attention in the past few years following an idea of Satoh [24, 29, 11, 7, 25, 14]. Mestre generalized Satoh's method to higher dimension using theta constants. His purely 2-adic method [15, 22] is based on a generalization of Gauss' *arithmetic*

*This work was supported by the Australian Research Council grant DP0453134.

geometric mean (AGM) formulas. In this article we present formulas which may be seen as a 3-adic analogue of Mestre's generalized AGM equations. In contrast to the latter ones, our equations do not contain information about the action of a lift of relative Frobenius on the cohomology. In order to construct the canonical lift, we apply a modified version of the lifting algorithm of Lercier and Lubicz [12] to our equations.

Next we compare our 3-adic CM method to the 2-adic CM method for genus 2 of Gaudry et al. [8], which uses the classical Richelot correspondence for canonical lifting. The latter method applies only to those CM fields K in which the prime 2 splits completely in the quadratic extension K/K_0, where K_0 is the real subfield. For any other CM field K, the reduction of the CM curve at 2 will be non-ordinary. Thus there exists no ordinary curve with CM by K to serve as input to the algorithm. The method presented in this paper exchanges this condition at 2 with the analogous condition at 3. Hence the resulting 3-adic CM method applies to a large class of CM fields which are not treatable by the prior 2-adic CM method [8].

Finally, we describe the techniques that are used in order to prove the equations introduced in the present paper. We prove our equations using the theory of algebraic theta functions which was developed by Mumford [17]. In the 3-adic arithmetic situation we make use of a canonical coordinate system on the canonical lift whose existence is proven in [2]. Our algorithm is proven by 3-adic analytic means and Serre-Tate theory.

This article is structured as follows. In Section 2 we prove equations which are satisfied by the canonical theta null points of canonical lifts of ordinary abelian varieties over a perfect field of characteristic 3. In Section 3, for lack of a suitable reference, we prove some properties of algebraic theta functions which are used in the proof of the modular equations for the prime 3. In Section 4 we describe a method for CM construction via canonical lifting of abelian surfaces in characteristic 3. In Section 5 we recall classical results about the moduli of hyperelliptic genus 2 curves and provide examples of the CM invariants of abelian surfaces and genus 2 curves.

2 Modular equations of degree 3 and level 4

In this section we prove equations which have as solutions the theta null points of the canonical lifts of ordinary abelian varieties over a perfect field of characteristic 3. The latter equations form an essential ingredient of the 3-adic CM construction which is given in Section 4. Our proof uses Mumford's formalism of *algebraic theta functions* [17]. The results of Section 2.2 cannot be obtained in a complex analytic setting. We remark that in [10] Y. Kopeliovich proves higher dimensional theta identities of degree 3 using complex analytic methods. Our purely algebraic method yields similar equations. Our set of equations is 'complete' in the sense that it defines a higher dimensional analogue of the classical modular curve $X_0(3)$.

2.1 Theta null points of 3-adic canonical lifts

For the basics about algebraic theta functions and standard notation we refer to [17]. Let R be a complete noetherian local ring with perfect residue field k of characteristic 3. Assume that there exists $\sigma \in \mathrm{Aut}(R)$ lifting the 3-rd power Frobenius automorphism of k. Let A be an abelian scheme of relative dimension g over R, which is assumed to have ordinary reduction, and let $\mathcal{L}$ be an ample symmetric line bundle of degree 1 on A. We set $Z_n = (\mathbb{Z}/n\mathbb{Z})^g_R$ for an integer $n \geq 1$. Assume that we are given a symmetric theta structure Θ_4 of type Z_4 for the pair $(A, \mathcal{L}^4)$. Let $(a_u)_{u \in Z_4}$ denote the theta null point with respect to the theta structure Θ_4. In the following we identify Z_2 with its image in Z_4 under the morphism which maps component-wise $1 \mapsto 2$. We define

$$S = \{(x, y, z) \in Z_4^3 \mid (x - 2y, x + y - z, x + y + z) \in Z_2^3\}.$$

For $(x_1, y_1, z_1), (x_2, y_2, z_2) \in S$ we denote $(x_1, y_1, z_1) \sim (x_2, y_2, z_2)$ if there exists a permutation matrix $P \in \mathbb{M}_3(\mathbb{Z})$ such that

$$(x_1 - 2y_1, x_1 + y_1 - z_1, x_1 + y_1 + z_1) = (x_2 - 2y_2, x_2 + y_2 - z_2, x_2 + y_2 + z_2)P.$$

Theorem 2.1 *Assume that A is the canonical lift of A_k. For $(x, y_1, z_1), (x, y_2, z_2) \in S$ such that $(x, y_1, z_1) \sim (x, y_2, z_2)$ one has*

$$\sum_{u \in Z_2} a^{\sigma}_{y_1+u} a_{z_1+u} = \sum_{v \in Z_2} a^{\sigma}_{y_2+v} a_{z_2+v}.$$

Proof. There exists a unique theta structure Θ_2 of type Z_2 for $(A, \mathcal{L}^2)$ which is 2-compatible with the given theta structure Θ_4 (see [17, §2,Rem.1]). Now assume that we have chosen an isomorphism

$$Z_3 \xrightarrow{\sim} A[3]^{\mathrm{et}}. \tag{1}$$

In order to do so we may have to extend locally-étale the base ring R. Note that σ admits a unique continuation to local-étale extensions. Our assumption is justified by the following observation. As we shall see lateron, the resulting theta relations have coefficients in $\mathbb{Z}$ and hence are defined over the original ring R.

By [2, Th.2.2] the isomorphism (1) determines a canonical theta structure Θ^{can}_3 of type Z_3 for $\mathcal{L}^3$. By Lemma 3.3 there exist semi-canonical product theta structures $\Theta_6 = \Theta_2 \times \Theta^{\mathrm{can}}_3$ and $\Theta_{12} = \Theta_4 \times \Theta^{\mathrm{can}}_3$ of type Z_6 and Z_{12} for $\mathcal{L}^6$ and $\mathcal{L}^{12}$, respectively. By [2, Th.5.1] and Lemma 3.2 the canonical theta structure Θ^{can}_3 is symmetric. We conclude by Lemma 3.4 that the theta structures Θ_2, Θ_4, Θ_6 and Θ_{12} are compatible in the sense of [3, §5.3]. For the following we assume that we have chosen rigidifications for the line bundles $\mathcal{L}^i$ and theta invariant isomorphisms

$$\mu_i : \pi_* \mathcal{L}^i \xrightarrow{\sim} V(Z_i) = \underline{\mathrm{Hom}}(Z_i, \mathcal{O}_R),$$

where $i = 2, 4, 6, 12$ and $\pi : A \to \mathrm{Spec}(R)$ denotes the structure morphism. Our choice determines theta functions $q_{\mathcal{L}^i} \in V(Z_i)$ which interpolate the coordinates of the theta null point with respect to Θ_i (see [17, §1]). Let $\{\delta_w\}_{w \in Z_2}$ denote the Dirac basis of the module of finite theta functions $V(Z_2)$. Let now $(x_0, y_i, z_i) \in S$ where $i = 1, 2$ and set

$$(a_i, b_i, c_i) = (x_0 - 2y_i, x_0 + y_i - z_i, x_0 + y_i + z_i).$$

Suppose that $(x_0, y_1, z_1) \sim (x_0, y_2, z_2)$, i.e. there exists a permutation matrix $P \in \mathbb{M}_3(\mathbb{Z})$ such that

$$(a_1, b_1, c_1) = (a_2, b_2, c_2)P. \tag{2}$$

For $i = 1, 2$ we set

$$S^{(i)}_{x_0} = \{(x, y, z) \in S \mid (x = x_0) \wedge (x - 2y, x + y - z, x + y + z) = (a_i, b_i, c_i)\}.$$

By Theorem 3.11 there exists a $\lambda \in R^*$ such that

$$\begin{aligned} &\big(\delta_{a_i} \star \delta_{b_i} \star \delta_{c_i}\big)(x_0) \\ &\quad = \lambda \sum_{(x,y,z) \in S^{(i)}_{x_0}} \delta_{a_i}(x - 2y)\delta_{b_i}(x + y - z)\delta_{c_i}(x + y + z) q_{\mathcal{L}^{12}}(y) q_{\mathcal{L}^4}(z) \\ &\quad = \lambda \sum_{t \in Z_2} q_{\mathcal{L}^{12}}(y_i + t) q_{\mathcal{L}^4}(z_i + t). \end{aligned} \tag{3}$$

It follows by Theorem 2.4 and Lemma 3.5 that there exists an $\alpha \in R^*$ such that

$$q_{\mathcal{L}^{12}}(z) = \alpha q_{\mathcal{L}^4}(z)^{\sigma} \tag{4}$$

for all $z \in Z_4$. Combining the equations (3) and (4) we conclude that there exists $\lambda \in R^*$ such that

$$\big(\delta_{a_i} \star \delta_{b_i} \star \delta_{c_i}\big)(x_0) = \lambda \sum_{t \in Z_2} q_{\mathcal{L}^4}(y_i + t)^{\sigma} q_{\mathcal{L}^4}(z_i + t). \tag{5}$$

The commutativity of the $\star$-product and equality (2) imply that

$$\big(\delta_{a_1} \star \delta_{b_1} \star \delta_{c_1}\big)(x_0) = \big(\delta_{a_2} \star \delta_{b_2} \star \delta_{c_2}\big)(x_0). \tag{6}$$

As a consequence of the equalities (5) and (6) we have

$$\sum_{u \in Z_2} q_{\mathcal{L}^4}(y_1 + u)^\sigma q_{\mathcal{L}^4}(z_1 + u) = \sum_{v \in Z_2} q_{\mathcal{L}^4}(y_2 + v)^\sigma q_{\mathcal{L}^4}(z_2 + v).$$

This completes the proof of Theorem 2.1. □

Note that by symmetry one has $a_u = a_{-u}$ for all $u \in Z_4$. For the sake of completeness we also give the well-known higher dimensional modular equations of level 4 which generalize Riemann's relation. Let

$$S' = \{(v, w, x, y) \in Z_4^4 \ \mid \ (v + w, v - w, x + y, x - y) \in Z_2^4\}.$$

For $(v_1, w_1, x_1, y_1), (v_2, w_2, x_2, y_2) \in S'$ we write $(v_1, w_1, x_1, y_1) \sim (v_2, w_2, x_2, y_2)$ if there exists a permutation matrix $P \in \mathbb{M}_4(\mathbb{Z})$ such that

$$(v_1 + w_1, v_1 - w_1, x_1 + y_1, x_1 - y_1) = (v_2 + w_2, v_2 - w_2, x_2 + y_2, x_2 - y_2)P.$$

Theorem 2.2 *For $(v_1, w_1, x_1, y_1), (v_2, w_2, x_2, y_2) \in S'$ such that $(v_1, w_1, x_1, y_1) \sim (v_2, w_2, x_2, y_2)$, the following equality holds*

$$\sum_{t \in Z_2} a_{v_1+t} a_{w_1+t} \sum_{s \in Z_2} a_{x_1+s} a_{y_1+s} = \sum_{t \in Z_2} a_{v_2+t} a_{w_2+t} \sum_{s \in Z_2} a_{x_2+s} a_{y_2+s}.$$

A proof of the above theorem can be found in [17, §3].

2.1.1 Theta null values in dimensions 1 and 2

In this section we make the equations of Theorem 2.1 and Theorem 2.2 explicit in the case of dimensions 1 and 2. Let $\mathbb{F}_q$ be a finite field of characteristic 3 having q elements and let $R = W(\mathbb{F}_q)$ denote the Witt vectors with values in $\mathbb{F}_q$. There exists a canonical lift $\sigma \in \mathrm{Aut}(R)$ of the 3-rd power Frobenius of $\mathbb{F}_q$. Let A be an abelian scheme over R with ample symmetric line bundle $\mathcal{L}$ of degree 1 on A.

Dimension 1. Suppose that A is a proper smooth elliptic curve over R, and let $(a_0 : a_1 : a_2 : a_3)$ be the theta null point with respect to a symmetric theta structure of type $(\mathbb{Z}/4\mathbb{Z})_R$ for $(A, \mathcal{L}^4)$ where $\mathcal{L} = \mathcal{L}(0_A)$ and 0_A denotes the zero section of A. By symmetry we have $a_1 = a_3$, and Theorem 2.2 implies that the projective point $(a_0 : a_1 : a_2)$ lies on the smooth genus 3 curve $\mathcal{A}_1(\Theta_4) \subseteq \mathrm{Proj}(\mathbb{Z}[\frac{1}{2}, x_0, x_1, x_2]) = \mathbb{P}^2_{\mathbb{Z}[\frac{1}{2}]}$ with defining equation

$$(x_0^2 + x_2^2)x_0 x_2 = 2x_1^4. \tag{7}$$

The latter classical equation is known as *Riemann's relation.* We remark that the points on $\mathcal{A}_1(\Theta_4)$ give the moduli of elliptic curves with symmetric 4-theta structure.

Now assume that A has ordinary reduction and that A is the canonical lift of $A_{\mathbb{F}_q}$. Theorem 2.1 implies that the coordinates of the projective point $(a_0 : a_1 : a_2)$ satisfy the equation

$$x_0 y_2 + x_2 y_0 = 2x_1 y_1, \tag{8}$$

where $x_i = a_i$ and $y_i = a_i^\sigma$ for $i = 0, 1, 2$.

Dimension 2. Now suppose that A has relative dimension 2 over R and that we are given a symmetric theta structure of type $(\mathbb{Z}/4\mathbb{Z})^2$ for the pair $(A, \mathcal{L}^4)$. Let $(a_{ij})_{(i,j) \in (\mathbb{Z}/4\mathbb{Z})^2}$ denote the theta null point with respect to the latter theta structure. By symmetry we have

$$a_{11} = a_{33}, \ \ a_{10} = a_{30}, \ \ a_{01} = a_{03}, \ \ a_{13} = a_{31}, \ \ a_{32} = a_{12}, \ \ a_{21} = a_{23}.$$

The 2-dimensional analogue of *Riemann's equation* (8) are the equations

$$\begin{aligned}
(x_{00}^2+x_{02}^2+x_{20}^2+x_{22}^2)(x_{00}x_{02}+x_{20}x_{22}) &= 2(x_{01}^2+x_{21}^2)^2\\
(x_{00}^2+x_{02}^2+x_{20}^2+x_{22}^2)(x_{00}x_{20}+x_{02}x_{22}) &= 2(x_{10}^2+x_{12}^2)^2\\
(x_{00}^2+x_{02}^2+x_{20}^2+x_{22}^2)(x_{00}x_{22}+x_{20}x_{02}) &= 2(x_{11}^2+x_{13}^2)^2\\
(x_{00}x_{20}+x_{02}x_{22})(x_{00}x_{22}+x_{02}x_{20}) &= 4x_{01}^2x_{21}^2\\
(x_{00}x_{02}+x_{20}x_{22})(x_{00}x_{22}+x_{02}x_{20}) &= 4x_{10}^2x_{12}^2\\
(x_{00}x_{02}+x_{20}x_{22})(x_{00}x_{20}+x_{02}x_{22}) &= 4x_{11}^2x_{13}^2\\
(x_{00}^2+x_{02}^2+x_{20}^2+x_{22}^2)x_{13}x_{11} &= (x_{12}^2+x_{10}^2)(x_{01}^2+x_{21}^2)\\
(x_{00}^2+x_{02}^2+x_{20}^2+x_{22}^2)x_{01}x_{21} &= (x_{12}^2+x_{10}^2)(x_{11}^2+x_{13}^2)\\
(x_{00}^2+x_{02}^2+x_{20}^2+x_{22}^2)x_{10}x_{12} &= (x_{01}^2+x_{21}^2)(x_{11}^2+x_{13}^2)\\
(x_{02}x_{20}+x_{00}x_{22})x_{11}x_{13} &= 2x_{01}x_{10}x_{21}x_{12}\\
(x_{20}x_{00}+x_{22}x_{02})x_{10}x_{12} &= 2x_{11}x_{13}x_{21}x_{01}\\
(x_{00}x_{02}+x_{20}x_{22})x_{21}x_{01} &= 2x_{11}x_{13}x_{10}x_{12}\\
(x_{02}x_{20}+x_{00}x_{22})(x_{01}^2+x_{21}^2) &= 2x_{10}x_{12}(x_{11}^2+x_{13}^2)\\
(x_{00}x_{02}+x_{20}x_{22})(x_{11}^2+x_{13}^2) &= 2x_{10}x_{12}(x_{01}^2+x_{21}^2)\\
(x_{02}x_{20}+x_{00}x_{22})(x_{10}^2+x_{12}^2) &= 2x_{21}x_{01}(x_{11}^2+x_{13}^2)\\
(x_{20}x_{00}+x_{22}x_{02})(x_{13}^2+x_{11}^2) &= 2x_{21}x_{01}(x_{10}^2+x_{12}^2)\\
(x_{20}x_{00}+x_{22}x_{02})(x_{21}^2+x_{01}^2) &= 2x_{11}x_{13}(x_{10}^2+x_{12}^2)\\
(x_{00}x_{02}+x_{20}x_{22})(x_{12}^2+x_{10}^2) &= 2x_{11}x_{13}(x_{01}^2+x_{21}^2)\\
x_{01}x_{21}(x_{01}^2+x_{21}^2) &= x_{10}x_{12}(x_{10}^2+x_{12}^2)\\
x_{01}x_{21}(x_{01}^2+x_{21}^2) &= x_{11}x_{13}(x_{11}^2+x_{13}^2).
\end{aligned} \tag{9}$$

By Theorem 2.2 the point $(a_{ij})_{(i,j)\in(\mathbb{Z}/4\mathbb{Z})^2}$ is a solution of the equations (9), i.e. the above equations hold for $x_{ij}=a_{ij}$. The latter equations determine a three dimensional subscheme $\mathcal{A}_2(\Theta_4)$ of the projective space

$$\mathbb{P}^9_{\mathbb{Z}[\frac{1}{2}]} = \mathrm{Proj}\big(\mathbb{Z}[\frac{1}{2}, x_{00}, x_{01}, x_{02}, x_{10}, x_{11}, x_{12}, x_{13}, x_{20}, x_{21}, x_{22}]\big).$$

The points on $\mathcal{A}_2(\Theta_4)$ give the moduli of abelian surfaces with symmetric theta structure of type $(\mathbb{Z}/4\mathbb{Z})^2$. We remark that the point

$$(a_{00}:a_{01}:a_{02}:a_{10}:a_{11}:a_{12}:a_{13}:a_{20}:a_{21}:a_{22}) \in \mathbb{P}^9_{\mathbb{Z}[\frac{1}{2}]}(R)$$

is a solution of the equations (9) if and only if the projective coordinates

$$\begin{gathered}
\big(a_{00}^2+a_{02}^2+a_{20}^2+a_{22}^2 : 2(a_{01}^2+a_{21}^2) : 2(a_{12}^2+a_{10}^2) : 2(a_{11}^2+a_{13}^2)\big),\\
\big(a_{01}^2+a_{21}^2 : a_{00}a_{02}+a_{20}a_{22} : 2a_{11}a_{13} : 2a_{10}a_{12}\big),\\
\big(a_{12}^2+a_{10}^2 : 2a_{11}a_{13} : a_{00}a_{20}+a_{02}a_{22} : 2a_{01}a_{21}\big),\\
\big(a_{11}^2+a_{13}^2 : 2a_{10}a_{12} : 2a_{01}a_{21} : a_{00}a_{22}+a_{02}a_{20}\big)
\end{gathered}$$

describe the same point in $\mathbb{P}^3_{\mathbb{Z}[\frac{1}{2}]}(R)$. In fact the above formulas define a morphism to the space of abelian surfaces with 2-theta structure which embeds in $\mathbb{P}^3_{\mathbb{Z}[\frac{1}{2}]}$. Together with the Riemann equations, the following corollary of Theorem 2.1 forms the basis of our construction algorithm for CM abelian surfaces.

Corollary 2.3 *Assume that A has ordinary reduction and that A is the canonical lift of $A_{\mathbb{F}_q}$. Let (a_{ij}) denote the theta null point of A with respect to a given symmetric 4-theta structure. Then the coordinates of the point*

$$(a_{00}:a_{01}:a_{02}:a_{10}:a_{11}:a_{12}:a_{13}:a_{20}:a_{21}:a_{22}) \in \mathbb{P}^9_{\mathbb{Z}[\frac{1}{2}]}(R)$$

satisfy the following relations

$$\begin{aligned}
x_{00}y_{02}+x_{02}y_{00}+x_{20}y_{22}+x_{22}y_{20}-2(x_{01}y_{01}+x_{21}y_{21}) &= 0\\
x_{00}y_{20}+x_{20}y_{00}+x_{02}y_{22}+x_{22}y_{02}-2(x_{10}y_{10}+x_{12}y_{12}) &= 0\\
x_{00}y_{22}+x_{22}y_{00}+x_{02}y_{20}+x_{20}y_{02}-2(x_{13}y_{13}+x_{11}y_{11}) &= 0\\
x_{01}y_{21}+x_{21}y_{01}-(x_{12}y_{10}+x_{10}y_{12}) &= 0\\
x_{01}y_{21}+x_{21}y_{01}-(x_{11}y_{13}+x_{13}y_{11}) &= 0,
\end{aligned} \tag{10}$$

where $x_{ij} = a_{ij}$ *and* $y_{ij} = a_{ij}^{\sigma}$.

2.2 Galois properties of the canonical theta structure

For our notation and standard definitions we refer to [17] and [2]. Let R be a complete noetherian local ring with perfect residue field k of characteristic $p > 2$. Suppose that we are given an abelian scheme A over R which has ordinary reduction. Let $\mathcal{L}$ be an ample symmetric line bundle of degree 1 on A. We set $q = p^d$ where $d \geq 1$ is an integer. Assume that there exists a $\sigma \in \mathrm{Aut}(R)$ lifting the q-th power Frobenius automorphism of k. Recall that there exists a canonical lift $F : A \to A^{(q)}$ of the relative q-Frobenius morphism and a canonical ample symmetric line bundle $\mathcal{L}^{(q)}$ of degree 1 on $A^{(q)}$ such that $F^*\mathcal{L}^{(q)} \cong \mathcal{L}^q$ (see [2, §5]). Let $A^{(\sigma)}$ be defined by the Cartesian diagram

$$\begin{tikzcd} A^{(\sigma)} \arrow[r, "\mathrm{pr}"] \arrow[d] & A \arrow[d] \\ \mathrm{Spec}(R) \arrow[r, "\mathrm{Spec}(\sigma)"] & \mathrm{Spec}(R), \end{tikzcd} \tag{11}$$

where the right hand vertical arrow is the structure morphism. Let $\mathcal{L}^{(\sigma)}$ be the pull back of $\mathcal{L}$ along the morphism $\mathrm{pr} : A^{(\sigma)} \to A$ which is defined by the diagram (11).

Now let $n \geq 1$ be a natural number such that $(n,p) = 1$, i.e. the numbers n and p are coprime. Assume that we are given a symmetric theta structure Θ_n of type $Z_n = (\mathbb{Z}/n\mathbb{Z})_R^g$ for $\mathcal{L}^n$ where $g = \dim_R(A)$. We denote by $\mathcal{L}_n^{(\sigma)}$ the n-th power of $\mathcal{L}^{(\sigma)}$. We obtain a theta structure $\Theta_n^{(\sigma)}$ for $\mathcal{L}_n^{(\sigma)}$ on $A^{(\sigma)}$ by extension of scalars along $\mathrm{Spec}(\sigma)$ applied to the theta structure $\Theta_n : G(Z_n) \xrightarrow{\sim} G(\mathcal{L}_n)$ and by chaining with the natural isomorphism $Z_n \xrightarrow{\sim} Z_{n,\sigma}$ and the inverse of its dual. Assume that A is the canonical lift of A_k. Our assumption implies that the abelian schemes $A^{(q)}$ and $A^{(\sigma)}$ are canonical lifts which are canonically isomorphic over the residue field k. In the following we will assume that the special fibers of $A^{(q)}$ and $A^{(\sigma)}$ are indeed equal. There exists a canonical isomorphism $\tau : A^{(q)} \xrightarrow{\sim} A^{(\sigma)}$ over R lifting the identity on special fibers.

We claim that $\tau^*\mathcal{L}^{(\sigma)} \cong \mathcal{L}^{(q)}$. We set $\mathcal{M} = \tau^*\mathcal{L}^{(\sigma)} \otimes (\mathcal{L}^{(q)})^{-1}$. It follows by the definition of $\mathcal{L}^{(q)}$ that the class of $\mathcal{M}$ reduces to the trivial class. Note that $\tau^*\mathcal{L}^{(\sigma)}$ is symmetric. By [2, Th.5.1] also the line bundle $\mathcal{L}^{(q)}$ is symmetric. As a consequence the line bundle $\mathcal{M}$ is symmetric and gives an element of $\mathrm{Pic}^0_{A^{(q)}/R}[2](R)$. We observe that the group $\mathrm{Pic}^0_{A^{(q)}/R}[2]$ is finite étale because of the assumption $p > 2$. We conclude by the connectedness of the ring R that the class of $\mathcal{M}$ is the trivial class. Hence our claim follows.

By the above discussion there exists an isomorphism $\gamma : \tau^*\mathcal{L}^{(\sigma)} \xrightarrow{\sim} \mathcal{L}^{(q)}$. We define a $\mathbb{G}_{m,R}$-invariant morphism of theta groups $\tau^* : G(\mathcal{L}^{(\sigma)}) \to G(\mathcal{L}^{(q)})$ by setting $(x,\varphi) \mapsto \left(y, T_y^*\gamma \circ \tau^*\varphi \circ \gamma^{-1}\right)$ where $y = \tau^{-1}(x)$ and $\varphi : \mathcal{L}^{(\sigma)} \xrightarrow{\sim} T_x\mathcal{L}^{(\sigma)}$. Obviously, our definition is independent of the choice of γ. For trivial reasons the morphism τ^* gives an isomorphism.

Theorem 2.4 *There exists a canonical theta structure* $\Theta_n^{(q)}$ *of type* Z_n *for* $\mathcal{L}_n^{(q)}$ *depending on* Θ_n *such that*

$$\tau^* \circ \Theta_n^{(\sigma)} = \Theta_n^{(q)}. \tag{12}$$

Proof. Assume that we have chosen an isomorphism

$$Z_q = (\mathbb{Z}/q\mathbb{Z})_R^g \xrightarrow{\sim} A[q]^{\mathrm{et}}, \tag{13}$$

where $A[q]^{\mathrm{et}}$ denotes the maximal étale quotient of $A[q]$. In order to do so we may have to extend R locally-étale. By [2, Th.2.2] there exists a canonical theta structure Θ_q^{can} of type Z_q for the pair $\left(A, \mathcal{L}^q\right)$ depending on the isomorphism (13). We remark that the canonical theta structure is symmetric by [2, Th.5.1] and Lemma 3.2. By Lemma 3.3 there exists a semi-canonical symmetric product theta structure $\Theta_{nq} = \Theta_n \times \Theta_q^{\mathrm{can}}$ of type $Z_{nq} = (\mathbb{Z}/nq\mathbb{Z})_R^g$ for the pair $\left(A, \mathcal{L}_{nq}\right)$ where $\mathcal{L}_{nq} = \mathcal{L}^{\otimes nq}$. It follows from [3, Prop.5.3] that the theta structure Θ_{nq} descends along the Frobenius lift F to a canonical theta structure $\Theta_n^{(q)}$ for $\mathcal{L}_n^{(q)}$. We choose $\Theta_n^{(q)} = \Theta_{nq}(\mathrm{id})$ where our notation is as in [3, §5.2]. In the following we will prove that $\Theta_n^{(q)}$ has the desired pull back property (12).

First we check the pull back property for the induced Lagrangian structures. Let δ_n, $\delta_n^{(q)}$ and $\delta_n^{(\sigma)}$ be the Lagrangian structures which are induced by Θ_n, $\Theta_n^{(q)}$ and $\Theta_n^{(\sigma)}$, respectively. We claim that

$$\delta_n^{(\sigma)} = \tau \circ \delta_n^{(q)}. \tag{14}$$

As $\Theta_n^{(q)} = \Theta_{nq}(\mathrm{id})$ (notation as in [3, §5.2]) the restriction of the Lagrangian structure $\delta_n^{(q)}$ to Z_n equals the restriction of $F \circ \delta_n$. As a consequence the restrictions of the morphisms $\tau \circ \delta_n^{(q)}$ and $\delta_n^{(\sigma)}$ coincide on the special fiber. By general theory the reduction functor on the category of finite étale schemes over R gives an equivalence of categories. We conclude that the equality (14) restricted to Z_n is true over R. The equality for Z_n^D can be proven analogously. Note that Z_n^D is étale because of the assumption $(n,p)=1$. Hence the claim follows.

It remains to show, on top of Lagrangian structures, the equality of theta structures as claimed in (12). By [2, Prop.4.5] the theta structures Θ_n, $\Theta_n^{(\sigma)}$ and $\Theta_n^{(q)}$ give rise to sections s, $s^{(\sigma)}$ and $s^{(q)}$ of theta exact sequences

$$\begin{tikzcd}
0 \arrow[r] & \mathbb{G}_{m,R} \arrow[r] \arrow[dd, "\mathrm{id}"] & G(\mathcal{L}_n^{(q)}) \arrow[rr] & & H(\mathcal{L}_n^{(q)}) \arrow[r] \arrow[dd, "\tau"] & 0 \\
 & & & Z_n \arrow[ul, "s^{(q)}"'] \arrow[ur, "\delta_n^{(q)}"] \arrow[dl, "s^{(\sigma)}"] \arrow[dr, "\delta_n^{(\sigma)}"] & & \\
0 \arrow[r] & \mathbb{G}_{m,R} \arrow[r] & G(\mathcal{L}_n^{(\sigma)}) \arrow[rr] \arrow[uu, "\tau^*"] & & H(\mathcal{L}_n^{(\sigma)}) \arrow[r] & 0.
\end{tikzcd} \tag{15}$$

We claim that the diagram (15) commutes. By definition, the squares of the above diagram commute. By equation (14) the right hand triangle commutes. It remains to show that

$$\tau^* \circ s^{(\sigma)} = s^{(q)}. \tag{16}$$

The difference of $\tau^* \circ s^{(\sigma)}$ and $s^{(q)}$ gives a point $\varphi \in \mathrm{Hom}_R(Z_n, \mathbb{G}_{mR}) = \mu_{n,R}(R)$. It suffices to show that the point φ reduces to the neutral element of $\mu_{n,k}$, because the group $\mu_{n,R}$ is étale and the ring R is connected. In the following we prove that φ has trivial reduction. Consider the diagram

$$\begin{tikzcd}
G(\mathcal{L}_n) \arrow[r, "\epsilon_q"] & G(\mathcal{L}_{nq}) & G(\mathcal{L}_{nq})^* \arrow[l, hook'] \arrow[r] & G(\mathcal{L}_{nq})^*/\tilde{K} \arrow[r, "\mathrm{can},F"] & G(\mathcal{L}_n^{(q)}) \\
G(Z_n) \arrow[r, "E_q"] \arrow[u, "\Theta_n"] & G(Z_{nq}) \arrow[u, "\Theta_{nq}"] & \mathbb{G}_{m,R} \times Z_n \times Z_{nq}^D \arrow[l, hook'] \arrow[r] \arrow[u, "\cong"'] & \mathbb{G}_{m,R} \times Z_n \times (Z_{nq}^D/K) \arrow[r] \arrow[u, "\cong"'] & G(Z_n) \arrow[u, "\Theta_n^{(q)}"']
\end{tikzcd}$$

where E_q and ϵ_q are defined as in [3, §5.3], $K = \mathrm{Ker}(F)$ and $\tilde{K}$ is a canonical lift of K to the theta group $G(\mathcal{L}_{nq})$. The group $G(\mathcal{L}_{nq})^*$ is defined as the centralizer of $\tilde{K}$ in $G(\mathcal{L}_{nq})$. By Lemma 3.4 the left hand square of the above diagram is commutative. The lift $\tilde{K}$ is induced by some isomorphism $\alpha : F^*\mathcal{L}_n^{(q)} \xrightarrow{\sim} \mathcal{L}_{nq}$. Let $x \in Z_n$, $y = \delta_n(x,1)$ and $z = \delta_n^{(q)}(x,1)$. Suppose that $s(x) = \Theta_n(1,x,1) = (y, \psi_y)$ and $s^{(q)}(x) = \Theta_n^{(q)}(1,x,1) = (z, \gamma_z)$. Note that $z = F(y)$. It follows by the commutativity of the above diagram that

$$\psi_y^{\otimes q} = T_y^* \alpha \circ F^* \gamma_z \circ \alpha^{-1}. \tag{17}$$

Equation (17) says in down-to-earth terms that, on the special fiber, the isomorphism γ_z is the pull back of ψ_y under the isomorphism $\mathrm{pr} : A^{(\sigma)} \to A$ where the latter is defined by the diagram

(11). This proves that the above character φ is trivial on the special fibre. This proves the equality (16) and hence the diagram (15) is commutative. The proof for Z_n^D is analogous.

We remark that the equality (12) implies by means of descent that $\Theta_n^{(q)}$ is defined over R. This completes the proof of the theorem. □

3 On the theory of algebraic theta functions

In this section we prove some basic facts about algebraic theta functions which are needed in the proof of Theorem 2.1. These results are absent from the literature. For an introduction to algebraic theta functions we refer to [17].

3.1 Symmetric theta structures

In this section we recall the notion of a *symmetric theta structure*. The symmetry turns out to be an essential ingredient in the proof of the theta relations of Theorem 2.1. We give a characterization of the symmetry of a theta structure in terms of the symmetry of the associated line bundles. This characterization is not obvious from the definitions given in [17, §2]. The results of this section imply that the canonical theta structure, whose existence is proven in [2], is a symmetric theta structure. Note that our definition of symmetry is weaker than the one given in [17, §2].

Let A be an abelian scheme over a ring R and let $\mathcal{L}$ be a line bundle on A. Consider the morphism

$$\varphi_{\mathcal{L}} : A \to \mathrm{Pic}^0_{A/R}, \;\; x \mapsto \langle T_x^* \mathcal{L} \otimes \mathcal{L}^{-1} \rangle$$

where $\langle \cdot \rangle$ denotes the class in $\mathrm{Pic}^0_{A/R}$. We denote the kernel of $\varphi_{\mathcal{L}}$ by $A[\mathcal{L}]$. The line bundle $\mathcal{L}$ is called *symmetric* if $[-1]^* \mathcal{L} \cong \mathcal{L}$.

Now assume that we are given an isomorphism $\psi : \mathcal{L} \xrightarrow{\sim} [-1]^* \mathcal{L}$. We denote the theta group of the line bundle $\mathcal{L}$ by $G(\mathcal{L})$. Let $(x, \varphi) \in G(\mathcal{L})$, where $x \in A[\mathcal{L}]$ and $\varphi : \mathcal{L} \xrightarrow{\sim} T_x^* \mathcal{L}$ is an isomorphism, and let τ_φ denote the composed isomorphism

$$\mathcal{L} \xrightarrow{\psi} [-1]^* \mathcal{L} \xrightarrow{[-1]^* \varphi} [-1]^* T_x^* \mathcal{L} = T_{-x}^* [-1]^* \mathcal{L} \xrightarrow{T_{-x}^* \psi^{-1}} T_{-x}^* \mathcal{L}.$$

One defines a morphism $\delta_{-1} : G(\mathcal{L}) \to G(\mathcal{L})$ by setting $\delta_{-1}(x, \varphi) = (-x, \tau_\varphi)$. We remark that the definition of τ_φ does not depend on the choice of the isomorphism ψ. Obviously δ_{-1} is an automorphism of order 2 of the group $G(\mathcal{L})$.

Let K be a finite constant group over R. We define an automorphism D_{-1} of the standard theta group $G(K) = \mathbb{G}_{m,R} \times K \times K^D$ by mapping $(\alpha, x, l) \mapsto (\alpha, -x, l^{-1})$. Assume now that we are given a theta structure $\Theta : G(K) \xrightarrow{\sim} G(\mathcal{L})$.

Definition 3.1 *The theta structure Θ is called* symmetric *if the following equality holds*

$$\Theta \circ D_{-1} = \delta_{-1} \circ \Theta. \tag{18}$$

Note that we do not assume that the line bundle $\mathcal{L}$ is totally symmetric as it is done in [17, §2]. In the following we will give a necessary and sufficient condition for a theta structure to be symmetric. Recall (see [2, §4]) that the theta structure Θ corresponds to a Lagrangian structure of type K and isomorphisms

$$\alpha_K : I_K^* \mathcal{M}_K \xrightarrow{\sim} \mathcal{L} \quad \text{and} \quad \alpha_{K^D} : I_{K^D}^* \mathcal{M}_{K^D} \xrightarrow{\sim} \mathcal{L},$$

where $I_K : A \to A_K$ and $I_{K^D} : A \to A_{K^D}$ are isogenies with kernel K and K^D, and $\mathcal{M}_K$ and $\mathcal{M}_{K^D}$ are line bundles on A_K and A_{K^D}, respectively.

Lemma 3.2 *The theta structure Θ is symmetric if and only if the line bundles $\mathcal{M}_K$ and $\mathcal{M}_{K^D}$ are symmetric.*

Proof. We prove that the equality (18) holds on the image of the morphism

$$s_K : K \to G(K), x \mapsto (1, x, 1)$$

if and only if the line bundle $\mathcal{M}_K$ is symmetric. An analogous proof exists for the dual construction. Consider the following diagram

$$\begin{tikzcd}
A[\mathcal{L}] & G(\mathcal{L}) \arrow[l, "\mathrm{proj}"'] \arrow[r, "\delta_{-1}"] & G(\mathcal{L}) \\
K \arrow[u, "j"] \arrow[r, "s_K"] & G(K) \arrow[u, "\Theta"] \arrow[r, "D_{-1}"] & G(K). \arrow[u, "\Theta"]
\end{tikzcd}$$

Here the morphism j denotes the inclusion induced by the Lagrangian structure, which is part of the theta structure Θ. By [2, Prop.4.2 and Prop.4.5] we have $\Theta(1, x, 1) = \big(j(x), T^*_{j(x)}\alpha_K \circ \alpha_K^{-1}\big)$. We conclude that

$$\delta_{-1}\big(\Theta(1, x, 1)\big) = \Big(-j(x), T^*_{-j(x)}\psi^{-1} \circ [-1]^*(T^*_{j(x)}\alpha_K \circ \alpha_K^{-1}) \circ \psi\Big)$$

where $\psi : \mathcal{L} \xrightarrow{\sim} [-1]^*\mathcal{L}$ is an isomorphism as above. On the other hand one has

$$\Theta\big(D_{-1}(1, x, 1)\big) = \big(- j(x), T^*_{-j(x)}\alpha_K \circ \alpha_K^{-1}\big).$$

Hence the equation (18) restricted to elements of the form $(1, x, 1)$ translates as

$$T^*_{-j(x)}\psi^{-1} \circ [-1]^*(T^*_{j(x)}\alpha_K \circ \alpha_K^{-1}) \circ \psi = T^*_{-j(x)}\alpha_K \circ \alpha_K^{-1}.$$

The latter equality is equivalent to

$$[-1]^*\alpha_K^{-1} \circ \psi \circ \alpha_K = T^*_{-j(x)}([-1]^*\alpha_K^{-1} \circ \psi \circ \alpha_K).$$

The latter equality means that the composed isomorphism

$$I_K^*\mathcal{M}_K \overset{\alpha_K}{\to} \mathcal{L} \overset{\psi}{\to} [-1]^*\mathcal{L} \overset{[-1]^*\alpha_K^{-1}}{\longrightarrow} [-1]^*I_K^*\mathcal{M}_K = I_K^*[-1]^*\mathcal{M}_K$$

is invariant under $T^*_{-j(x)}$ for all $x \in K$. This is true if and only if this isomorphism equals the pull back of an isomorphism $\mathcal{M}_K \xrightarrow{\sim} [-1]^*\mathcal{M}_K$ along I_K. Thus the lemma is proven. $\square$

3.2 Product theta structures

The construction of *product theta structures* is considered as known to the experts. But the reader should be aware of the fact that a product theta structure of given theta structures does not always exist. In this section we clarify the situation by proving the existence of a product theta structure under a reasonable coprimality assumption. We provide detailed proofs because of the lack of a suitable reference.

Let A be an abelian scheme of relative dimension g over a ring R and let $\mathcal{L}$ be an ample symmetric line bundle of degree 1 on A. For an integer $n \geq 1$ we set $Z_n = (\mathbb{Z}/n\mathbb{Z})^g_R$. Now let $n, m \geq 1$ be integers such that $(n, m) = 1$, i.e. the numbers n and m are coprime. Assume we are given theta structures

$$\Theta_n : G(Z_n) \xrightarrow{\sim} G(\mathcal{L}^n) \quad \text{and} \quad \Theta_m : G(Z_m) \xrightarrow{\sim} G(\mathcal{L}^m).$$

We consider Z_n and Z_m as subgroups of Z_{nm} via the morphisms that map component-wise $1 \mapsto m$ and $1 \mapsto n$, respectively.

Lemma 3.3 *There exists a natural product theta structure*

$$\Theta_{nm} : G(Z_{nm}) \xrightarrow{\sim} G(\mathcal{L}^{nm})$$

depending on the theta structures Θ_n *and* Θ_m.

Proof. Let ϵ_n, ϵ_m, E_n, E_m, η_n, η_m, H_n and H_m be defined as in [3, §5.3]. We claim that for all $g \in G(\mathcal{L}^n)$ and $h \in G(\mathcal{L}^m)$ we have

$$\epsilon_n(h)\epsilon_m(g) = \epsilon_m(g)\epsilon_n(h), \tag{19}$$

where the product is taken in $G(\mathcal{L}^{nm})$. Let δ_n and δ_m denote the Lagrangian structures that are induced by Θ_n and Θ_m. We set $\delta_{nm} = \delta_n \times \delta_m$. Condition (19) is equivalent to

$$\mathrm{e}_{\mathcal{L}^{nm}}\big(\delta_{nm}(x_g, l_g), \delta_{nm}(x_h, l_h)\big) = 1,$$

where the elements $\delta_{nm}(x_g, l_g)$ and $\delta_{nm}(x_h, l_h)$ are the images of $\epsilon_m(g)$ and $\epsilon_n(h)$, respectively, under the natural projection $G(\mathcal{L}^{nm}) \to H(\mathcal{L}^{nm})$. The vanishing of the commutator pairing follows from the bilinearity and the assumption $(n, m) = 1$. This proves the above claim. As a consequence there exists a canonical morphism of groups

$$\epsilon : G(\mathcal{L}^n) \times G(\mathcal{L}^m) \to G(\mathcal{L}^{nm}) \quad \text{given by} \quad (g, h) \mapsto \epsilon_m(g)\epsilon_n(h).$$

Because of our assumption $(n, m) = 1$ the subgroup $C = \ker(\epsilon)$ is contained in the subtorus $\mathbb{G}_{m,S} \times \mathbb{G}_{m,S}$ of $G(\mathcal{L}^n) \times G(\mathcal{L}^m)$. In the following we will prove that ϵ is surjective. Consider the diagram

$$\begin{tikzcd}
G(\mathcal{L}^n) \times G(\mathcal{L}^m) \arrow[r, "\epsilon"] \arrow[d, "\pi_n \times \pi_m"'] & G(\mathcal{L}^{nm}) \arrow[d, "\pi"] \\
H(\mathcal{L}^n) \times H(\mathcal{L}^m) \arrow[r, "\mathrm{can}"] \arrow[u, bend right, "s"'] & H(\mathcal{L}^{nm})
\end{tikzcd}$$

where π and $\pi_n \times \pi_m$ denote the natural projections. Let s be the section of $\pi_n \times \pi_m$ induced by the theta structures Θ_n and Θ_m. We have $\pi \circ \epsilon = \pi_n \times \pi_m$ (up to canonical isomorphism). As a consequence we have $\pi \circ \epsilon \circ s = (\pi_n \times \pi_m) \circ s = \mathrm{id}$. We conclude that $\pi \circ \epsilon \circ s \circ \pi = \pi$. Let $g \in G(\mathcal{L}^{nm})$. Then by the latter equality the group element $\epsilon(s(\pi(g)))$ differs from g by a unit. Hence the morphism ϵ maps a suitable multiple of $s(\pi(g))$ to g. This implies the surjectivity of ϵ. As a consequence ϵ induces an isomorphism

$$\tilde{\epsilon} : \big(G(\mathcal{L}^n) \times G(\mathcal{L}^m)\big)/C \to G(\mathcal{L}^{nm})$$

By the same reasoning as above one can define a natural morphism $E : G(Z_n) \times G(Z_m) \to G(Z_{nm})$, and it is readily verified that the induced morphism $\tilde{E} : \big(G(Z_n) \times G(Z_m)\big)/C \to G(Z_{nm})$ is an isomorphism of groups. Let Θ_{nm} denote the composed isomorphism

$$G(Z_{nm}) \xrightarrow{\tilde{E}^{-1}} \big(G(Z_n) \times G(Z_m)\big)/C \xrightarrow{\Theta_n \times \Theta_m} \big(G(\mathcal{L}^n) \times G(\mathcal{L}^m)\big)/C \xrightarrow{\tilde{\epsilon}} G(\mathcal{L}^{nm}).$$

The morphism Θ_{nm} establishes the theta structure whose existence is claimed in the lemma. □

Now let Θ_{nm} be as in Lemma 3.3 and define the m-compatibility of theta structures as in [3, §5.3].

Lemma 3.4 *Assume that Θ_n is symmetric. Then Θ_{nm} is m-compatible with Θ_n.*

Proof. Let ϵ_n, ϵ_m, E_n, E_m, η_n, η_m, H_n and H_m be defined as in [3, §5.3]. Note that by the definition of Θ_{nm} there is an equality $\Theta_{nm} \circ E_m = \epsilon_m \circ \Theta_n$. It remains to check that $\eta_m \circ \Theta_{nm} = \Theta_n \circ H_m$. In other words, we have to prove that

$$\Theta_n \circ H_m \circ E_m = \eta_m \circ \epsilon_m \circ \Theta_n \quad \text{and} \quad \Theta_n \circ H_m \circ E_n = \eta_m \circ \epsilon_n \circ \Theta_m. \tag{20}$$

Using the definition we compute $H_m(E_n(\alpha, x, l)) = (\alpha^{nm}, 0, 1)$. As $(n, m) = 1$, it follows that the image of $\eta_m \circ \epsilon_n$ is contained in $\mathbb{G}_{m,R}$. Hence the right hand equation in (20) is a consequence of the $\mathbb{G}_{m,R}$-equivariance of Θ_n and Θ_m. It remains to prove the left hand equation. We have

$$\eta_m \circ \epsilon_m = \delta_m \quad \text{and} \quad H_m \circ E_m = D_m \tag{21}$$

where D_m denotes the map $G(Z_n) \to G(Z_n), (\alpha, x, l) \mapsto (\alpha^{m^2}, mx, l^m)$ and $\delta_m : G(\mathcal{L}^n) \to G(\mathcal{L}^n)$ is given by

$$g \mapsto g^{(m^2+m)/2} \cdot \delta_{-1}(g)^{(m^2-m)/2}.$$

Here δ_{-1} is defined as in Section 3.1. The right hand equation in (21) follows by expanding the definitions. The left hand equation in (21) is proven in [17, §2, Prop.5]. A straight forward calculation yields that for all $g \in G(Z_n)$ one has

$$D_m(g) = g^{(m^2+m)/2} \cdot D_{-1}(g)^{(m^2-m)/2}. \tag{22}$$

The left hand equality in (20) is implied by the equalities (21) and (22) using the assumption that Θ_n is symmetric, i.e. equation (18) holds. This completes the proof of the lemma. □

3.3 Descent of theta structures by isogeny

In this section we prove some lemma which forms an important ingredient of the proof of Theorem 2.1. The lemma is about special theta relations which are induced by descent along isogenies. A proof of this key lemma in terms of algebraic theta functions is absent from the literature. In the following we use the notion of compatibility as defined in [3, §5.2-5.3].

Let R be a local ring, and let $\pi_A : A \to \mathrm{Spec}(R)$ and $\pi_B : B \to \mathrm{Spec}(R)$ be abelian schemes of relative dimension g. We set $Z_n = (\mathbb{Z}/n\mathbb{Z})^g_R$ for an integer $n \geq 1$. As usual, we consider Z_n as embedded in Z_{mn} via the morphism that maps component-wise $1 \mapsto n$. Let $\mathcal{M}$ be an ample symmetric line bundle on B. Suppose that we are given 2-compatible theta structures $\Sigma_j : G(Z_{jm}) \xrightarrow{\sim} G(\mathcal{M}^j)$ for some $m \geq 1$, where $j \in \{1, 2\}$. Let $F : A \to B$ be an isogeny of degree d^g. Assume that there exists an ample symmetric line bundle $\mathcal{L}$ on A such that $F^*\mathcal{M} \cong \mathcal{L}$. Now assume that we are given 2-compatible theta structures $\Theta_j : G(Z_{jmd}) \xrightarrow{\sim} G(\mathcal{L}^j)$ such that Θ_j and Σ_j are F-compatible. By general theory there exist theta group equivariant isomorphisms

$$\mu_j : \pi_{A,*}\mathcal{L}^j \xrightarrow{\sim} V(Z_{jmd}) \quad \text{and} \quad \gamma_j : \pi_{B,*}\mathcal{M}^j \xrightarrow{\sim} V(Z_{jm}).$$

Suppose that we have chosen rigidifications of $\mathcal{L}$ and $\mathcal{M}$. This defines, by means of μ_j and γ_j, theta functions $q_{\mathcal{M}^j} \in V(Z_{jm})$ and $q_{\mathcal{L}^j} \in V(Z_{jmd})$ (see [17, §1] [3, §5.1]). Here we denote the module of algebraic theta functions by $V(Z_n) = \underline{\mathrm{Hom}}(Z_n, \mathcal{O}_R)$ for an integer $n \geq 1$. The following lemma generalizes [3, Lem.6.4].

Lemma 3.5 *There exists a $\lambda \in R^*$ such that for all $x \in Z_{2m}$ one has*

$$q_{\mathcal{M}^2}(x) = \lambda q_{\mathcal{L}^2}(x).$$

Proof. By Mumford's 2-*Multiplication Formula* [17, §3] there exists a $\lambda \in R^*$ such that for all $z \in Z_m$ and $x \in Z_{2m}$ we have

$$(\mathbb{1} \star \delta_z)(x) = \lambda \sum_{y \in x + Z_m} \delta_z(x-y) q_{\mathcal{M}^2}(y) = \lambda q_{\mathcal{M}^2}(x-z).$$

Here $\mathbb{1}$ denotes the finite theta function which takes the value 1 on all of Z_m. The *Isogeny Theorem* [17, §1,Th.4] implies that there exists a $\lambda \in R^*$ such that for $x \in Z_{2dm}$ we have

$$F^*(\mathbb{1} \star \delta_z)(x) = \begin{cases} \lambda q_{\mathcal{M}^2}(x-z), & x \in Z_{2m} \\ 0 \quad , & \text{else} \end{cases}$$

Also there exists a $\lambda_1, \lambda_2 \in R^*$ such that for $x \in Z_{md}$ we have

$$F^*(\mathbb{1})(x) = \begin{cases} \lambda_1, & x \in Z_m \\ 0\,, & \text{else} \end{cases} \quad \text{and} \quad F^*(\delta_z) = \lambda_2 \delta_z.$$

Again by Mumford's multiplication formula there exists a $\lambda \in R^*$ such that for all $x \in Z_{2md}$ we have

$$\begin{aligned} \big(F^*(\mathbb{1}) \star F^*(\delta_z)\big)(x) &= \lambda \sum_{y \in x + Z_{md}} F^*(\mathbb{1})(x+y)\delta_z(x-y)q_{\mathcal{L}^{2d}}(y) \\ &= \begin{cases} \lambda q_{\mathcal{L}^2}(x-z), & x \in Z_{2m} \\ 0 \quad , & \text{else} \end{cases} \end{aligned}$$

The Lemma now follows from the observation that $F^*(\mathbb{1}) \star F^*(\delta_z)$ and $F^*(\mathbb{1} \star \delta_z)$ differ by a unit. $\square$

3.4 Products of abelian varieties with theta structure

In this section we prove the existence of finite products abelian varieties with theta structures. This kind of product is needed in the proof of the 3-multiplication formula.

Let $A_1, \ldots, A_n$ be abelian schemes over a ring R. Assume we are given a line bundle $\mathcal{L}_i$ on A_i and a theta structure Θ_i of type K_i for $(A, \mathcal{L}_i)$ for all $i = 1, \ldots, n$. We set

$$A = \prod_{i=1}^n A_i, \quad K = \prod_{i=1}^n K_i \quad \text{and} \quad \mathcal{L} = \bigotimes_{i=1}^n p_i^* \mathcal{L}_i$$

where $p_i : A \to A_i$ denotes the projection on the i-th factor.

Lemma 3.6 *There exists a natural product theta structure of type K for $(A, \mathcal{L})$ depending on the theta structures Θ_i, where $i = 1, \ldots n$.*

Proof. We remark that there exists a canonical isomorphism $\prod_{i=1}^n H(\mathcal{L}_i) \xrightarrow{\sim} H(\mathcal{L})$. Consider the morphism $\varphi : \prod_{i=1}^n G(\mathcal{L}_i) \to G(\mathcal{L})$ given by $(x_i, \psi_i) \mapsto \big((x_i)_{i=1\ldots n}, \otimes_{i=1}^n p_i^* \psi_i\big)$. Note that

$$\bigotimes_{i=1}^n p_i^* T_{x_i}^* \mathcal{L}_i = \bigotimes_{i=1}^n T_{(x_1,\ldots,x_n)}^* p_i^* \mathcal{L}_i = T_{(x_1,\ldots,x_n)}^* \mathcal{L}.$$

Obviously, $C = \ker(\varphi) \subseteq \mathbb{G}_{m,R}^n$. We claim that φ is surjective. Consider the diagram

$$\begin{tikzcd} \prod_{i=1}^n G(\mathcal{L}_i) \arrow[r, "\varphi"] \arrow[d, "\pi_1 \times \ldots \times \pi_n"'] & G(\mathcal{L}) \arrow[d, "\pi"] \\ \prod_{i=1}^n H(\mathcal{L}_i) \arrow[r, "\mathrm{can}"] \arrow[u, bend right, "s"'] & H(\mathcal{L}) \end{tikzcd} ,$$

where π_i $(i = 1, \ldots, n)$ and π denote the natural projections. Let s be the canonical section of $\pi_1 \times \ldots \times \pi_n$ induced by the theta structures Θ_i. We have $\pi \circ \varphi = \pi_1 \times \ldots \times \pi_n$ (up to canonical isomorphism). As a consequence we have $\pi \circ \varphi \circ s = (\pi_1 \times \ldots \times \pi_n) \circ s = \mathrm{id}$. We conclude that $\pi \circ \varphi \circ s \circ \pi = \pi$. Let $g \in G(\mathcal{L})$. Then by the latter equality the group element $\varphi(s(\pi(g)))$ differs from g by a unit. Hence the morphism φ maps a suitable multiple of $s(\pi(g))$ to g. This implies the surjectivity of φ and proves our claim.

Analogously, one defines a surjective morphism $\Phi : \prod_{i=1}^n G(K_i) \to G(K)$ having kernel equal to C. Let $\tilde{\varphi}$ and $\tilde{\Phi}$ denote the induced isomorphisms

$$\left(\prod_{i=1}^n G(\mathcal{L}_i) \right) / C \xrightarrow{\sim} G(\mathcal{L}) \quad \text{and} \quad \left(\prod_{i=1}^n G(K_i) \right) / C \xrightarrow{\sim} G(K).$$

The theta structure Θ whose existence is claimed in the lemma is given by the composed isomorphism

$$G(K) \xrightarrow{\tilde{\Phi}^{-1}} \left(\prod_{i=1}^n G(K_i) \right) / C \quad \xrightarrow{\Theta_1 \times \ldots \times \Theta_n} \quad \left(\prod_{i=1}^n G(\mathcal{L}_i) \right) / C \xrightarrow{\tilde{\varphi}} G(\mathcal{L}).$$

This completes the proof of the lemma. $\square$

3.5 An algebraic proof of the 3-multiplication formula

In the following we give a 3-*multiplication formula* for algebraic theta functions in the context of Mumford's theory [17]. Our method of proof extends to an arbitrary n-product of algebraic theta functions. For this reason it seems to be instructive to give a detailed proof in terms of Mumford's algebraic theta functions. The following proof generalizes in a straight forward manner Mumford's proof of his 2-*multiplication formula* [17, §3]. The classical complex analytic 3-multiplication formula does not apply in our case because we are working in an arithmetic setting. The theory of algebraic theta functions allows us to keep track of the reduction modulo the prime 3. Let us remind the reader, that our aim is to use the 3-multiplication formula in order to lift theta null points from the special fiber to characteristic 0. For the proof of the complex analytic 3-multiplication formula we refer to [1, Ch.7.6].

Let A be an abelian scheme over a local ring R and let ξ denote the isogeny $A^3 \to A^3$ given by

$$(x_1, x_2, x_3) \mapsto (x_1 - 2x_2, x_1 + x_2 - x_3, x_1 + x_2 + x_3)$$

Assume we are given an ample line bundle $\mathcal{L}$ on A and theta structures Θ_i of type K_i for $\mathcal{L}^i$ where $i \in I = \{1, 2, 3, 6\}$. We assume that the theta structures Θ_i, $i \in I$, are compatible in the sense of [3, §5.3]. We set

$$\mathcal{M}_{i,j,l} = p_1^*\mathcal{L}^i \otimes p_2^*\mathcal{L}^j \otimes p_3^*\mathcal{L}^l,$$

where $p_r : A^3 \to A$, $r = 1, 2, 3$, is the projection on the r-th factor, and $K_{i,j,l} = K_i \times K_j \times K_l$ for $i, j, l \in I$. By Lemma 3.6 there exist product theta structures $\Theta_{1,1,1}$ and $\Theta_{3,6,2}$ of type $K_{1,1,1}$ and $K_{3,6,2}$ for $\mathcal{M}_{1,1,1}$ and $\mathcal{M}_{3,6,2}$, respectively, depending on the theta structures Θ_i where $i \in I$.

Proposition 3.7 *There exists an isomorphism*

$$\xi^*\mathcal{M}_{1,1,1} \overset{\sim}{\to} \mathcal{M}_{3,6,2}. \tag{23}$$

Proof. Let $b = (b_1, b_2) \in A^2$ and $a \in A$. We define

$$s_1 : A^2 \to A^3, (x_1, x_2) \mapsto (a, x_1, x_2) \quad \text{and} \quad s_2 : A \to A^3, x \mapsto (x, b_1, b_2).$$

One computes

$$s_2^*\mathcal{M}_{3,6,2} = s_2^*p_1^*\mathcal{L}^3 \otimes s_2^*p_2^*\mathcal{L}^6 \otimes s_2^*p_3^*\mathcal{L}^2 = (p_1 \circ s_2)^*\mathcal{L}^3 \otimes (p_2 \circ s_2)^*\mathcal{L}^6 \otimes (p_3 \circ s_2)^*\mathcal{L}^2 = \mathcal{L}^3.$$

and

$$\begin{aligned} s_2^*\xi^*\mathcal{M}_{1,1,1} &= (p_1 \circ \xi \circ s_2)^*\mathcal{L} \otimes (p_2 \circ \xi \circ s_2)^*\mathcal{L} \otimes (p_3 \circ \xi \circ s_2)^*\mathcal{L} \\ &= T^*_{-2b_1}\mathcal{L} \otimes T^*_{b_1 - b_2}\mathcal{L} \otimes T^*_{b_1 + b_2}\mathcal{L} = \mathcal{L}^3. \end{aligned}$$

The latter equality follows by the Theorem of the Square. Now take $a = 0_A$ where 0_A denotes the zero section of A. Let $p_{23} : A^3 \to A^2$ be the projection on the 2-nd and 3-rd factor and let $\tilde{p}_m : A^2 \to A$ denote the projection on the m-th factor ($m = 1, 2$). We have

$$\begin{aligned} s_1^*\mathcal{M}_{3,6,2} &= (p_1 \circ s_1)^*\mathcal{L}^3 \otimes s_1^*(p_2^*\mathcal{L}^6 \otimes p_3^*\mathcal{L}^2) \\ &= (p_1 \circ s_1)^*\mathcal{L}^3 \otimes (p_{23} \circ s_1)^*(\tilde{p}_1^*\mathcal{L}^6 \otimes \tilde{p}_2^*\mathcal{L}^2) = \tilde{p}_1^*\mathcal{L}^6 \otimes \tilde{p}_2^*\mathcal{L}^2. \end{aligned}$$

By [17, §3,Prop.1] we conclude that

$$\begin{aligned} s_1^*\xi^*\mathcal{M}_{1,1,1} &= (p_1 \circ \xi \circ s_1)^*\mathcal{L} \otimes (p_{23} \circ \xi \circ s_1)^*(\tilde{p}_1^*\mathcal{L} \otimes \tilde{p}_2^*\mathcal{L}) \\ &= \tilde{p}_1^*[2]^*[-1]^*\mathcal{L} \otimes (\tilde{p}_1^*\mathcal{L} \otimes \tilde{p}_2^*\mathcal{L})^2 = \tilde{p}_1^*\mathcal{L}^6 \otimes \tilde{p}_2^*\mathcal{L}^2. \end{aligned}$$

The latter equality follows by the symmetry of $\mathcal{L}$. Note that $p_{23} \circ \xi \circ s_1$ equals the isogeny used in [17, §3,Prop.1]. The proposition now follows by applying the Seesaw Principle. □

Lemma 3.8 *The theta structure $\Theta_{3,6,2}$ is ξ-compatible with $\Theta_{1,1,1}$.*

Proof. We have to check the compatibility assumptions of [2, §5.2]. We have already shown in Proposition 3.7 that there exists an isomorphism $\alpha : \xi^*\mathcal{M}_{1,1,1} \xrightarrow{\sim} \mathcal{M}_{3,6,2}$. Let τ be the morphism $A \to A^3, x \mapsto (2x, x, 3x)$. The kernel of ξ is given by the restriction of τ to $A[6]$. In the following we will identify the groups $K_6 \times K_6^D$, $K_{1,1,1} \times K_{1,1,1}^D$ and $K_{3,6,2} \times K_{3,6,2}^D$ with their images under the Lagrangian decompositions induced by the theta structures Θ_6, $\Theta_{1,1,1}$ and $\Theta_{3,6,2}$, respectively. Note that $A[6]$ is contained in the image of $K_6 \times K_6^D$ under τ. By the compatibility assumptions we have $\tau\big(K_6\big) \subseteq K_{3,6,2}$ and $\tau\big(K_6^D\big) \subseteq K_{3,6,2}^D$. We conclude that condition (†) of [2, §5.2] is satisfied with $Z_1 = \tau\big(A[6] \cap K_6\big)$ and $Z_2 = \tau\big(A[6] \cap K_6^D\big)$. The isomorphism (23) gives rise to a subgroup $\tilde{K} \leq G(\mathcal{M}_{3,6,2})$ lifting the kernel of ξ. Let $G(\mathcal{M}_{3,6,2})^*$ denote the centralizer of $\tilde{K}$ in $G(\mathcal{M}_{3,6,2})$. By [17, §1,Prop.2] we have

$$G(\mathcal{M}_{3,6,2})^* = \big\{g \in G(\mathcal{M}_{3,6,2}) | \xi\big(\pi_{3,6,2}(g)\big) \in A^3[\mathcal{M}_{1,1,1}]\big\} \tag{24}$$

where $\pi_{3,6,2} : G(\mathcal{M}_{3,6,2}) \to A^3[\mathcal{M}_{3,6,2}]$ is the natural projection. Here we denote

$$A^3[\mathcal{M}_{i,j,l}] = \{x \in A^3 | T_x^*\mathcal{M}_{i,j,l} \cong \mathcal{M}_{i,j,l}\}$$

for all $i, j, l \in I$. Because of the equality (24) we have

$$Z_1^\perp = \{(x,y,z) \in K_{3,6,2} | \xi(x,y,z) \in K_{1,1,1}\} \quad \text{and} \quad Z_2^\perp = \{(x,y,z) \in K_{3,6,2}^D | \xi(x,y,z) \in K_{1,1,1}^D\}$$

(notation as in [2, §5.2]). Obviously the isogeny ξ induces a surjective morphism $\sigma : Z_1^\perp \to K_{1,1,1}$ having kernel Z_1. Let σ_1 be the inverse of the isomorphism $Z_1^\perp/Z_1 \xrightarrow{\sim} K_{1,1,1}$ induced by σ. Let σ_2 be defined as in [3, §5.2]. It remains to check the commutativity of the following diagram

$$\begin{tikzcd} G(\mathcal{M}_{3,6,2})^*/\tilde{K} \arrow[d, "\mathrm{can},\xi"] & \mathbb{G}_{m,R} \times Z_1^\perp/Z_1 \times Z_2^\perp/Z_2 \arrow[l, "\Theta_{3,6,2}"'] \\ G(\mathcal{M}_{1,1,1}) & \mathbb{G}_{m,R} \times K_{1,1,1} \times K_{1,1,1}^D \arrow[l, "\Theta_{1,1,1}"'] \arrow[u, "\mathrm{id}\times\sigma_1\times\sigma_2"'] \end{tikzcd} \tag{25}$$

where the left hand vertical morphism is defined as in the proof of [17, §1,Prop.2]. We claim that the group $\mathbb{G}_{m,R} \times Z_1^\perp/Z_1 \times Z_2^\perp/Z_2$ is generated by $\mathbb{G}_{m,R}$ and elements of the form

$$(1, 2x, x, 3x, l^2, l, l^3), \quad (1, 2x, x, -3x, l^2, l, l^{-3}) \quad \text{and} \quad (1, 2x, -2x, 0, l^2, l^{-2}, 1)$$

where $(x, l) \in K_6 \times K_6^D$. Let ξ' denote the isogeny $A^3 \to A^3$ given by

$$(x_1, x_2, x_3) \mapsto (2x_1 + 2x_2 + 2x_3, -2x_1 + x_2 + x_3, -3x_2 + 3x_3).$$

Assume we are given an element $(1, x, l)$ of $\mathbb{G}_{m,R} \times Z_1^\perp \times Z_2^\perp$. We denote $\xi(x, l) = (\bar{x}, \bar{l})$. Choose $\tilde{x} \in K_{6,6,6}$ and $\tilde{l} \in K_{6,6,6}^D$ such that $[6](\tilde{x}, \tilde{l}) = (\bar{x}, \bar{l})$. One verifies that $\xi \circ \xi' = [6]$ and hence the element $\xi'(\tilde{x}, \tilde{l}) \in K_{3,6,2} \times K_{3,6,2}^D$ differs from (x, l) by an element of $Z_1 \times Z_2$. This implies the above claim.

In the sequel we will prove the commutativity of the diagram (25) for elements of the form $(1, 2x, x, 3x, l^2, l, l^3)$. The proof for elements of the form

$$(1, 2x, x, -3x, l^2, l, l^{-3}) \quad \text{and} \quad (1, 2x, -2x, 0, l^2, l^{-2}, 1)$$

goes analogously and is left to the reader. We define

$$\iota : G(K_6) \to G(K_{3,6,2}), (\alpha, x, l) \mapsto (\alpha^6, 2x, x, 3x, l^2, l, l^3)$$

and set $\kappa = \Theta_{3,6,2} \circ \iota \circ \Theta_6^{-1}$. Let $G(K_6)^\sharp = \iota^{-1}G(K_{3,6,2})^*$ and $G(\mathcal{L}^6)^\sharp = \Theta_6\big(G(K_6)^\sharp\big)$. We define $\varphi_3 : G(\mathcal{L}) \to G(\mathcal{M}_{1,1,1})$ and $\Phi_3 : G(K_1) \to G(K_{1,1,1})$ to be the restriction on the 3-rd factor of the morphism φ and Φ introduced in the proof of Lemma 3.6. It is readily checked that the following diagram (dotted arrows ignored) is commutative

$$\begin{tikzcd}
G(\mathcal{L}^6)^\sharp \arrow[dr, "\kappa"] \arrow[dd, "\eta_6"'] & & G(K_6)^\sharp \arrow[ll, "\Theta_6"'] \arrow[dr, "\iota"] \arrow[dd, "H_6"] & \\
& G(\mathcal{M}_{3,6,2})^*/\tilde{K} \arrow[dd, dotted, "\mathrm{can},\xi"] & & \mathbb{G}_{m,R} \times Z_1^\perp/Z_1 \times Z_2^\perp/Z_2 \arrow[ll, "\Theta_{3,6,2}"] \\
G(\mathcal{L}) \arrow[dr, "\varphi_3"] & & G(K_1) \arrow[ll, "\Theta_1"'] \arrow[dr, "\Phi_3"] & \\
& G(\mathcal{M}_{1,1,1}) & & \mathbb{G}_{m,R} \times K_{1,1,1} \times K_{1,1,1}^D. \arrow[ll, "\Theta_{1,1,1}"'] \arrow[uu, "\mathrm{id}\times\sigma_1\times\sigma_2"']
\end{tikzcd}$$

Here η_6 and H_6 are defined as in [3, §5.3]. Note that the upper left square is commutative since Θ_6 and Θ_1 are assumed to be 6-compatible.

In order to show that the diagram (25) is commutative on the subset of elements of the form $(1, 2x, x, 3x, l^2, l, l^3)$ it suffices to prove that the following diagram commutes

$$\begin{tikzcd}
G(\mathcal{L}^6)^\sharp \arrow[r, "\kappa"] \arrow[d, "\eta_6"'] & G(\mathcal{M}_{3,6,2})^*/\tilde{K} \arrow[d, "\mathrm{can},\xi"] \\
G(\mathcal{L}) \arrow[r, "\varphi_3"] & G(\mathcal{M}_{1,1,1}).
\end{tikzcd}$$

Consider the commutative diagram

$$\begin{tikzcd}
A^3 \arrow[r, "\xi"] & A^3 \\
A \arrow[u, "\tau"] \arrow[r, "{[6]}"] & A \arrow[u, "\mathrm{i}_3"']
\end{tikzcd}$$

where $\mathrm{i}_3(x) = (0, 0, x)$. There exist isomorphisms

$$\beta : [6]^*\mathcal{L} \xrightarrow{\sim} \mathcal{L}^{36} \quad \text{and} \quad \gamma : \mathrm{i}_3^*\mathcal{M}_{1,1,1} \xrightarrow{\sim} \mathcal{L}.$$

The existence of the isomorphism β is implied by the symmetry of $\mathcal{L}$. Consider the isomorphism δ given by the composition

$$\tau^*\mathcal{M}_{3,6,2} \overset{\tau^*\alpha^{-1}}{\longrightarrow} \tau^*\xi^*\mathcal{M}_{1,1,1} = (\xi \circ \tau)^*\mathcal{M}_{1,1,1} = (i_3 \circ [6])^*\mathcal{M}_{1,1,1} = [6]^* i_3^*\mathcal{M}_{1,1,1} \overset{[6]^*\gamma}{\longrightarrow} [6]^*\mathcal{L} \overset{\beta}{\to} \mathcal{L}^{36},$$

where α is as above. The isomorphism δ induces a morphism

$$\mathrm{can}, \tau : G(\mathcal{M}_{3,6,2}) \to G(\mathcal{L}^{36}), (x, \psi) \mapsto \big(p_2(x), T^*_{p_2(x)}\delta \circ \tau^*\psi \circ \delta^{-1}\big)$$

where $p_2 : A^3 \to A$ denotes the projection on the second factor. We claim that the following diagram is commutative

$$\begin{tikzcd}
G(\mathcal{L}^6) \arrow[r, "\kappa"] \arrow[d, "\epsilon_6"'] & G(\mathcal{M}_{3,6,2}) \arrow[dl, "\mathrm{can},\tau"] \\
G(\mathcal{L}^{36}) &
\end{tikzcd} \tag{26}$$

where ϵ_6 is defined as in [3, §5.3]. Let $g = \big((x,l),\psi\big) \in G(\mathcal{L}^6)$ and $h = \Theta_6^{-1}(g)$. By definition we have

$$\iota(h) = \Phi\big(H_2(h), h, H_3(h)\big)$$

and hence

$$\kappa(g) = \varphi\big(\eta_2(g), g, \eta_3(g)\big) = \big((2x, x, 3x, l^2, l, l^3), p_1^*\eta_2(\psi) \otimes p_2^*\psi \otimes p_3^*\eta_3(\psi)\big).$$

The image of $\kappa(g)$ under the canonical morphism induced by δ is given by

$$\Big(x, T_x^*\delta \circ \tau^*\big(p_1^*\eta_2(\psi) \otimes p_2^*\psi \otimes p_3^*\eta_3(\psi)\big) \circ \delta^{-1}\Big).$$

Choose isomorphisms $\rho_2 : [2]^*\mathcal{L} \xrightarrow{\sim} \mathcal{L}^4$ and $\rho_3 : [3]^*\mathcal{L} \xrightarrow{\sim} \mathcal{L}^9$. Consider the composed isomorphism δ' given by

$$\begin{aligned}\tau^*\mathcal{M}_{3,6,2} = \tau^*(p_1^*\mathcal{L}^3 \otimes p_2^*\mathcal{L}^6 \otimes p_3^*\mathcal{L}^2) &= (p_1\circ\tau)^*\mathcal{L}^3 \otimes (p_2\circ\tau)^*\mathcal{L}^6 \otimes (p_3\circ\tau)^*\mathcal{L}^2 \\ &= [2]^*\mathcal{L}^3 \otimes \mathcal{L}^6 \otimes [3]^*\mathcal{L}^2 \overset{\rho_2\otimes\mathrm{id}\otimes\rho_3}{\longrightarrow} \mathcal{L}^{36}.\end{aligned}$$

The isomorphism δ' differs from δ by a unit. Thus we have

$$\begin{aligned}&T_x^*\delta \circ \tau^*\big(p_1^*\eta_2(\psi) \otimes p_2^*\psi \otimes p_3^*\eta_3(\psi)\big) \circ \delta^{-1} \\ &\quad= T_x^*\delta' \circ \tau^*\big(p_1^*\eta_2(\psi) \otimes p_2^*\psi \otimes p_3^*\eta_3(\psi)\big) \circ (\delta')^{-1} \\ &\quad= T_x^*\delta' \circ \big((p_1\circ\tau)^*\eta_2(\psi) \otimes (p_2\circ\tau)^*\psi \otimes (p_3\circ\tau)^*\eta_3(\psi)\big) \circ (\delta')^{-1} \\ &\quad= T_x^*\delta' \circ \big([2]^*\eta_2(\psi) \otimes \psi \otimes [3]^*\eta_3(\psi)\big) \circ (\delta')^{-1} \\ &\quad= \big(T_x^*\rho_2 \circ [2]^*\eta_2(\psi) \circ \rho_2^{-1}\big) \otimes \psi \otimes \big(T_x^*\rho_3 \circ [3]^*\eta_3(\psi) \circ \rho_3^{-1}\big) \\ &\quad= \epsilon_2(\psi) \otimes \psi \otimes \epsilon_3(\psi) = \epsilon_6(\psi).\end{aligned}$$

This proves our claim, i.e. the commutativity of diagram (26). The isomorphism γ induces a morphism

$$\mathrm{can}, i_3 : G(\mathcal{M}_{1,1,1}) \to G(\mathcal{L}), (x,\psi) \mapsto \big(p_3(x), T_{p_3(x)}^*\gamma \circ i_3^*\psi \circ \gamma^{-1}\big)$$

where $p_3 : A^3 \to A$ denotes the projection on the 3rd factor. Consider the diagram

$$\begin{tikzcd}
G(\mathcal{M}_{3,6,2})^* \arrow[rr] \arrow[dd, "\mathrm{can},\tau"] & & G(\mathcal{M}_{3,6,2})^*/\tilde{K} \arrow[rr, "\mathrm{can},\xi"] & & G(\mathcal{M}_{1,1,1}) \arrow[dd, bend left, "\mathrm{can},i_3"] \\
& & G(\mathcal{L}^6)^\sharp \arrow[ull, "\kappa"'] \arrow[dll, "\epsilon_6"'] \arrow[drr, "\eta_6"] & & \\
G(\mathcal{L}^{36}) & G(\mathcal{L}^{36})^* \arrow[l, hook'] \arrow[r] & G(\mathcal{L}^{36})^*/\widetilde{A[6]} \arrow[rr, "\mathrm{can},[6]"'] & & G(\mathcal{L}). \arrow[uu, bend left, "\varphi_3"]
\end{tikzcd}$$

Here $G(\mathcal{L}^{36})^*$ denotes the centralizer of the lifted subgroup $\widetilde{A[6]}$ in $G(\mathcal{L}^{36})$. By the above discussion the left hand triangle is commutative. By the same reasoning as above it follows that the composed morphism

$$G(\mathcal{L}) \xrightarrow{\varphi_3} G(\mathcal{M}_{1,1,1}) \xrightarrow{\mathrm{can},i_3} G(\mathcal{L})$$

equals the identity. This implies that the canonical morphism induced by γ is surjective. As a consequence the commutativity of diagram (25) is equivalent to the commutativity of the following diagram

$$\begin{tikzcd}
G(\mathcal{L}^6)^\sharp \arrow[r, "\kappa"] \arrow[d, "\eta_6"] & G(\mathcal{M}_{3,6,2})^*/\tilde{K} \arrow[d, "\mathrm{can},\xi"] \\
G(\mathcal{L}) & G(\mathcal{M}_{1,1,1}). \arrow[l, "\mathrm{can},i_3"']
\end{tikzcd} \tag{27}$$

Let

$$g \in G(\mathcal{L}^6)^\sharp \quad \text{and} \quad \kappa(g) = (x, \psi).$$

By definition the image of $\kappa(g)$ under the canonical morphism induced by δ is given by

$$\Big(p_2(x), T^*_{p_2(x)}\delta \circ \tau^*\psi \circ \delta^{-1}\Big).$$

Since $\tau\big(p_2(x)\big) = x$ it follows that

$$\begin{aligned}
T^*_{p_2(x)}\delta \circ \tau^*\psi \circ \delta^{-1} &= T^*_{p_2(x)}\big(\beta \circ [6]^*\gamma \circ \tau^*\alpha^{-1}\big) \circ \tau^*\psi \circ \big(\beta \circ [6]^*\gamma \circ \tau^*\alpha^{-1}\big)^{-1} \\
&= T^*_{p_2(x)}\beta \circ T^*_{p_2(x)}[6]^*\gamma \circ T^*_{p_2(x)}\tau^*\alpha^{-1} \circ \tau^*\psi \circ \tau^*\alpha \circ [6]^*\gamma^{-1} \circ \beta^{-1} \\
&= T^*_{p_2(x)}\beta \circ [6]^*T^*_{p_2(6x)}\gamma \circ \tau^*T^*_x\alpha^{-1} \circ \tau^*\psi \circ \tau^*\alpha \circ [6]^*\gamma^{-1} \circ \beta^{-1} \\
&= T^*_{p_2(x)}\beta \circ [6]^*T^*_{p_2(6x)}\gamma \circ \tau^*\big(T^*_x\alpha^{-1} \circ \psi \circ \alpha\big) \circ [6]^*\gamma^{-1} \circ \beta^{-1} \\
&= T^*_{p_2(x)}\beta \circ [6]^*T^*_{p_2(6x)}\gamma \circ \tau^*\xi^*\psi' \circ [6]^*\gamma^{-1} \circ \beta^{-1}
\end{aligned}$$

where $\xi^*\psi' = T^*_x\alpha^{-1} \circ \psi \circ \alpha$. Note that such an isomorphism ψ' exists since $\kappa(g) \in G(\mathcal{M}_{3,6,2})^*$. We remark that the pair $\big(\xi(x), \psi'\big) \in G(\mathcal{M}_{1,1,1})$ is the image of $\kappa(g)$ under the canonical morphism induced by α. Continuing the above calculation we get

$$\begin{aligned}
T^*_{p_2(x)}\delta \circ \tau^*\psi \circ \delta^{-1} &= T^*_{p_2(x)}\beta \circ [6]^*T^*_{p_2(6x)}\gamma \circ \tau^*\xi^*\psi' \circ [6]^*\gamma^{-1} \circ \beta^{-1} \\
&= T^*_{p_2(x)}\beta \circ [6]^*T^*_{p_2(6x)}\gamma \circ [6]^*i_3^*\psi' \circ [6]^*\gamma^{-1} \circ \beta^{-1} \\
&= T^*_{p_2(x)}\beta \circ [6]^*\big(T^*_{p_2(6x)}\gamma \circ i_3^*\psi' \circ \gamma^{-1}\big) \circ \beta^{-1} \\
&= T^*_{p_2(x)}\beta \circ [6]^*\big(T^*_{p_3(\xi(x))}\gamma \circ i_3^*\psi' \circ \gamma^{-1}\big) \circ \beta^{-1}.
\end{aligned}$$

By definition the pair

$$g' = \Big(p_3\big(\xi(x)\big), T^*_{p_3(\xi(x))}\gamma \circ i_3^*\psi' \circ \gamma^{-1}\Big)$$

is the image of $\big(\xi(x), \psi'\big)$ under the canonical morphism induced by γ. We conclude by the above equality, the commutativity of diagram (26) and the definition of η_6 that $g' = \eta_6(g)$. Thus we have shown that diagram (27) is commutative. As a consequence diagram (25) is commutative. This finishes the proof of the lemma. □

Assume that we have chosen $G(K_{1,1,1})$- and $G(K_{3,6,2})$-equivariant isomorphisms

$$\mu_{1,1,1} : \pi_{3,*}\mathcal{M}_{1,1,1} \xrightarrow{\sim} V(K_{1,1,1}) \quad \text{and} \quad \mu_{3,6,2} : \pi_{3,*}\mathcal{M}_{3,6,2} \xrightarrow{\sim} V(K_{3,6,2})$$

where π_3 denotes the structure morphism of A^3. The following lemma is a generalization of the *Addition Formula* which is stated in [17, §3]. We use the intuitively simplified notation introduced in the proof of Lemma 3.8.

Corollary 3.9 *There exists a $\lambda \in R^*$ such that for all $g \in V(K_{1,1,1})$ we have*

$$\xi^*g(x,y,z) = \begin{cases} \lambda g(\xi(x,y,z)), & \xi(x,y,z) \in K_{1,1,1} \\ 0 \quad\quad\quad\quad\quad , & \text{else} \end{cases}$$

where $(x,y,z) \in K_{3,6,2}$.

Proof. By Lemma 3.8 we can apply the *Isogeny Theorem* (see [17, §1,Th.4] [3, §5.2,Th.5.4]) in order to obtain the formula given in the lemma. □

Assume that we have chosen $G(K_i)$-equivariant isomorphisms

$$\mu_i : \pi_*\mathcal{L}^i \xrightarrow{\sim} G(K_i), \quad i \in I,$$

where π denotes the structure morphism of A, and that we have rigidified the line bundle $\mathcal{L}$. This defines theta functions $q_{\mathcal{L}^i} \in V(K_i)$ (see [17, §1] and [3, §5.1]).

Let $\Delta : A \to A^3$ the diagonal morphism. There exists a canonical isomorphism $\beta : \Delta^*\mathcal{M}_{1,1,1} \xrightarrow{\sim} \mathcal{L}^3$. The following theorem describes the morphism of $\mathcal{O}_R$-modules φ defined as the composition

$$\pi_*\mathcal{L} \otimes \pi_*\mathcal{L} \otimes \pi_*\mathcal{L} \xrightarrow{\text{can}} \pi_{3,*}\mathcal{M}_{1,1,1} \xrightarrow{\text{can}} \pi_{3,*}\Delta_*\Delta^*\mathcal{M}_{1,1,1} = \pi_*\Delta^*\mathcal{M}_{1,1,1} \xrightarrow{\pi_*\beta} \pi_*\mathcal{L}^3,$$

where the left hand morphism is the Künneth morphism, in terms of finite theta functions.

Definition 3.10 *For $s_1, s_2, s_3 \in \pi_*\mathcal{L}$ and $f_1, f_2, f_3 \in V(K_1)$ such that $\mu(s_i) = f_i$ ($i = 1, 2, 3$) we set*

$$f_1 \star f_2 \star f_3 = (\mu_1 \otimes \mu_1 \otimes \mu_1)\big(s_1 \otimes s_2 \otimes s_3\big).$$

We define for $x \in K_3$

$$G_x = \{(y, z) \in K_{6,2} \mid \xi(x, y, z) \in K_{1,1,1}\}.$$

Theorem 3.11 (3-multiplication formula) *There exists a $\lambda \in R^*$ such that for all $x \in K_3$ and $f_1, f_2, f_3 \in V(K_1)$ we have*

$$(f_1 \star f_2 \star f_3)(x) = \lambda \sum_{(y,z)\in G_x} f_1(x - 2y) f_2(x + y - z) f_3(x + y + z) q_{\mathcal{L}^6}(y) q_{\mathcal{L}^2}(z).$$

Proof. Consider the commutative diagram

$$\begin{tikzcd} A \arrow[d, "i_1"'] \arrow[dr, "\Delta"] & \\ A^3 \arrow[r, "\xi"] & A^3 \end{tikzcd} \tag{28}$$

where $i_1 : A \to A^3$ is defined by $x \mapsto (x, 0, 0)$ and Δ is the diagonal morphism. Note that there exists an isomorphism $\gamma : i_1^*\mathcal{M}_{3,6,2} \xrightarrow{\sim} \mathcal{L}^3$. By Proposition 3.7 there exists an isomorphism $\alpha : \xi^*\mathcal{M}_{1,1,1} \xrightarrow{\sim} \mathcal{M}_{3,6,2}$. Because of the commutativity of the diagram (28) the morphism φ defined above equals up to a unit the composed morphism

$$\begin{aligned} \pi_*\mathcal{L} \otimes \pi_*\mathcal{L} \otimes \pi_*\mathcal{L} &\xrightarrow{\text{can}} \pi_{3,*}\mathcal{M}_{1,1,1} \xrightarrow{\text{can}} \pi_{3,*}\Delta_*\Delta^*\mathcal{M}_{1,1,1} \\ &= \pi_*\Delta^*\mathcal{M}_{1,1,1} = \pi_* i_1^*\xi^*\mathcal{M}_{1,1,1} \xrightarrow{\pi_* i_1^*\alpha} \pi_* i_1^*\mathcal{M}_{3,6,2} \xrightarrow{\pi_*\gamma} \pi_*\mathcal{L}^3. \end{aligned}$$

Passing over from sections to finite theta functions we get a diagram

$$V(K_1) \otimes V(K_1) \otimes V(K_1) \xrightarrow{\text{can}} V(K_{1,1,1}) \xrightarrow{\xi^*} V(K_{3,6,2}) \xrightarrow{\text{eval}} V(K_3). \tag{29}$$

The left hand map is defined to be the canonical isomorphism mapping

$$f_1 \star f_2 \star f_3 \mapsto \tilde{f}_1\tilde{f}_2\tilde{f}_3$$

where $\tilde{f}_i$ is the function on $K_{1,1,1}$ defined by

$$\tilde{f}_i(x_1, x_2, x_3) = f_i(x_i), \quad i = 1, 2, 3.$$

The map ξ^* is given by Corollary 3.9. The right hand eval-map in diagram (29) corresponds to the map on sections which maps a section $s_1 \otimes s_2 \otimes s_3 \in \pi_*\mathcal{M}_{3,6,2}$ to the section $(s_2)_0(s_3)_0 s_1$ where $(\cdot)_0$ indicates the evaluation at zero by means of the chosen rigidification. The claim now follows by expressing $(s_2)_0$ and $(s_3)_0$ in terms of theta null values (see [17, §1,Cor.3]). ☐

4 Explicit CM construction in characteristic 3

In this section we apply Corollary 2.3 to the explicit CM construction of invariants of ordinary abelian surfaces by canonical lifting from characteristic 3. The CM algorithm has two main phases:

- first (see Section 4.4), the multivariate Newton lifting of a given canonical theta null point based on the equations of Corollary 2.3 by means of the algorithm of Lercier and Lubicz [12, Th.2],
- second (see Section 4.5), the LLL reconstruction of the defining polynomials over $\mathbb{Z}$ for the ideal of relations between the canonically lifted moduli, following Gaudry et al. [8].

The existence of the lifting algorithm is a consequence of the following facts. The ordinary locus at 3 of the moduli space of abelian varieties with symmetric 4-theta structure, which is constructed in [18], is smooth. The space of pairs of ordinary abelian varieties with symmetric 4-theta structure admitting a compatible isogeny of degree 3^g, where g is the dimension, forms an étale covering of the latter space.

The lifting algorithm applies to a rationally parametrized moduli space X over $\mathbb{Z}_q$, and a complete intersection in $X \times X$. We replace the rational parametrization with a local analytic parametrization. We describe the construction in detail in the application to the explicit moduli of abelian varieties of dimensions 1 and 2 described herein, but the approach applies in greater generality to any dimension.

4.1 Complexity hypothesis

We will denote by $\mathbb{F}_q$ a finite field of characteristic $p > 0$ having q elements. Let $\mathbb{Z}_q$ denote the ring of Witt vectors with values in $\mathbb{F}_q$. There exists a canonical lift $\sigma \in \mathrm{Aut}(\mathbb{Z}_q)$ of the p-th power Frobenius morphism of $\mathbb{F}_q$. If a is an element of $\mathbb{Z}_q$ we denote by $\bar{a}$ its reduction modulo p in $\mathbb{F}_q$. We say that we have computed an element $x \in \mathbb{Z}_q$ to precision m if we can write down a bit-string representing its class in the quotient ring $\mathbb{Z}_q/p^m\mathbb{Z}_q$. In order to assess the complexity of our algorithms we use the computational model of a Random Access Machine [21]. We assume that the multiplication of two n-bit length integers takes $O(n^\mu)$ bit operations. One has $\mu = 1 + \epsilon$ (for n sufficiently large), $\mu = \log_2(3)$ and $\mu = 2$ using the FFT multiplication algorithm, the Karatsuba algorithm and a naive multiplication method, respectively. Let $x, y \in \mathbb{Z}_q/p^m\mathbb{Z}_q$. For the following we assume the sparse modulus representation which is explained in [4, pp.239]. Under this assumption one can compute the product xy to precision m by performing $O(m^\mu \log(q)^\mu)$ bit operations.

4.2 A lifting algorithm for moduli of elliptic curves

We first describe a canonical lifting algorithm for theta null points of elliptic curves, hence take an abelian scheme E of relative dimension 1 over $\mathbb{Z}_q$. Its theta null point $(a_0 : a_1 : a_2 : a_1)$ determines a Legendre model for E of the form

$$y^2 = x(x-1)(x-\lambda), \text{ where } \lambda = \left(\frac{2a_0a_2}{a_0^2 + a_2^2}\right)^2.$$

In particular we make use of the maps of modular curves

$$\mathcal{A}_1(\Theta_4) \longrightarrow \mathcal{A}_1(\Theta_4[2]) \longrightarrow X(2),$$

where the first map is $(a_0 : a_1 : a_2) \mapsto (a_0 : a_2)$ is the restriction to the 2-torsion part of the theta structure, and $X(2)$ is the full modular curve of level 2 with function field generated by λ.

We recall that the curve $\mathcal{A}_1(\Theta_4)$ is determined by Riemann's equation (7) and the correspondence equation (8) determines a curve in the product $\mathcal{A}_1(\Theta_4) \times \mathcal{A}_1(\Theta_4)$. Projecting this correspondence curve onto the 2-torsion part with coordinates $(x_0 : x_2)$ and $(y_0 : y_2)$, gives rise to an affine curve

$$x^4 - 4x^3y^3 + 6x^2y^2 - 4xy + y^4 = 0, \tag{30}$$

by setting $x = x_2/x_0$ and $y = y_2/y_0$. This curve is singular of geometric genus 3, with singularities

$$\{(0,0),(1,1),(-1,-1),(i,-i)\},$$

where $i^2 = -1$ in $\mathbb{Z}_q$. It is easily verified that all x in $\{\infty, 0, 1, -1, i, i\}$ determine degenerate, singular cubic curves. Moreover, the special fiber at 3 takes the form

$$(x^3 - y)(x - y^3) = 0,$$

whose singularities consist of all points (x, x^σ) for x in $\mathbb{F}_9$. Outside of the image of the above degenerate points, the remaining $\mathbb{F}_9$-rational points are supersingular.

The remaining points correspond to theta null points of ordinary elliptic curves, for which it is easily verified that the conditions of Lercer-Lubicz [12] for an Artin-Schreier equation are satisfied. Hence their Newton algorithm applies to uniquely lift a solution to equation (30) with the constraint to $y = x^\sigma$. From a solution to this system, we set $(a_0 : a_2) = (1 : x)$ and determine a_1 by one Newton lifting step. This gives the following theorem.

Theorem 4.1 *There exists a deterministic algorithm which has as input the theta null point $(\bar{a}_i)$ of an elliptic curve $\bar{E}$ over $\mathbb{F}_q$ and as output the theta null point (a_i) of its canonical lift E to a given precision $m \geq 1$, with time complexity*

$$O(\log(m) d^\mu m^\mu)$$

where $d = \log(q)$.

4.3 A lifting algorithm for split abelian surfaces

As in Section 2.1.1 we let $\mathcal{A}_g(\Theta_4[2])$ denote the moduli space of 4-theta null points, projected on the coordinates which are parametrized by the 2-torsion subgroup. We recall that

$$a_{00}a_{22} - a_{02}a_{20} = 0,$$

determines one component in $\mathcal{A}_2(\Theta_4[2])$ of split abelian surfaces. We refer to Runge [23]) for a complex analytic description of this locus as a degenerate Humbert surface.

The remaining components are obtained by the action of a geometric automorphism group acting on theta structures and preserving the moduli of abelian varieties. Explicitly this group is generated by the projective automorphism group generated by the matrices

$$\begin{pmatrix} 1 & 1 & 0 & 0 \\ -1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & -1 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 1 & 0 \\ -1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & -1 & 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & i & 0 \\ 0 & 0 & 0 & i \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & i & 0 & 0 \\ 0 & 0 & i & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

acting on $\mathcal{A}_g(\Theta_4[2]) \cong \mathbb{P}^3$. These automorphism determine a transitive action on the 10 components of the Humbert surface. In particular, given a theta null point of a split abelian variety, by means of an automorphism (defined over an extension of degree at most 2), we may assume that it lies on the locus $a_{00}a_{22} = a_{02}a_{20}$.

We now recall that the locus $a_{00}a_{22} = a_{02}a_{20}$ is the image of $\mathcal{A}_1(\Theta_4[2]) \times \mathcal{A}_1(\Theta_4[2])$ in $\mathcal{A}_2(\Theta_4[2])$ by a Segre embedding

$$\big((a_0 : a_2), (a'_0 : a'_2)\big) \longmapsto (a_{00} : a_{02} : a_{20} : a_{22}) = (a_0a'_0 : a_0a'_2 : a_2a'_0 : a_2a'_2).$$

The canonical lift of this theta null point is obtained by means of the canonical lifting to algorithm applied to $(a_{00} : a_{20}) = (a_{02} : a_{22})$ and to $(a_{00} : a_{02}) = (a_{20} : a_{22})$. This yields the canonical lift of the theta null point with the same complexity as for elliptic curves. We summarize this result in the general theorem for abelian surfaces in the next section.

4.4 A lifting algorithm for moduli of abelian surfaces

We use the notation introduced in Section 4.1. For the rest of this section let A be an abelian scheme of relative dimension 2 over $\mathbb{Z}_q$ having ordinary reduction. Suppose A is the canonical lift of $A_{\mathbb{F}_q}$. Let $\mathcal{L}$ be an ample symmetric line bundle of degree 1 on A and assume we are given a theta structure of type $(\mathbb{Z}/4\mathbb{Z})^2$ for $(A, \mathcal{L}^4)$. We denote the theta null point with respect to the latter theta structure by (a_{ij}) where $(i,j) \in (\mathbb{Z}/4\mathbb{Z})^2$.

Theorem 4.2 *There exists a deterministic algorithm which has as input the theta null point $(\bar{a}_{ij})$ of $A_{\mathbb{F}_q}$ and as output the theta null point (a_{ij}) of A to a given precision $m \geq 1$, with time complexity*

$$O(\log(m) d^{\mu} m^{\mu})$$

where $d = \log(q)$.

Proof. The complexity result of Theorem 4.2 is an analytic version of [12, Th.2]. We explain below how our system of equations can be adapted to an analytic context from which the result will follow.

By means of a geometric automorphism, we may assume that a_{00} is a unit and embed the corresponding open subscheme of $\mathcal{A}_2(\Theta_4)$ in $\mathbb{A}^9$. We identify its image in $\mathcal{A}_2(\Theta_4[2])$ with $\mathbb{A}^3$. We denote the open analytic subspace of sections in $\mathbb{A}^9(\mathbb{Z}_q) = \mathbb{Z}_q^9$ by X, and suppose that α is a point of X. This determines a projection $\Psi : X \to \mathbb{Z}_q^3$, under which we denote $a = \Psi(\alpha)$.

In the following we let $U \subseteq \mathbb{Z}_q^3$ be an analytic neighborhood of a, and we construct an analytic map $\Phi : U \to \mathbb{Z}_q^3$, such that $\Phi(a) = 0$. We first choose pairwise distinct polynomials

$$f_1, f_2, f_3 \in \mathbb{Z}[\{x_{ij}\}, \{y_{ij}\}]$$

from the equations (10) of Corollary 2.3, and let Ξ be the function $X \times X \to \mathbb{Z}_q^3$ given by

$$(x,y) \mapsto \big(f_1(x,y), f_2(x,y), f_3(x,y)\big).$$

By the smoothness of the ordinary locus at the prime 3 of the moduli space of abelian surfaces with symmetric theta structure of type $(\mathbb{Z}/4\mathbb{Z})^2$ we conclude that there exists an analytic local inverse $\Pi : U \to X$ of Ψ such that $\Pi(a) = \alpha$ where $U \subseteq \mathbb{Z}_q^3$ is a neighborhood of a with respect to the 3-adic topology. Note that for an arbitrary choice of square roots we have

$$\begin{aligned}
a_{01} &= \frac{\lambda}{2}\big(\sqrt{b_{00}b_{01} + b_{10}b_{11}} + \sqrt{b_{00}b_{01} - b_{10}b_{11}}\big), & a_{21} &= \frac{\lambda}{2}\big(\sqrt{b_{00}b_{01} + b_{10}b_{11}} - \sqrt{b_{00}b_{01} - b_{10}b_{11}}\big),\\
a_{10} &= \frac{\lambda}{2}\big(\sqrt{b_{00}b_{10} + b_{01}b_{11}} + \sqrt{b_{00}b_{10} - b_{01}b_{11}}\big), & a_{12} &= \frac{\lambda}{2}\big(\sqrt{b_{00}b_{10} + b_{01}b_{11}} - \sqrt{b_{00}b_{10} - b_{01}b_{11}}\big),\\
a_{11} &= \frac{\lambda}{2}\big(\sqrt{b_{00}b_{11} + b_{01}b_{10}} + \sqrt{b_{00}b_{11} - b_{01}b_{10}}\big), & a_{13} &= \frac{\lambda}{2}\big(\sqrt{b_{00}b_{11} + b_{01}b_{10}} - \sqrt{b_{00}b_{11} - b_{01}b_{10}}\big),
\end{aligned}$$

where

$$\begin{aligned}
b_{00} &= 1, & b_{01} &= \sqrt{\lambda^{-1}(a_{00}a_{02} + a_{20}a_{22})},\\
b_{20} &= \sqrt{\lambda^{-1}(a_{00}a_{20} + a_{02}a_{22})}, & b_{22} &= \sqrt{\lambda^{-1}(a_{00}a_{22} + a_{02}a_{20})},
\end{aligned}$$

and where $\lambda = (a_{00}^2 + a_{02}^2 + a_{20}^2 + a_{22}^2)/2$. The above formulas can be deduced from Mumford's 2-multiplication formula [17, §3]. We note that the zero set of b_{ij} and of

$$b_{00}b_{01} \pm b_{10}b_{11}, \quad b_{00}b_{10} \pm b_{01}b_{11}, \quad b_{00}b_{11} \pm b_{01}b_{10},$$

lie over the components of the moduli of split abelian varieties. Applying the algorithm of the previous section to such points, we may thus assume that the map is unramified at (a_{ij}).

Consider the subset $Y \subseteq X \times X$ which is defined by the equations of Corollary 2.3. Let $p_i : Y \subseteq X \times X \to X$ $(i = 1,2)$ be the map induced by the projection on the ith factor. The map p_i forms an étale covering. We can choose a local analytic section $i_1 : V \to Y$ of the projection p_1 in a neighbourhood V of α such that $i_1(\alpha) = (\alpha, \alpha^{\sigma})$. Let $\Sigma = p_2 \circ i_1$. Note that $\Sigma(\alpha) = \alpha^{\sigma}$.

By Serre-Tate theory the morphism Σ is analytic in a neighborhood of α. More precisely, this is a consequence of the representability of the local deformation space of an ordinary abelian variety over $\mathbb{F}_q$ by a formal torus and the fact that the unique lift of the relative 3-Frobenius equals up to isomorphism the 3rd powering map on this torus (see [9] and [16]).

We define Φ to be the composition

$$U \xrightarrow{\Delta} U \times U \xrightarrow{\Pi^2} X \times X \xrightarrow{\mathrm{Id}\times\Sigma} X \times X \xrightarrow{\Xi} \mathbb{Z}_q^3$$

where Δ is the diagonal map and $\Pi^2 = \Pi \times \Pi$. The equality $\Phi(a) = 0$ holds by Corollary 2.3. By the above discussion, Φ is analytic and is defined on the open disc U with center a and radius 1. The fact that the radius equals 1 can be deduced from the interpretation of the points in the image of Ψ as moduli points of abelian varieties with 2-theta structure.

In the following we verify that the assumptions of [12, Th.2] are satisfied. For an analytic function F we denote its first order derivative by D_F. We have $\Phi(x) \equiv 0 \bmod 3$ for all $x \in U$, because all points of U reduce to the same canonical theta null point satisfying the equations (9) and (10), and hence $D_\Phi(a) \equiv 0 \bmod 3$. We write D_{Ξ_X} and D_{Ξ_Y} for the submatrices of D_Ξ being the derivative of Ξ with respect to the first and second factor of the product $X \times X$. By the chain rule we conclude that

$$0 \equiv D_\Phi(a) = D_{\Xi_X}\big(\Pi(a), \Pi(a)^\sigma\big) D_\Pi(a) + D_{\Xi_Y}\big(\Pi(a), \Pi(a)^\sigma\big) D_\Sigma\big(\Pi(a)\big) D_\Pi(a) \bmod 3. \tag{31}$$

By general theory [9] the Frobenius lift acts on the Serre-Tate formal torus as the 3-rd powering map and hence $D_\Sigma\big(\Pi(a)\big) \equiv 0 \bmod 3$. We conclude by equation (31) that

$$D_{\Xi_X}\big(\Pi(a), \Pi(a)^\sigma\big) D_\Pi(a) \equiv 0 \bmod 3. \tag{32}$$

Next we prove by contradiction that for a suitable choice of the triple (f_1, f_2, f_3) (notation as above) we have

$$\det\Big(D_{\Xi_Y}\big(\Pi(a), \Pi(a)^\sigma\big) D_\Pi(a)\Big) \not\equiv 0 \bmod 3. \tag{33}$$

We remark that in the lifting algorithm the choice of the triple (f_1, f_2, f_3) has to be done depending on the initial data. Suppose condition (33) is not satisfied for any triple (f_1, f_2, f_3). Then by the Jacobi criterion we conclude that the moduli space of pairs of ordinary abelian surfaces with symmetric 4-theta structure and compatible $(3,3)$-isogeny is not smooth at the point $\big(\Pi(a), \Pi(a)^\sigma\big)$. This contradicts the fact that the latter space forms an étale covering of the smooth space X. Clearly the equations (32) and (33) imply the assumptions of [12, Th.2]. By the algorithm suggested there and the above discussion we can compute $x \in U$ such that $\Phi(x) \equiv 0 \bmod 3^m$ for given precision m with complexity as stated in the theorem.

In the following we explain why the output of the latter algorithm is indeed the theta null point of the canonical lift to given precision. We claim that for $x \in U$ one has an equivalence

$$x \equiv a \bmod 3^m \quad \Leftrightarrow \quad \Phi(x) \equiv 0 \bmod 3^m. \tag{34}$$

It suffices to prove that $\Phi(x) \equiv 0 \bmod 3^m$ implies $x \equiv a \bmod 3^m$ since the converse is obvious. The proof is done by induction on m. Assume that equivalence (34) holds for some $m \geq 1$. Assume that $\Phi(x) \equiv 0 \bmod 3^{2m}$. By the induction hypothesis we have $\delta = 3^{-m}(x - a) \in \mathbb{Z}_q^3$. Then by Taylor expansion of the analytic function Φ at a we get

$$0 \equiv \Phi(x) = \Phi(a + 3^m\delta) \equiv \Phi(a) + D_\Phi(a)3^m\delta + \ldots \equiv D_\Phi(a)3^m\delta \bmod 3^{2m}. \tag{35}$$

By equation (35) we conclude that

$$0 \equiv D_\Phi(a)\delta \bmod 3^m. \tag{36}$$

We set

$$
\begin{aligned}
D_X &= D_{\Xi_X}\big(\Pi(a), \Pi(a^\sigma)\big) D_\Pi(a), \\
D_Y &= D_{\Xi_Y}\big(\Pi(a), \Pi(a^\sigma)\big) D_\Pi(a).
\end{aligned}
$$

By (31) the equation (36) is equivalent to

$$
\delta \equiv D(\delta) \bmod 3^m \tag{37}
$$

where D is the linear operator given by

$$
y \mapsto -\left(D_Y^{-1} D_X y\right)^{\sigma^{-1}}
$$

Here we have used that the map Σ already exists as an endomorphism of U which commutes with the application Π. Note that by condition (33) the matrix D_Y is invertible. By condition (32) the entries of the matrix $D_Y^{-1} D_X$ are all divisible by 3. As a consequence we conclude from equation (37) that $\delta \equiv 0 \bmod 3^m$. This proves our claim.

In the following we will show how to compute the matrices D_X and D_Y, since they are needed for the algorithm of Lercier and Lubicz [12]. By the above discussion, we can compute compatible branches of the local inverse Π at a and a^σ such that $\Pi(a^\sigma) = \Pi(a)^\sigma$. From this it is straightforward to compute $D_{\Xi_X}\big(\Pi(a), \Pi(a^\sigma)\big)$ and $D_{\Xi_Y}\big(\Pi(a), \Pi(a^\sigma)\big)$. Next we explain how to compute $D_\Pi(a)$. Let $\Lambda : \mathbb{Z}_q^9 \to \mathbb{Z}_q^{20}$ be defined by

$$
x = (x_{ij}) \longmapsto (\Lambda_1(x), \ldots, \Lambda_{20}(x))
$$

where Λ_i are the Riemann relations (9), so that $\Lambda(\Pi(a)) = 0$. By the chain rule we conclude that

$$
D_\Lambda\big(\Pi(a)\big) D_\Pi(a) = 0. \tag{38}
$$

Let $\pi : \mathbb{Z}_q^3 \to \mathbb{Z}_q^6$ be the morphism such that $\Pi(a) = \big(a, \pi(a)\big)$. Then D_Π is the vertical join of the unit matrix of rank 3 and D_π where D_π denotes the derivative of π. We write

$$
D_\Lambda = \left(D_\Lambda^{(1)} D_\Lambda^{(2)}\right)
$$

where $D_\Lambda^{(1)}$ and $D_\Lambda^{(2)}$ have 3 and 6 columns, respectively. Note that by the smoothness of the space X the rank of $D_\Lambda^{(2)}$ at $\Pi(a)$ equals 6. There exists a matrix $T \in \mathrm{GL}_{20}(\mathbb{Z}_q)$ such that the matrix

$$
E = T \cdot D_\Lambda^{(2)}\big(\Pi(a)\big)
$$

is in echelon form. It follows from equation (38) and the above discussion that

$$
E \cdot D_\pi(a) = -T \cdot D_\Lambda^{(1)}\big(\Pi(a)\big).
$$

From this it is straightforward to compute $D_\pi(a)$ inverting the unique invertible $(6,6)$-square submatrix of E. We remark that the above computation can be done modulo any given precision. This completes the proof of Theorem 4.2. $\square$

We conclude this section by a practical remark. Our implementation uses a multivariate version of the algorithm of R. Harley (compare [28, §3.10]) for solving generalized Artin-Schreier equations instead of the the method suggested in [12].

4.5 LLL reconstruction

From the theory of complex multiplication we know that the invariants of canonical lifts are algebraic over $\mathbb{Q}$. We briefly recall the method of Gaudry et al. [8] for LLL reconstruction of algebraic relations over $\mathbb{Z}$. Let γ be a p-adic integer in an extension of degree r over $\mathbb{Z}_p$, and let m

be the precision to which it is determined. We assume that the degree n of its minimal polynomial over $\mathbb{Q}$ is known, i.e. that there exists $f(x) \in \mathbb{Z}[x]$, with

$$f(\gamma) = a_n \gamma^n + \ldots + a_0 = 0,$$

where the $a_i \in \mathbb{Z}$ are unknown. We determine a basis of the left kernel in $\mathbb{Z}^{n+r+1}$ of the vertical join of the matrix

$$\begin{bmatrix} 1 & 0 & \cdots & 0 \\ \gamma_{1,0} & \gamma_{1,1} & \cdots & \gamma_{1,(r-1)} \\ \vdots & & & \vdots \\ \gamma_{n,0} & \gamma_{n,1} & \cdots & \gamma_{n,(r-1)} \end{bmatrix}$$

with p^m times the $r \times r$ identity matrix, where $\gamma_{i,j}$ are defined by

$$\gamma^i = \gamma_{i,0} + \gamma_{i,1} w_1 + \ldots + \gamma_{i,(r-1)} w_{r-1},$$

in terms of a $\mathbb{Z}_p$ basis $\{1, w_1, \ldots, w_{r-1}\}$ for $\mathbb{Z}_q$. The minimal polynomial $f(x)$ is determined by LLL as a short vector $(a_0, \ldots, a_n, \varepsilon_1, \ldots, \varepsilon_r)$ in the kernel.

The complexity of the LLL step depends on the values r, n, and m. The values of r and n can be recovered by a curve selection and analysis of the Galois theory of the class fields. The required precision m, determined by the size of the output, is less well-understood, and we express the complexity in terms of these three parameters. Using the L^2 variant of LLL by Nguyễn and Stehlé [20], the complexity estimate of [8] gives $O((n+r)^5(n+r+m)m)$ in general, and in our case the special structure of the lattice gives a complexity of $O((n+r)^4(n+r+m)m)$.

5 Moduli equations and parametrizations

In this section we give the equations which form a higher dimensional analogue of Riemann's quartic theta relation. Then we state the classical Thomae formulas in an algebraic context, relating the invariants of genus 2 curves to theta null points. Finally we apply the algorithm of Section 4 to the construction of CM invariants of abelian surfaces and genus 2 curves.

5.1 The Thomae formulas for genus 2

Let R be an unramified local ring of odd residue characteristic, and H a hyperelliptic curve over R given by an affine equation

$$y^2 = \prod_{i=1}^{5} (x - e_i),$$

where the $e_i \in R$ are pairwise distinct in the residue field. Let (J, φ) denote the Jacobian of H where φ denotes the canonical polarization. There exists a finite unramified extension S of R and an ample symmetric line bundle $\mathcal{L}$ of degree 1 on J_S which induces the polarization φ_S. We assume that S is chosen such that there exists an S-rational symmetric theta structure Θ of type $(\mathbb{Z}/4\mathbb{Z})^2$ for the pair $(J_S, \mathcal{L})$. Let (a_{ij}), where $(i,j) \in (\mathbb{Z}/4\mathbb{Z})^2$, denote the theta null point with respect to the latter theta structure.

Theorem 5.1 (Thomae formulas) *With the notation as above, one has*

$$a_{00} = 1 \qquad a_{02} = \sqrt[4]{\frac{(e_1 - e_4)(e_2 - e_5)(e_3 - e_4)}{(e_1 - e_5)(e_2 - e_4)(e_3 - e_5)}}$$

$$a_{20} = \sqrt[4]{\frac{(e_1 - e_2)(e_1 - e_4)}{(e_1 - e_3)(e_1 - e_5)}} \qquad a_{22} = \sqrt[4]{\frac{(e_1 - e_2)(e_2 - e_5)(e_3 - e_4)}{(e_1 - e_3)(e_2 - e_4)(e_3 - e_5)}}$$

such that $a_{02}^2 = (e_1 - e_3)/(e_1 - e_2) a_{20}^2 a_{22}^2$.

For a complex analytic proof of the Thomae formulas see [19, p.120].

Conversely, let A be an abelian surface over S with ample symmetric line bundle $\mathcal{L}$ of degree 1 on A. Assume we are given a symmetric theta structure of type $(\mathbb{Z}/4\mathbb{Z})^2$ for the pair $(A, \mathcal{L}^4)$, and let (a_{ij}) denote the theta null point with respect to the latter theta structure. We associate a curve to the theta null point in the following way. Let μ be a solution of the equation (possibly over an unramified extension)

$$\mu^2 - \frac{(a_{00}^4 - a_{02}^4 + a_{20}^4 - a_{22}^4)}{(a_{00}^2 a_{20}^2 - a_{02}^2 a_{22}^2)}\mu + 1 = 0,$$

and set

$$\lambda_1 = \left(\frac{a_{00}a_{02}}{a_{22}a_{20}}\right)^2, \quad \lambda_2 = \left(\frac{a_{02}}{a_{22}}\right)^2\mu, \quad \lambda_3 = \left(\frac{a_{00}}{a_{20}}\right)^2\mu.$$

Corollary 5.2 *The curve*

$$y^2 = x(x-1)(x-\lambda_1)(x-\lambda_2)(x-\lambda_3)$$

has as Jacobian the abelian surface A.

Proof. Inverting Theorem 5.1, one verifies that the roots μ give rise to values $(\lambda_1, \lambda_2, \lambda_3)$ in the set

$$\left\{\left(\frac{e_1-e_3}{e_1-e_2}, \frac{e_1-e_4}{e_1-e_2}, \frac{e_1-e_5}{e_1-e_2}\right), \left(\frac{e_1-e_3}{e_1-e_2}, \frac{e_1-e_3}{e_1-e_5}, \frac{e_1-e_3}{e_1-e_4}\right)\right\},$$

which determine curves isomorphic to the curve with affine equation $y^2 = \prod_{i=1}^5 (x - e_i)$. □

Unfortunately, the Rosenhain invariants $(\lambda_1, \lambda_2, \lambda_3)$ of the above curve are not determined by the 2-torsion part $(a_{00} : a_{02} : a_{20} : a_{22})$ of the theta null point. Instead we must pass to a $(2,2)$-isogenous curve to determine a genus 2 curve parametrized by this theta null point.

Theorem 5.3 *The curve*

$$y^2 = x(x-1)(x-\mu_1)(x-\mu_2)(x-\mu_3),$$

where

$$\mu_1 = \frac{(a_{00}^2 + a_{02}^2 + a_{20}^2 + a_{22}^2)(a_{00}a_{02} + a_{20}a_{22})}{2(a_{00}a_{20} + a_{02}a_{22})(a_{00}a_{22} + a_{02}a_{20})}$$

$$\mu_2 = \frac{(a_{00}^2 - a_{02}^2 + a_{20}^2 - a_{22}^2)(a_{00}a_{02} + a_{20}a_{22})}{2(a_{00}a_{22} + a_{02}a_{20})(a_{00}a_{20} - a_{02}a_{22})}$$

$$\mu_3 = \frac{(a_{00}^2 + a_{02}^2 + a_{20}^2 + a_{22}^2)(a_{00}^2 - a_{02}^2 + a_{20}^2 - a_{22}^2)}{(a_{00}a_{02} + a_{20}a_{22})(a_{00}a_{02} - a_{20}a_{22})}$$

has Jacobian $(2,2)$-isogenous of the abelian surface A.

Proof. The Richelot isogeny determined by the polynomials

$$G_1 = x, \quad G_2 = (x-1)(x-\lambda_1), \quad G_3 = (x-\lambda_2)(x-\lambda_3),$$

determines a curve isomorphic to the above curve. □

Thus we obtain a rational map from the space $\mathcal{A}_2(\Theta_4[2])$, determined by the 2-torsion part $(a_{00} : a_{02} : a_{20} : a_{22})$ of a theta null point, to the moduli space $\mathcal{M}_2(2)$ of genus 2 curves with level-2 structure, determined by the Rosenhain invariants (μ_1, μ_2, μ_3). The latter point specifies an ordered six-tuple of Weierstrass points over $(\infty, 0, 1, \mu_1, \mu_2, \mu_3)$. We note that this map is defined on the open subspace outside of the components defining split abelian surfaces.

5.2 Examples of canonical lifts

In this section we give examples of canonical lifts of 3-adic theta null points. The examples were computed using implementations of our algorithms in the computer algebra system Magma [13]. Generic algorithms and databases of CM invariants for genus 2 curves can be found from the authors' web pages (see [6]).

Example 1. Consider the genus 2 hyperelliptic curve $\bar{H}$ over $\mathbb{F}_3$ defined by the equation

$$y^2 = x^5 + x^3 + x + 1.$$

Let $\bar{J}$ denote the Jacobian of $\bar{H}$. The abelian surface $\bar{J}$ is ordinary. Over an extension of degree 40 there exists a theta structure of type $(\mathbb{Z}/4\mathbb{Z})^2$ for $(\bar{J}, \mathcal{L}^4)$ where $\mathcal{L}$ is the line bundle corresponding to the canonical polarization. Let $(\bar{a}_{ij})$ denote the theta null point of $(\bar{J}, \mathcal{L}^4)$ with respect to the latter theta structure. We can assume that $\bar{a}_{00} = 1$. Note that the coordinates $\bar{a}_{02}$, $\bar{a}_{20}$ and $\bar{a}_{22}$ are defined over an extension of degree 10. We set $\mathbb{F}_{3^{10}} = \mathbb{F}_3[z]$ where $z^{10} + 2z^6 + 2z^5 + 2z^4 + z + 2 = 0$. We choose

$$\bar{a}_{02} = z^{9089}, \quad \bar{a}_{20} = z^{18300} \quad \text{and} \quad \bar{a}_{22} = z^{8601}.$$

By the algorithm described in Section 4 we lift the triple $(\bar{a}_{02}, \bar{a}_{20}, \bar{a}_{22})$ to the unramified extension of $\mathbb{Z}_3$ of degree 10. We denote the lifted coordinates by a_{02}, a_{20} and a_{22}. Let P_{ij} be the minimal polynomial of a_{ij} over $\mathbb{Q}$. A search for algebraic relations using the LLL-algorithm yields

$$\begin{aligned}
P_{02} &= x^{80} - 69x^{76} + 4911x^{72} + 20749x^{68} + 299094x^{64} - 202217x^{60} \\
&\quad +1093161x^{56} - 7393871x^{52} + 11951456x^{48} + 7541235x^{44} \\
&\quad -26349059x^{40} + 7541235x^{36} + 11951456x^{32} - 7393871x^{28} \\
&\quad +1093161x^{24} - 202217x^{20} + 299094x^{16} + 20749x^{12} + 4911x^{8} \\
&\quad -69x^{4} + 1, \\
P_{20} &= x^{20} - 5x^{19} + 23x^{18} - 53x^{17} + 112x^{16} - 203x^{15} + 279x^{14} - 345x^{13} \\
&\quad +360x^{12} - 333x^{11} + 329x^{10} - 333x^{9} + 360x^{8} - 345x^{7} + 279x^{6} \\
&\quad -203x^{5} + 112x^{4} - 53x^{3} + 23x^{2} - 5x + 1, \\
P_{22} &= x^{80} + 5x^{76} + 184x^{72} + 2254x^{68} + 4470x^{64} + 160109x^{60} + 768428x^{56} \\
&\quad +421488x^{52} + 36971535x^{48} - 75225290x^{44} + 44767882x^{40} \\
&\quad -43287046x^{36} + 86078086x^{32} - 75568556x^{28} + 31873762x^{24} \\
&\quad -7293064x^{20} + 989181x^{16} - 32859x^{12} + 4318x^{8} + 44x^{4} + 1.
\end{aligned}$$

We conclude that the field k_0 generated by the coordinates a_{02}, a_{20} and a_{22} is a Galois extension of $\mathbb{Q}$ having degree 160. Note that k_0 contains $\mathbb{Q}(i)$.

The characteristic polynomial of the absolute Frobenius endomorphism of $\bar{J}$ equals

$$x^4 + 3x^3 + 5x^2 + x + 9.$$

Let $K = \mathrm{End}_{\mathbb{F}_3}(\bar{J}) \otimes \mathbb{Q}$. The field K is a normal CM field of dimension 4 whose Galois group equals $\mathbb{Z}/4\mathbb{Z}$. The class number of K equals 1. The maximal totally real subfield of K is given by $\mathbb{Q}(\sqrt{13})$. Note that K equals its own reflex field K^*. The compositum k_0K^* forms an abelian extension of K^* having conductor 8 and Galois group $(\mathbb{Z}/2\mathbb{Z})^2 \times \mathbb{Z}/10\mathbb{Z}$. Note that the polynomial P_{20} generates the ray class field of K^* modulo 2.

We remark that the curve H with defining equation

$$y^2 = 52x^5 - 156x^4 + 208x^3 - 156x^2 + 64x - 11$$

is a canonical lift of $\bar{H}$ in the sense that H reduces to the curve $\bar{H}$ and the Jacobian of H is isomorphic to the canonical lift of $\bar{J}$. For a list of curves of genus 2 over $\mathbb{Q}$ having complex multiplication we refer to [27].

Example 2. Let $\bar{H}$ be the hyperelliptic curve over $\mathbb{F}_{3^6} = \mathbb{F}_3[z]$ where $z^3 - z + 1 = 0$, defined by the affine equation

$$y^2 = x(x-1)(x-z)(x-z^8)(x-z^2).$$

We may associate a theta null point to $\bar{H}$ over an extension and apply our algorithm to determine the canonical lifted Rosenhain invariants from the lift of the theta null point. By LLL reconstruction, the Igusa invariants

$$j_1 = \frac{J_2^5}{J_{10}}, \quad j_2 = \frac{J_2^3 J_4}{J_{10}}, \quad j_4 = \frac{J_2 J_8}{J_{10}},$$

of the canonically lifted curve H satisfy the minimal polynomials

$$\begin{aligned}
&116757924411252876637960400005285561864702968 3j_1^6\\
&\quad - 1525767784980361395557123622213314279362766603989013154811084 8j_1^5\\
&\quad + 11961318792770942132132378266256566166672909862164391206962387695981035 52j_1^4\\
&\quad - 150269018396453856629059955144199405450450308907846393164867913708931692416204 8j_1^3\\
&\quad + 94949600514980451348563662445123861714429688472687490461831537573194959983476736000 00j_1^2\\
&\quad - 9489242494532768198621993753759532669268063460725268563272920396343489385558179840000000 0j_1\\
&\quad + 3154745183558232433309182902721654489400212652045192101874580090073682713333727232000000000000000 0
\end{aligned}$$

$$\begin{aligned}
&315246395910382766922493080014271017034698014 41j_2^6\\
&\quad - 1674563480772362082820759294084403649513820408562842840911052 8j_2^5\\
&\quad - 12265164179615739710029144012197055859859725320474999182497036825001984j_2^4\\
&\quad + 3521417753190328034602856404605304284768052270328078417883753670682859274 24j_2^3\\
&\quad - 115886117015701373170818041387627276397709556079989081954770457714548434534400000j_2^2\\
&\quad + 6241088101000204747012315559761320786612924621590641411279130896395801722880000000000j_2\\
&\quad - 119116948667007461483450210289814155018636097544277843858343319784591982592000000000000000
\end{aligned}$$

$$\begin{aligned}
&2298146226186690370864974553304035714182948525048 9j_4^6\\
&\quad - 383331333858223309758723425956263962397050002437871963112463 36j_4^5\\
&\quad - 13445890564402694049486311582599736771794395285600128293985309687808j_4^4\\
&\quad - 25587083283087299157726904789352095023627415391850896175427316095123456j_4^3\\
&\quad - 209226530786623089829458949348683221193067366018178627955988245271019520 00j_4^2\\
&\quad - 61259814230097056731768967829978518304429009163243510825472679508705280000 00j_4\\
&\quad - 12260055755474262524570670484641566489377734821667749961858456108400640000000000
\end{aligned}$$

We note that neither of these Jacobians has good ordinary reduction at 2, thus extend the realm of applicability of the 2-adic CM method [8].

6 Conclusion and perspectives

This work generalizes prior higher dimensional 2-adic canonical lifting algorithms to a 3-adic setting. Firstly, in Theorem 2.1, we introduce the moduli equations which provide the higher dimensional analogues of the modular curve $X_0(3)$. Secondly, we describe a general multivariate Hensel lifting algorithm in an analytic framework (removing the need for a rational parametrization of a variety). As an application our work gives an explicit CM construction for moduli of genus 2 curves (and their Jacobian surfaces), yielding a 3-adic alternative to the 2-adic construction of Gaudry et al. [8], and extending the domain of applicability to additional quartic CM fields. We expect that our method extends to primes $p > 3$, for which the primary ingredient will be an analogue of our Theorem 2.1. With an increasing complexity for the resulting schemes, as both p and the dimension grow, we expect our approach through analytic parametrizations will become essential.

Acknowledgments. We are grateful to Y. Kopeliovich for explaining his results and for giving some very valuable references to the literature.

References

[1] C. Birkenhage, H. Lange. *Complex abelian varieties*, Springer, 2004.

[2] R. Carls. *Canonical coordinates on the canonical lift.* J. Ramanujan Math. Soc. 22(1), p. 1–14, 2007.

[3] R. Carls. *Theta null points of* 2*-adic canonical lifts.*
A preprint is available at `http://arxiv.org/math.NT/0509092`.

[4] H. Cohen, G. Frey, R. Avanzi, C. Doche, T. Lange, K. Nguyen, F. Vercauteren (eds.). *Handbook of elliptic and hyperelliptic curve cryptography.* Discrete Mathematics and its Applications, Chapman & Hall/CRC, 2006.

[5] J.-M. Couveignes, T. Henocq. Action of modular correspondences around CM points. In proceedings of the *Algorithmic Number Theory Symposium ANTS-V*, LNCS 2369, p. 234–243, Springer, 2002.

[6] Kohel et al. *Magma share code.* Available at `http://www.maths.usyd.edu.au/u/kohel/alg`.

[7] P. Gaudry. A comparison and a combination of SST and AGM algorithms for counting points of elliptic curves in characteristic 2. In *Advances in cryptology—Asiacrypt 2002*, LNCS 2501, p. 621–628, Springer, 2002.

[8] P. Gaudry, T. Houtmann, D. Kohel, C. Ritzenthaler, and A. Weng. A 2-adic CM method for genus 2 curves with application to cryptography. In *Advances in cryptology—Asiacrypt 2006*, LNCS 4284, p. 114–129, Springer, 2006.

[9] N. Katz. Serre-Tate local moduli. In *Surfaces algébriques*, LNM 868, p. 138–202, Springer, 1981.

[10] Y. Kopeliovich. Multi-dimensional theta constant identities. *Journ. Geom. Analysis* 8(4), p. 571–581, 1998.

[11] R. Lercier, D. Lubicz. Counting Points on Elliptic Curves over Finite Fields of Small Characteristic in Quasi Quadratic Time. In *Advances in cryptology – Eurocrypt 2003*, LNCS 2656, Springer, 2003.

[12] R. Lercier, D. Lubicz. A quasi-quadratic time algorithm for hyperelliptic curve point counting. *Ramanujan J.* 12(3), p. 399–423, 2006.

[13] J. Cannon, W. Bosma (eds.). The Magma Handbook. `http://magma.maths.usyd.edu.au/magma/htmlhelp/MAGMA.htm`.

[14] J.-F. Mestre. Lettre à Gaudry et Harley, 2001.
Available at `http://www.math.jussieu.fr/~mestre`.

[15] J.-F. Mestre. Talk given at the Cryptography Seminar Rennes, 2002. Notes available at `http://www.math.univ-rennes1.fr/crypto/2001-02/mestre.ps`.

[16] B. Moonen. *Special points and linearity properties of Shimura varieties.* PhD thesis, Universiteit Utrecht, 1995.

[17] D. Mumford. On the equations defining abelian varieties I. *Invent. Math.* 1, p. 287–354, 1966.

[18] D. Mumford. On the equations defining abelian varieties II. *Invent. Math.* 3, p. 75–135, 1967.

[19] D. Mumford. *Tata lectures on theta II: Jacobian theta functions and differential equations.* Birkhäuser, 1984.

[20] P. Nguyễn, D. Stehlé. Floating-point LLL revisited. In *Advances in cryptology – Eurocrypt 2005*, LNCS 3494, p. 215–233, Springer, 2005.

[21] C.H. Papadimitriou. *Computational complexity.* Addison-Wesley, 1994.

[22] C. Ritzenthaler. *Problèmes arithmétiques relatifs à certaines familles de courbes sur les corps finis.* PhD thesis, Université Paris 7, 2003.

[23] B. Runge. Endomorphism rings of abelian surfaces and projective models of their moduli spaces. *Tohoku Math. J.* 51(3), 2nd Ser., p. 283–303, 1999.

[24] T. Satoh. The canonical lift of an ordinary elliptic curve over a finite field and its point counting. *J. Ramanujan Math. Soc.* 15(4), p. 247–270, 2000.

[25] T. Satoh, B. Skjernaa, and Y. Taguchi. Fast computation of canonical lifts of elliptic curves and its application to point counting. *Finite Fields and Their Applications* 9(1), p. 89–101, 2003.

[26] J.H. Silverman. *Advanced topics in the arithmetic of elliptic curves.* GTM 151, Springer, 1994.

[27] P. Van Wamelen. Examples of genus two CM curves defined over the rationals. *Math. Comp.* 68, p. 307–320, 1999.

[28] F. Vercauteren. *Computing zeta functions of curves over finite fields.* PhD thesis, Katholieke Universiteit Leuven, 2003.

[29] F. Vercauteren, B. Preneel, J. Vandewalle. A memory efficient version of Satoh's algorithm. In *Advances in cryptology – Eurocrypt 2001*, LNCS 2045, p. 1–13, Springer, 2001.