Modular invariants for genus 3 hyperelliptic curves

Sorina Ionica, Pinar Kilicer, Kristin Lauter, Elisa Lorenzo García, Adelina Manzateanu, Maike Massierer, Christelle Vincent

MODULAR INVARIANTS FOR GENUS 3 HYPERELLIPTIC CURVES

SORINA IONICA, PINAR KILIÇER, KRISTIN LAUTER, ELISA LORENZO GARCÍA, MAIKE MASSIERER, ADELINA MĂNZĂŢEANU, AND CHRISTELLE VINCENT

Abstract. In this article we prove an analogue of a theorem of Lachaud, Ritzenthaler, and Zykin, which allows us to connect invariants of binary octics to Siegel modular forms of genus 3. We use this connection to show that certain modular functions, when restricted to the hyperelliptic locus, assume values whose denominators are products of powers of primes of bad reduction for the associated hyperelliptic curves. We illustrate our theorem with explicit computations. This work is motivated by the study of the value of these modular functions at CM points of the Siegel upper-half space, which, if their denominators are known, can be used to effectively compute models of (hyperelliptic, in our case) curves with CM.

1. Introduction

Given a CM field K, Shimura and Taniyama's Complex Multiplication Theory shows that the values of Siegel modular functions evaluated at points with CM by $\mathcal{O}_K$, the maximal order of K, in the Siegel upper half-space lie in an abelian extension of the reflex field of K with prescribed ramification. Because of the classical connection between the ideal class group of K and the construction of the points with CM by $\mathcal{O}_K$ in the Siegel upper half-space, these modular functions are often called *modular invariants*, and the minimal polynomials of their CM values are called *class polynomials*.

For example, in the genus 1 case, the field of modular functions of level 1 is generated by the j-invariant. It is well known that adjoining the j-invariant of an elliptic curve with endomorphism ring $\mathcal{O}_K$ to K generates the Hilbert class field of K. Furthermore, one can then construct an elliptic curve with this given j-invariant, thus giving an elliptic curve with endomorphism ring $\mathcal{O}_K$. In the genus 2 case, the field of Siegel modular functions of level 1 is generated by the absolute Igusa invariants [Igu62]. Similarly, when evaluated at CM points corresponding to a primitive quartic CM field, their values give invariants of hyperelliptic curves whose Jacobian has complex multiplication, and the curve can be recovered from the invariants. As a consequence, the effective computation of the values of Siegel modular forms at CM points makes it possible to compute models for CM curves, and also to effectively construct the related class fields.

In the genus 2 case, there is an obstacle to this effective computation. Indeed, while the j-invariant is an algebraic integer, the Igusa invariants are algebraic numbers and the running time for their computation can be greatly improved when a good description of the denominators is at hand. It is well known that the primes

2010 *Mathematics Subject Classification.* 11G15, 14K22.

Maike Massierer was supported by the Australian Research Council (DP150101689).

appearing in these denominators are primes of bad reduction for the hyperelliptic curves. Building on the work of Goren and Lauter [GL07], who gave a bound for these primes, Lauter and Viray [LV15b, LV15a] gave a formula for computing a multiple of the denominators of Igusa invariants for an arbitrary primitive quartic field.

In genus 3, the situation is more complicated and hence more interesting. Indeed, even though the algebra of Siegel modular forms is known [Tsu86, Tsu87], there is no "standard" set of generators for the field of Siegel modular functions for which one might compute class polynomials. Thankfully, one can work around this difficulty in the following way: Matsusaka and Ran [Mat59, Ran81] prove that up to isomorphism over $\mathbb{C}$, every simple principally polarized abelian variety of dimension 3 is the Jacobian of a complete smooth projective curve of genus 3. Furthermore, if C is such a curve, then by the Riemann–Roch Theorem, C is isomorphic to either a hyperelliptic or a plane quartic curve. The hyperelliptic and the plane quartic loci, when considered separately, do each have a standard set of invariants. For hyperelliptic curves of genus 3, these are the Shioda invariants [Shi67], and in the plane quartic case, one can use the Dixmier–Ohno invariants [Dix87, Ohn05].

For many applications (and especially the explicit construction of genus 3 curves with complex multiplication), it would be interesting to relate these invariants to a set of modular analogues, that can be computed in terms of a generating set of Siegel modular functions. However, in contrast to the genus 2 case, little is known on the relation between these invariants and the Siegel modular function field of degree 3 as of yet. This work takes steps in this direction.

We focus in this work on the hyperelliptic locus. In [Igu67], Igusa defines two distinguished Siegel modular forms of genus 3,

$$\Sigma_{140}(Z) = \sum_{i=1}^{36} \prod_{j \neq i} \vartheta[\xi_j](0, Z)^8 \tag{1.1}$$

and

$$\chi_{18}(Z) = \prod_{i=1}^{36} \vartheta[\xi_i](0, Z),$$

where for simplicity of notation the 36 even theta characteristics have been ordered arbitrarily (we define the even theta characteristics in Section 2.2). In the same article, Igusa shows that $\Sigma_{140}(Z)$ vanishes exactly on the locus of period matrices Z that are symplectically reducible (this is equivalent to requiring that the associated polarized abelian variety is isomorphic to a product of lower-dimensional polarized abelian varieties), and $\chi_{18}(Z)$ vanishes on the locus of period matrices Z whose associated principally polarized abelian variety is a hyperelliptic Jacobian.

In this paper we introduce a family of modular functions of degree 3 who, when evaluated on the hyperelliptic locus, yield values whose denominators are the primes of bad reduction for the hyperelliptic curve. To do so, we begin by establishing an analogue of a result of Lachaud, Ritzenthaler, and Zykin [LRZ10, Corollary 3.3.2], and then extend and rephrase a result of Lockhart [Loc94, Proposition 3.2] on the discriminant of the hyperelliptic curve, to prove the following theorem:

Theorem 1.1. *Let Z be a CM point in $\mathcal{H}_3$ corresponding to a smooth genus 3 hyperelliptic curve C with CM by the ring of integers of a sextic CM field K and CM type Φ_K. Let f be a Siegel modular form of weight k such that the invariant Φ*

obtained in Corollary 3.6 is integral. Then

$$j(Z) = \frac{f^{\frac{140}{\gcd(k,140)}}}{\Sigma_{140}^{\frac{k}{\gcd(k,140)}}}(Z)$$

is an algebraic number lying in the compositum $F = H_{K^r}L$ of the field L and the Hilbert class field H_{K^r} of the reflex field K^r of the CM type (K, Φ_K). Moreover, if an odd prime $\mathfrak{p}$ of $\mathcal{O}_F$ divides the denominator of this number, then the curve C has geometrically bad reduction modulo $\mathfrak{p}$.

To illustrate this theorem, we computed values of certain modular invariants, whose expressions have a power of Σ_{140} in the denominator and showed that they exhibit the behavior predicted by the Theorem. For our experiments, we used genus 3 hyperelliptic CM curves defined over $\mathbb{Q}$, a complete list of which is given in [KS16b].

Outline. This paper is organized as follows. We begin in Section 2 with some background on CM theory, theta functions and theta constants and the Shioda invariants of hyperelliptic curves. Only the most basic facts are given, and references are provided for the reader who would like to delve further.

Then, in Section 3, we give a correspondence that allows us to relate invariants of octics to Siegel modular forms of degree 3. Using this correspondence, we show that the primes dividing the denominators of modular invariants that have the Siegel modular form Σ_{140} in the denominator are primes of bad reduction, which is our main theorem (Theorem 1.1 above).

Finally, in Section 4 we present the complete set of hyperelliptic curves of genus 3 with complex multiplication and defined over $\mathbb{Q}$. These curves are used as examples for which we compute the values of several modular invariants having Σ_{140} in the denominator evaluated at a period matrix of their Jacobian, and compare their factorization against that of the denominators of the Shioda invariants of these curves and the odd primes of bad reduction of these curves.

2. Hyperelliptic curves of genus 3 with complex multiplication

In this section we introduce quickly the notation we will use to discuss abelian varieties with complex multiplication by the ring of integers of a CM field K and their period matrices. We then discuss theta functions and theta characteristics, as they are crucial to the definition of the Siegel modular invariants we consider in this paper. Finally, we discuss the invariants of hyperelliptic curves.

2.1. CM abelian varieties and period matrices.

In this Section we quickly present some basic facts of the construction of CM abelian varieties, based on the work of Shimura and Taniyama [Shi98].

Let K be a CM field of degree $2g$ (i.e., a totally imaginary quadratic extension of a totally real number field of degree g) over $\mathbb{Q}$, and let $\mathcal{O}$ be an order of the ring of integers of K. We say that an abelian variety $\mathcal{A}$ defined over a field k *has CM by* $\mathcal{O}$ if there exists an embedding $\mathcal{O} \hookrightarrow \mathrm{End}(\mathcal{A})$, where $\mathrm{End}(\mathcal{A})$ is the geometric endomorphism ring of $\mathcal{A}$. In this article we focus on the case where $\mathrm{End}(\mathcal{A}) \cong \mathcal{O}_K$, the ring of integers of K.

A *CM type* of K is a set $\Phi_K = \{\phi_1, \ldots, \phi_g\}$ of g embeddings $K \hookrightarrow \mathbb{C}$ such that no two embeddings appearing in Φ_K are complex conjugates. We say that Φ_K is

induced from a CM subfield K_0 of K if the set $\{\phi|_{K_0} : \phi \in \Phi_K\}$ is a CM type of K_0. A CM type of K is called *primitive* if it is not induced by a proper CM subfield $K_0 \subset K$. In the case where K is quartic, if all of its CM types are primitive we say that K is a primitive quartic CM field.

Given a pair (K, Φ_K) formed of a CM field and one of its CM types, there exists an algorithm to generate data associated to each principally polarized abelian variety with CM by $\mathcal{O}_K$ and of CM type Φ_K. First steps towards this were taken by [vW99], who gave an algorithm which enumerates all principally polarized abelian varieties with CM by the ring of integers of a given CM field, and the algorithm was completed by Streng [Str14] so that every principally polarized abelian variety is listed only once, up to isomorphism. We refer the interested reader to their work for more details and only note here that our work uses this theory in Section 4 for the computations.

The way in which we will interact with this data in this work is via a *period matrix* for the abelian variety. In this work, by period matrix we will mean a $g \times g$ symmetric matrix Z with positive imaginary part. In this case, the relationship between the abelian variety and the period matrix is that the complex points of the abelian variety are exactly the torus $\mathbb{C}^g/(\mathbb{Z}^g + Z\mathbb{Z}^g)$. We denote the space of all such matrices by $\mathcal{H}_g$. There exist several good references that show how to do so; we refer the reader to [BILV16a, Appendix A] for a particularly quick treatment.

2.2. **Theta functions and theta characteristics.** We now turn our attention to the subject of theta functions. For $\omega \in \mathbb{C}^g$ and $Z \in \mathcal{H}_g$, we define the following important series:

$$\vartheta(\omega, Z) = \sum_{n \in \mathbb{Z}^g} \exp(\pi i n^T Z n + 2\pi i n^T \omega). \tag{2.1}$$

Given a period matrix $Z \in \mathcal{H}_g$, we obtain a set of coordinates on the torus $\mathbb{C}^g/(\mathbb{Z}^g + Z\mathbb{Z}^g)$ in the following way: A vector $x \in [0,1)^{2g}$ corresponds to the point $x_2 + Zx_1 \in \mathbb{C}^g/(\mathbb{Z}^g + Z\mathbb{Z}^g)$, where x_1 denotes the first g entries and x_2 denotes the last g entries of the vector x of length $2g$.

For reasons beyond the scope of this short text, it is of interest to consider the value of this theta function as we translate ω by points that, under the natural quotient map $\mathbb{C}^g \to \mathbb{C}^g/(\mathbb{Z}^g + Z\mathbb{Z}^g)$, map to 2-torsion points. These points are of the form $\xi_2 + Z\xi_1$ for $\xi \in (1/2)\mathbb{Z}^{2g}$. This motivates the following definition:

$$\vartheta[\xi](\omega, Z) = \exp(\pi i \xi_1^T Z \xi_1 + 2\pi i \xi_1^T(\omega + \xi_2))\vartheta(\omega + \xi_2 + Z\xi_1, Z),$$

which is given in [Mum07a, page 123]. In this context, ξ is customarily called a *characteristic* or *theta characteristic*. The value $\vartheta[\xi](0, Z)$ is called a *theta constant*.

For $\xi \in (1/2)\mathbb{Z}^{2g}$, let

$$e_*(\xi) = \exp(4\pi i \xi_1^T \xi_2). \tag{2.2}$$

We say that a characteristic $\xi \in (1/2)\mathbb{Z}^{2g}$ is *even* if $e_*(\xi) = 1$ and *odd* if $e_*(\xi) = -1$. If ξ is even we call $\vartheta[\xi](0, Z)$ an *even theta constant* and if ξ is odd we call $\vartheta[\xi](0, Z)$ an *odd theta constant*.

We have the following fact about the series $\vartheta[\xi](\omega, Z)$ [Mum07a, Chapter II, Proposition 3.14]: For $\xi \in (1/2)\mathbb{Z}^{2g}$,

$$\vartheta[\xi](-\omega, Z) = e_*(\xi)\vartheta[\xi](\omega, Z).$$

From this we conclude that all odd theta constants vanish. Furthermore, we have that if $n \in \mathbb{Z}^{2g}$ is a vector with integer entries,

$$\vartheta[\xi + n](\omega, Z) = \exp(2\pi i \xi_1^T n_2)\vartheta[\xi](\omega, Z).$$

In other words, if ξ is modified by a vector with integer entries, the theta value at worst acquires a factor of -1.

We can now finally fully describe and justify the definitions of the Siegel modular forms Σ_{140} and χ_{18} given in the Introduction, which are due to Igusa [Igu67]. Indeed, their definition rests on a certain vanishing behavior for the theta constants associated to a hyperelliptic period matrix in genus $g = 3$ that was noticed by Igusa. Since we remarked above that all odd theta constants vanish and the vanishing or non-vanishing of an even theta constant is unaffected by its class modulo $\mathbb{Z}^6$, it suffices, if we are concerned with vanishing, to consider classes in $(1/2)\mathbb{Z}^6/\mathbb{Z}^6$. As in the Introduction, we note that there are exactly 36 even classes in that set. This explains the notation we used.

2.3. **Shioda Invariants and class polynomials.** We lastly turn our attention to the invariants under study in this article. In [Shi67], the author gives a set of generators for the algebra of invariants of binary octavics over the complex numbers, which are now called *Shioda invariants*. In addition, over the complex numbers Shioda invariants completely classify isomorphism classes of hyperelliptic curves of genus 3. More specifically, the Shioda invariants are 9 weighted projective invariants $(J_2, J_3, J_4, J_5, J_6, J_7, J_8, J_9, J_{10})$, where J_i has degree i, and $J_2, \ldots, J_7$ are algebraically independent, while J_8, J_9, J_{10} depend algebraically on the previous Shioda invariants.

In [LR12], the authors show that those invariants are also generators of the algebra of invariants and determine hyperelliptic genus 3 curves up to isomorphism in characteristic $p > 7$. Later, in his thesis [Bas15], Basson provided some extra invariants that together with the classical Shioda invariants classify hyperelliptic curves of genus 3 up to isomorphism in characteristic 3 and 7. The characteristic 5 case is still an unpublished work.

We note that the discriminant Δ of a hyperelliptic curve C of genus 3, which we will give in formula (3.1), is an invariant of degree 14 (Section 1.5 in [LR12]), and that it does not appear in this generating set of invariants. We consider the following absolute[1] Shioda invariants:

$$\begin{aligned}\mathrm{Shioda}_{\mathrm{abs}}(C) = (&J_2^7/\Delta, J_3^{14}/\Delta^3, J_4^7/\Delta^2, J_5^{14}/\Delta^5, J_6^7/\Delta^3,\\ &J_7^2/\Delta, J_8^7/\Delta^4, J_9^{14}/\Delta^9, J_{10}^7/\Delta^5).\end{aligned}$$

3. Denominators of modular invariants and primes of bad reduction

The aim of this Section is to prove Theorem 1.1, which can be found in the Introduction, and which is an analogue to Corollary 5.1.2 of [GL07] for hyperelliptic curves of genus 3. While the result was certainly greatly inspired by this reference, the proof we present here does not follow the template of the proof of the original theorem, as we ran into difficulties generalizing certain parts of the argument. The proof of this result has three main ingredients. We first adapt to the case of hyperelliptic curves a result of Lachaud, Ritzenthaler and Zykin [LRZ10] that connects invariants of curves to Siegel modular forms. We then generalize a result of

[1] An absolute invariant is a ration of homogeneous invariants of the same degree.

Lockhart [Loc94] to specifically connect the discriminant of a hyperelliptic curve to the Siegel modular form Σ_{140} of equation (1.1). Finally, we deduce the divisibility of Σ_{140} by an odd prime $\mathfrak{p}$ to the bad reduction of the curve using a result of Kılıçer, Lauter, Lorenzo García, Newton, Ozman, and Streng [KLLG$^+$16].

3.1. **Invariants of hyperelliptic curves and Siegel modular forms.** The aim of this section is to establish an analogue for the hyperelliptic locus of Corollary 3.3.2 of [LRZ10]. Our result, while technically new, does not use any ideas that do not appear in the original paper. We begin by establishing the basic ingredients necessary, using the same notation as in [LRZ10] for clarity, and with the understanding that, when omitted, all details may be found in *loc. cit.*

Roughly speaking, the main idea of the proof is to compare three different "flavors" of modular forms and invariants of non-hyperelliptic curves (which will here be replaced with invariants of hyperelliptic curves). The comparison goes as follows: to connect analytic Siegel modular forms to invariants of curves, the authors first connect analytic Siegel modular forms to geometric modular forms. Following this, geometric modular forms are connected to Teichmüller modular forms, via the Torelli map and a result of Ichikawa. Finally Teichmüller forms are connected to invariants of curves.

3.2. **From analytic Siegel modular forms to geometric Siegel modular forms.** Let $\mathbf{A}_g$ be the moduli stack of principally polarized abelian schemes of relative dimension g, and $\pi\colon \mathbf{V}_g \to \mathbf{A}_g$ the universal abelian scheme with zero section $\epsilon\colon \mathbf{A}_g \to \mathbf{V}_g$. Then the relative canonical line bundle over $\mathbf{A}_g$ is given in terms of the rank g bundle of relative regular differential forms of degree one on $\mathbf{V}_g$ over $\mathbf{A}_g$ by the expression

$$\boldsymbol{\omega} = \bigwedge^g \epsilon^* \Omega^1_{\mathbf{V}_g/\mathbf{A}_g}.$$

With this notation, a *geometric Siegel modular form of genus g and weight h*, for h a positive integer, over a field k, is an element of the k-vector space

$$\mathbf{S}_{g,h}(k) = \Gamma(\mathbf{A}_g \otimes k, \boldsymbol{\omega}^{\otimes h}).$$

If $f \in \mathbf{S}_{g,h}(k)$ and A is a principally polarized abelian variety of dimension g defined over k equipped with a basis α of the 1-dimensional space $\boldsymbol{\omega}_k(A) = \bigwedge^g \Omega^1_k(A)$, we define

$$f(A, \alpha) = \frac{f(A)}{\alpha^{\otimes h}}.$$

In this way $f(A, \alpha)$ is an algebraic or geometric modular form in the usual sense, i.e.,

(1) $f(A, \lambda\alpha) = \lambda^{-h} f(A, \alpha)$ for any $\lambda \in k^\times$, and
(2) $f(A, \alpha)$ depends only on the $\bar{k}$-isomorphism class of the pair (A, α).

Conversely, such a rule defines a unique $f \in \mathbf{S}_{g,h}$.

We first compare these geometric Siegel modular forms to the usual analytic Siegel modular forms:

Proposition 3.1 (Proposition 2.2.1 of [LRZ10])**.** *Let $\mathbf{R}_{g,h}(\mathbb{C})$ denote the usual space of analytic Siegel modular forms of genus g and weight h. Then there is an isomorphism*

$$\mathbf{S}_{g,h}(\mathbb{C}) \to \mathbf{R}_{g,h}(\mathbb{C}),$$

given by sending $f \in \mathbf{S}_{g,h}(\mathbb{C})$ *to*

$$\tilde{f}(Z) = \frac{f(A_Z)}{(2\pi i)^{gh}(dz_1 \wedge \ldots \wedge dz_g)^{\otimes h}},$$

where $A_Z = \mathbb{C}^g/(\mathbb{Z}^g + Z\mathbb{Z}^g)$, $Z \in \mathcal{H}_g$ *and each* $z_i \in \mathbb{C}$.

Furthermore, this isomorphism has the following pleasant property:

Proposition 3.2 (Proposition 2.4.4 of [LRZ10])**.** *Let* (A, a) *be a principally polarized abelian variety of dimension* g *defined over* $\mathbb{C}$*, let* $\omega_1, \ldots, \omega_g$ *be a basis of* $\Omega^1_{\mathbb{C}}(A)$ *and let* $\omega = \omega_1 \wedge \ldots \wedge \omega_g \in \boldsymbol{\omega}_{\mathbb{C}}(A)$*. If* $\Omega = (\,\Omega_1\ \Omega_2\,)$ *is a Riemann matrix obtained by integrating the forms* ω_i *against a basis of* $H_1(A, \mathbb{Z})$ *for the polarization* a*, then* $Z \in \mathcal{H}_g = \Omega_2^{-1}\Omega_1$*, and*

$$f(A, \omega) = (2\pi i)^{gh}\frac{\tilde{f}(Z)}{\det \Omega_2^h}.$$

3.3. **From geometric Siegel modular forms to Teichmüller modular forms.** We now turn our attention to so-called Teichmüller modular forms, which were studied by Ichikawa [Ich94, Ich95, Ich96, Ich00]. Let $\mathbf{M}_g$ be the moduli stack of curves of genus g, let $\pi\colon \mathbf{C}_g \to M_g$ be the universal curve, and let

$$\boldsymbol{\lambda} = \bigwedge^g \pi_* \Omega^1_{\mathbf{C}_g/\mathbf{M}_g}$$

be the invertible sheaf associated to the Hodge bundle.

With this notation, a *Teichmüller modular form of genus* g *and weight* h, for h a positive integer, over a field k, is an element of the k-vector space

$$\mathbf{T}_{g,h}(k) = \Gamma(\mathbf{M}_g \otimes k, \boldsymbol{\lambda}^{\otimes h}).$$

As before, if $f \in \mathbf{T}_{g,h}(k)$ and C is a curve of genus g defined over k equipped with a basis λ of $\boldsymbol{\lambda}_k(C) = \bigwedge^g \Omega^1_k(C)$, we define

$$f(C, \lambda) = \frac{f(C)}{\lambda^{\otimes h}}.$$

Again, $f(C, \lambda)$ is an algebraic modular form in the usual sense. Ichikawa proves:

Proposition 3.3 (Proposition 2.3.1 of [LRZ10])**.** *The Torelli map* $\theta\colon \mathbf{M}_g \to \mathbf{A}_g$*, associating to a curve* C *its Jacobian* $\operatorname{Jac} C$ *with the canonical polarization* j*, satisfies* $\theta^*\boldsymbol{\omega} = \boldsymbol{\lambda}$*, and induces for any field a linear map*

$$\theta^*\colon \mathbf{S}_{g,h}(k) \to \mathbf{T}_{g,h}(k)$$

such that $(\theta^* f)(C) = \theta^*(f(\operatorname{Jac} C))$*. In other words, for a basis* λ *of* $\boldsymbol{\lambda}_k(C)$ *and fixing* α *such that* $\theta^*\alpha = \lambda$*,*

$$f(\operatorname{Jac} C, \alpha) = (\theta^* f)(C, \lambda).$$

3.4. **From Teichmüller modular forms to invariants of binary forms.** We finally connect the Teichmüller modular forms to invariants of hyperelliptic curves. To this end, let E be a vector space of dimension 2 over a field k of characteristic different from 2, and put $G = \mathrm{GL}(E)$ and $\mathbf{X}_d = \mathrm{Sym}^d(E^*)$, the space of homogeneous polynomials of degree d on E. We define the action of G on $\mathbf{X}_d$, $u \cdot F$ for $F \in \mathbf{X}_d$, by

$$(u \cdot F)(x, z) = F(u^{-1}(x, z)).$$

(By a slight abuse of notation we denote an element of E by the pair (x, z), effectively prescribing a basis. Our reason to do so will become clear later.)

We say that Φ is an *invariant of degree* h if Φ is a regular function on $\mathbf{X}_d$, homogeneous of degree h (by which we mean that $\Phi(\lambda F) = \lambda^h \Phi(F)$ for $\lambda \in k^\times$ and $F \in \mathbf{X}_d$) and

$$u \cdot \Phi = \Phi \quad \text{for every} \quad u \in \mathrm{SL}(E),$$

where the action $u \cdot \Phi$ is given by

$$(u \cdot \Phi)(F) = \Phi(u^{-1} \cdot F).$$

We note the space of invariants of degree h by $\mathrm{Inv}_h(\mathbf{X}_d)$. Note that in what follows we will define an open set of $\mathbf{X}_d^0$, and be interested in the invariants of degree h that are regular on that open set. The definition of invariance is the same, all that changes is the set on which the function is required to be regular.

From now on we require $d \geq 6$ to be even, and put $g = \frac{d-2}{2}$, then the *universal hyperelliptic curve* over the the affine space $\mathbf{X}_d = \mathrm{Sym}^d(E)$ is the variety

$$\mathbf{Y}_d = \left\{ (F, (x, y, z)) \in \mathbf{X}_d \times \mathbb{P}\left(1, \frac{d}{2}, 1\right) : y^2 = F(x, z) \right\},$$

where $\mathbb{P}(1, g+1, 1)$ is the weighted projective plane with x and z having weight 1 and y having weight $g+1$. The non-singular locus of $\mathbf{X}_d$ is the open set

$$\mathbf{X}_d^0 = \{F \in \mathbf{X}_d : \mathrm{Disc}(F) \neq 0\}.$$

We denote by $\mathbf{Y}_d^0$ the restriction of $\mathbf{Y}_d$ to the nonsingular locus. The projection gives a smooth surjective k-morphism

$$\pi \colon \mathbf{Y}_d^0 \to \mathbf{X}_d^0$$

and its fiber over F is the nonsingular hyperelliptic curve $C_F : y^2 = F(x, z)$ of genus g. In this case we have en explicit k-basis for the space of holomorphic differentials of C_F, denoted $\Omega^1(C_F)$, given by

$$\eta_1 = \frac{dx}{y}, \eta_2 = \frac{xdx}{y}, \ldots, \eta_g = \frac{x^{g-1}dx}{y}.$$

Now let $u \in G$ act on $\mathbf{Y}_d$ by

$$u \cdot (F, (x, y, z)) = (u \cdot F, u \cdot (x, y, z)),$$

where the action on F is given by

$$(u \cdot F)(x, z) = F(u^{-1}(x, z))$$

and the action of u on (x, y, z) is given by replacing the vector (x, z) by $u(x, z)$ and leaving y invariant. Then the projection

$$\pi \colon \mathbf{Y}_d^0 \to \mathbf{X}_d^0$$

is G-equivariant.

Then as in [LRZ10], the section

$$\eta = \eta_1 \wedge \ldots \wedge \eta_g$$

is a basis of the one-dimensional space $\Gamma(\mathbf{X}_d^0, \boldsymbol{\alpha})$, where

$$\boldsymbol{\alpha} = \bigwedge^g \pi_* \Omega^1_{\mathbf{Y}_d^0/\mathbf{X}_d^0},$$

the Hodge bundle of the universal curve over $\mathbf{X}_d^0$. For every $F \in \mathbf{X}_d^0$, an element $u \in G$ induces an isomorphism

$$\phi_u \colon C_F \to C_{u \cdot F},$$

and this defines a linear automorphism ϕ_u^* of $\boldsymbol{\alpha}$.

For any $h \in \mathbb{Z}$, we define $\Gamma(\mathbf{X}_d^0, \boldsymbol{\alpha}^{\otimes h})^G$ the subspace of sections $s \in \Gamma(\mathbf{X}_d^0, \boldsymbol{\alpha}^{\otimes h})$ such that

$$\phi_u^*(s) = s$$

for every $u \in G$. Then if $\alpha \in \Gamma(\mathbf{X}_d^0, \boldsymbol{\alpha})$ and $F \in \mathbf{X}_d^0$, we define

$$s(F, \alpha) = \frac{s(F)}{\alpha^{\otimes h}}.$$

This gives us the space that will be related to invariants of hyperelliptic curves, which we now define.

In this setting we have the exact analogue of Proposition 3.2.1 of [LRZ10]:

Proposition 3.4. *The section $\eta \in \Gamma(X_d^0, \boldsymbol{\alpha})$ satisfies the following properties:*

(1) If $u \in G$, then

$$\phi_u^* \eta = \det(u)^{w_0} \eta,$$

with

$$w_0 = \frac{dg}{4}.$$

(2) Let $h \geq 0$ be an integer. The linear map

$$\tau \colon \operatorname{Inv}_{\frac{gh}{2}}(\mathbf{X}_d^0) \to \Gamma(\mathbf{X}_d^0, \boldsymbol{\alpha}^{\otimes h})^G$$
$$\Phi \mapsto \Phi \cdot \eta^{\otimes h}$$

is an isomorphism.

Proof. The proof of the first part goes exactly as in the original: For $u \in G$, we have that

$$(\phi_u^* \eta)(F, \eta) = c(u, F) \eta(F, \eta),$$

and we can conclude, via the argument given in [LRZ10], that $c(u, F)$ is independent of F and a character χ of G, and that in fact

$$c(u, F) = \chi(u) = \det u^{w_0}$$

for some integer w_0. To compute w_0 we again follow the original and set $u = \lambda I_2$ with $\lambda \in k^\times$ to obtain

$$\frac{\eta_i(\lambda^{-d} F)}{\eta_i(F)} = \frac{x^{i-1} dx}{\sqrt{\lambda^{-d} F(x, y)}} \div \frac{x^{i-1} dx}{\sqrt{F(x, y)}} = \lambda^{d/2},$$

since $y = \sqrt{F(x, y)}$, for each $i = 1, \ldots, g$. Hence

$$(\phi_u^* \eta)(F, \eta) = \lambda^{dg/2} = \det(u)^{w_0}$$

and since $\det(u) = \lambda^2$ we have

$$w_0 = \frac{dg}{4} = \frac{d(d-2)}{8}.$$

The proof of the second part also goes exactly as in the original, with the replacement of a denominator of 4 instead of 3 in the quantity that is denoted w in [LRZ10]. □

3.5. **Final step.** With this in hand, we immediately obtain the analogue of Proposition 3.3.1 of [LRZ10]. We begin by setting up the notation we will need. We continue to have $d \geq 6$ an even integer and $g = \frac{d-2}{2}$. Because the fibers of $\pi\colon \mathbf{Y}_d^0 \to \mathbf{X}_d^0$ are smooth hyperelliptic curves of genus g, by the universal property of $\mathbf{M}_g$, we get a morphism

$$p\colon \mathbf{X}_g^0 \to \mathbf{M}_g^{hyp},$$

where this time $\mathbf{M}_g^{hyp}$ is the hyperelliptic locus of the moduli stack $\mathbf{M}_g$ of curves of genus g. By construction we have $p^*\boldsymbol{\lambda} = \boldsymbol{\alpha}$, and therefore we obtain a morphism

$$p^*\colon \Gamma(\mathbf{M}_g^{hyp}, \boldsymbol{\lambda}^{\otimes h}) \to \Gamma(\mathbf{X}_d^0, \boldsymbol{\alpha}^{\otimes h}).$$

As in [LRZ10], by the universal property of $\mathbf{M}_g^{hyp}$, we have

$$\phi_u^* \circ p^*(s) = p^*(s)$$

for $s \in \Gamma(\mathbf{M}_g^{hyp}, \boldsymbol{\lambda}^{\otimes h})$. From this we conclude that $p^*(s) \in \Gamma(X_d^0, \boldsymbol{\alpha})^G$, and combining this with the second part of Proposition 3.4, which establishes the isomorphism of $\Gamma(X_d^0, \boldsymbol{\alpha})^G$ and $\mathrm{Inv}_{gh}(X_d^0)$, we obtain:

Proposition 3.5. *For any even $h \geq 0$, the linear map given by $\sigma = \tau^{-1} \circ p^*$ is a homomorphism*

$$\sigma\colon \Gamma(\mathbf{M}_g^{hyp}, \boldsymbol{\lambda}^{\otimes h}) \to \mathrm{Inv}_{\frac{gh}{2}}(X_d^0)$$

satisfying

$$\sigma(f)(F) = f(C_F, (p^*)^{-1}\eta)$$

for any $F \in \mathbf{X}_d^0$ and any section $f \in \Gamma(\mathbf{M}_g^{hyp}, \boldsymbol{\lambda}^{\otimes h})$.

This is the last ingredient necessary to show the analogue of Corollary 3.3.2 of [LRZ10].

Corollary 3.6. *Let $f \in \mathbf{S}_{g,h}(\mathbb{C})$ be a geometric Siegel modular form, $\tilde{f} \in \mathbf{R}_{g,h}(\mathbb{C})$ be the corresponding analytic modular form, and $\Phi = \sigma(\theta^* f)$ the corresponding invariant. Let further $F \in \mathbf{X}_d^0$ give rise to the curve C_F equipped with a basis of regular differentials given by $\eta_1, \ldots, \eta_g$. Then if $\Omega = (\,\Omega_1\ \Omega_2\,)$ is a Riemann matrix for the curve C_F obtained by integrating the forms η_i against a symplectic basis for the homology group $H_1(C_F, \mathbb{Z})$ and $Z = \Omega_2^{-1}\Omega_1 \in \mathbb{H}_g$, we have*

$$\Phi(F) = (2i\pi)^{\frac{gh}{2}} \frac{\tilde{f}(Z)}{\det \Omega_2^h}.$$

The last two results display a connection between Siegel modular forms of even weight restricted to the hyperelliptic locus and invariants of binary forms of degree $2g+2$. In his beautiful paper, Igusa [Igu67] proved that there is a homomorphism from a subring (containing forms of even weight) of the graded ring of Siegel modular forms of genus g and level 1 to the graded ring of invariants of binary forms of degree $2g+2$. Interestingly, both constructions send a form of weight h to an invariant of degree $\frac{gh}{2}$. We leave it as an open question to prove that the two constructions are equivalent.

3.6. **The modular discriminant.** We now turn our attention to the work of Lockhart, [Loc94, Definition 3.1], in which the author gives a relationship between the discriminant Δ of a hyperelliptic curve of genus g given by $y^2 = F(x, 1)$, which is related to the discriminant of the binary form $F(x, z)$ by the relation

$$\Delta = 2^{4g} \operatorname{disc}(F), \tag{3.1}$$

and a Siegel modular form similar to Σ_{140}. From a computational perspective, the issue with the Siegel modular form proposed by Lockhart is that its value, as written, will be nonzero only for Z a period matrix in a certain $\Gamma(2)$-equivalence class. Indeed, on page 740, the author chooses a certain canonical symplectic basis for $H_1(C, \mathbb{Z})$ which is given by Mumford [Mum07b, Chapter III, Section 5]. If one acts on the symplectic basis by a matrix in $\Gamma(2)$, the value of the form given by Lockhart will change by a nonzero constant (the appearance of the principal congruence subgroup of level 2 is related to the use of half-integral theta characteristics to define the form), but if one acts on the symplectic basis by a general element of $\mathrm{Sp}_6(\mathbb{Z})$, the value of the form might become zero.

As explained in [BILV16a], in general to allow for the period matrix to belong to a different $\Gamma(2)$-equivalence class, one must attach to the period an element of a set defined by Poor [Poo94], which we call an η-map. Therefore in general one must either modify Lockhart's definition to vary with a map η admitted by the period matrix or use the form Σ_{140}, which is valid for any period matrix. We give here the connection between these two options. We begin by describing the maps η that can be attached to a hyperelliptic period matrix. We refer the reader to [Poo94] or [BILV16a] for full details.

Throughout, let C be a smooth hyperelliptic curve of genus g defined over $\mathbb{C}$ equipped with a period matrix Z for its Jacobian, and for which the branch points of the degree 2 morphism $\pi\colon C \to \mathbb{P}^1$ have been labeled with the symbols $\{1, 2, \ldots, 2g + 1, \infty\}$. We note that this choice of period matrix yields an Abel–Jacobi map,

$$AJ\colon \operatorname{Jac}(C) \to \mathbb{C}^g/(\mathbb{Z}^g + Z\mathbb{Z}^g).$$

We begin by defining a certain combinatorial group we will need.

Definition 3.7. *Let $B = \{1, 2, \ldots, 2g + 1, \infty\}$. For any two subsets $S_1, S_2 \subseteq B$, we define*

$$S_1 \circ S_2 = (S_1 \cup S_2) - (S_1 \cap S_2),$$

the symmetric difference of the two sets. For $S \subseteq B$ we also define $S^c = B - S$, the complement of S in B. Then we have that the set

$$\{S \subseteq B : \#S \equiv 0 \pmod 2\}/\{S \sim S^c\}$$

is a commutative group under the operation $\circ$, of order 2^{2g}, with identity $\emptyset \sim B$.

Given the labeling of the branch points of C, there is a group isomorphism (see [Mum07b, Corollary 2.11] for details) between the 2-torsion of the Jacobian of C and the group G_B in the following manner: To each set $S \subseteq B$ such that $\#S \equiv 0 \pmod 2$, associate the divisor class of the divisor

$$e_S = \sum_{i \in S} P_i - (\#S)P_\infty. \tag{3.2}$$

Then we can assign a map which we denote η by sending $S \subseteq B$ to the unique vector η_S in $(1/2)\mathbb{Z}^{2g}/\mathbb{Z}^{2g}$ such that $AJ(e_S) = (\eta_S)_2 + Z(\eta_S)_1$. Since there are

$(2g+2)!$ different ways to label the $2g+2$ branch points of a hyperelliptic curve X of genus g, there are several ways to assign a map η to a matrix $Z \in \mathcal{H}_g$. It suffices for our purposes to have one such map η.

Given a map η attached to Z, one may further define a set $U_\eta \subseteq B$:

$$U_\eta = \{i \in B - \{\infty\} : e_*(\eta(\{i\})) = -1\} \cup \{\infty\},$$

where for $\xi = \left(\begin{smallmatrix} \xi_1 & \xi_2 \end{smallmatrix}\right) \in (1/2)\mathbb{Z}^{2g}$, we write

$$e_*(\xi) = \exp(4\pi i \xi_1^T \xi_2).$$

Then following Lockhart [Loc94, Definition 3.1], we define

Definition 3.8. *Let $Z \in \mathcal{H}_g$ be a hyperelliptic period matrix. Then we write*

$$\phi_\eta(Z) = \prod_{T \in \mathcal{I}} \vartheta[\eta_{T \circ U_\eta}](0, Z)^4 \tag{3.3}$$

where $\mathcal{I}$ is the collection of subsets of $\{1, 2, \ldots, 2g+1, \infty\}$ that have cardinality $g+1$.

Remark 3.9. We note that in this work we write our hyperelliptic curves with a model of the form $y^2 = F(x, 1)$, where F is of degree $2g+2$. In other words we do not require one of the Weierstrass points of the curve to be at infinity. It is for this reason that we modify Lockhart's definition above, so that the analogue of his Proposition 3.2 holds for F of degree $2g+2$ rather than $2g+1$.

The form that we define here is equal to the one given in his Definition 3.1 for the following reason: Because $T^c \circ U_\eta = (T \circ U_\eta)^c$, it follows that $\eta_{T \circ U_\eta} \equiv \eta_{T^c \circ U_\eta} \pmod{\mathbb{Z}}$. Therefore $\vartheta[\eta_{T \circ U_\eta}](0, Z)$ differs from $\vartheta[\eta_{T^c \circ U_\eta}](0, Z)$ by at worse their sign. Since we are raising the theta function to the fourth power, the sign disappears, and the product above is equal to the product given by Lockhart, in which T ranges only over the subset of $\{1, 2, \ldots, 2g+1\}$ of cardinality $g+1$, but each theta function is raised to the eighth power.

We now restrict our attention to the case of genus $g = 3$ which is of interest to us in this work. We note that since Z is a hyperelliptic period matrix, by [Igu67] a single one of its even theta constants vanishes, and therefore, we have

$$\phi_\eta(Z) = \Sigma_{140}(Z).$$

Otherwise, in general ϕ_η has weight $2\binom{2g+2}{g+1} = 4\binom{2g+1}{g+1}$.

We then have the following Theorem, which is a generalization to our setting of Proposition 3.2 of [Loc94]:

Theorem 3.10. *Let C be a hyperelliptic curve of genus g defined over $\mathbb{C}$ with Weierstrass equation $y^2 = F(x, 1)$ and period matrix $Z = \Omega_2^{-1}\Omega_1$. Let $r = \binom{2g+1}{g+1}$ and $n = \binom{2g}{g+1}$. Then*

$$2^{4g} \operatorname{Disc}(F)^n = 2^{4gn} \pi^{4gr} \det(\Omega_2)^{-4r} \phi_\eta(Z). \tag{3.4}$$

Proof. We show how to modify Lockhart's proof. We first note that $\Delta = 2^{4g} \operatorname{Disc}(F)$ by [Loc94, Definition 1.6] Then as Lockhart does, we may use Thomae's formula, which by [BILV16a, Theorem 2] is true for any period matrix:

$$\vartheta[\eta_{T \circ U_\eta}](0, Z)^4 = (\det(\Omega_2))^2 \pi^{-2g} \prod_{\substack{i<j \\ i,j \in T}} (a_i - a_j) \prod_{\substack{i<j \\ i,j \notin T}} (a_i - a_j)$$

if T is a subset of $\{1, 2, \ldots, 2g+1, \infty\}$ that have cardinality $g+1$. Taking the product over all such T, we get

$$\phi_\eta(Z) = (\det \Omega_2)^{4r} \pi^{-4gr} \prod_T \left(\prod_{\substack{i<j \\ i,j \in T}} (a_i - a_j) \prod_{\substack{i<j \\ i,j \notin T}} (a_i - a_j) \right),$$

with $r = \binom{2g+1}{g+1} = \frac{1}{2}\binom{2g+2}{g+1}$. We now count how many times each factor of $(a_i - a_j)$ appears on the left-hand side:

$$\begin{aligned} \#\{T : i,j \in T \text{ or } i,j \notin T\} &= \#\{T : i,j \in T\} + \#\{T : i,j \notin T\} \\ &= \binom{2g}{g-1} + \binom{2g}{g+1} = 2\binom{2g}{g+1} = 2n. \end{aligned}$$

From here the proof follows as in [Loc94]. □

We note that, up to the factors of 2 appearing in the formula, this Theorem realizes Corollary 3.6, as it connects explicitly an invariant of a hyperelliptic curve to a Siegel modular form.

3.7. **Proof of Theorem 1.1.** We are now in a position to prove Theorem 1.1. For simplicity, we replace $f^{\frac{140}{\gcd(k,140)}}$ with $\tilde{f}$, a Siegel modular form of weight $\tilde{k} = \frac{140k}{\gcd(k,140)}$, and let $\ell = \frac{k}{\gcd(k,140)}$. Note that $\tilde{k} = 140\ell$ and is divisible by 4.

Using the notation of Section 3.1, the analytic Siegel modular form $\tilde{f}$ corresponds to a geometric Siegel modular form f by Proposition 3.1. Let $\Phi = \sigma(\theta^* f)$ be the corresponding invariant of the hyperelliptic curve. Then by Corollary 3.6, if the hyperelliptic curve $y^2 = F(x,1)$ has period matrix Z, we have

$$\Phi(F) = (2\pi i)^{3\tilde{k}} \det(\Omega_2)^{-\tilde{k}} f(Z).$$

Therefore we have

$$\begin{aligned} j(Z) = \frac{f}{\Sigma_{140}^\ell}(Z) &= \frac{(2\pi i)^{-3\tilde{k}} \det(\Omega_2)^{\tilde{k}} \Phi(F)}{2^{-168\ell} \pi^{-420\ell} \det(\Omega_2)^{140\ell} \operatorname{Disc}(F)^{15\ell}} \\ &= 2^{-\frac{252k}{\gcd(k,140)}} \frac{\Phi(F)}{\operatorname{Disc}(F)^{15\ell}}. \end{aligned}$$

We note that since Φ is assumed to be an integral invariant, it does not have a denominator when evaluated at $F \in \mathbb{Z}[x,z]$. We have thus obtained an invariant as in [KLLG+16, Theorem 7.1] (we note that this article assumes throughout that invariants of hyperelliptic curves are integral, see the discussion between Proposition 1.4 and Theorem 1.5), having negative valuation at the prime $\mathfrak{p}$. We conclude that C has bad reduction at this prime.

4. Computing class invariants

In this last Section, we recall the list of hyperelliptic curves of genus 3 that have simple Jacobian with CM by the ring of integers of a CM sextic field. We then define some modular functions having Σ_{140} in the denominator, evaluate them at a period matrix of these Jacobians with CM, and show that the denominators of these algebraic numbers are indeed divisible by the primes of geometrically bad reduction of the curve.

4.1. **Hyperelliptic curves of genus 3 with CM by a ring of integers.** There exist exactly 37 isomorphism classes of sextic CM fields for which there is exactly *one* geometrically simple CM point over $\mathbb{Q}$ in the moduli space of principally polarized abelian threefolds (see Theorems 4.3.1 and 4.1.1 in [Kıl16], which will be published as [KS16b]). The list of these 37 sextic CM fields is given in Table 3.1 of [Kıl16] and will be published in [Kıl17]. It is later proven in Theorem 1.1 of [KLL$^+$17] that the principally polarized abelian threefolds corresponding to these rational CM points are the Jacobians of genus 3 curves defined over $\mathbb{Q}$.

We pull from this list of curves those that are hyperelliptic; the curves numbered (1)–(8) below are the complete list of hyperelliptic CM curves of genus 3 that are defined over $\mathbb{Q}$. As we mentioned in the introduction, they are taken from a list that can be found in [KS16b]. We note more specifically that the curves (5), (6) and (8) were found by Balakrishnan, Ionica, Kilicer, Lauter, Somoza, Streng, and Vincent, and (1), (2), (3), and (7) were computed by Weng [Wen01]. Moreover, the hyperelliptic model of the curve with complex multiplication by the ring of integers in CM field (3) was proved to be correct by Tautz, Top, and Verberkmoes [TTV91, Proposition 4], and the hyperelliptic model of the curve with complex multiplication by the ring of integers in CM field (4) was given by Shimura and Taniyama [Shi98] (see Example (II) on page 76).

We note that as shown in [Kıl16], each of the CM fields K below will be Galois, with cyclic Galois group. Furthermore, as shown by Weng [Wen01, Lemma 4.5], if $i \in K$, then under our hypotheses (that the Jacobian is simple and has CM by $\mathcal{O}_K$) the curve is guaranteed to be hyperelliptic. Furthermore, in what follows every time we say that a prime is of bad reduction, we will mean that it is a prime of geometrically bad reduction of the curve.

For each curve below, the discriminant and the odd primes of bad reduction are computed using Proposition 4.5 and Corollary 4.6 in [BW17].

(1) ([Wen01, §6 - 3rd ex.]) Let $K = \mathbb{Q}[x]/(x^6 + 13x^4 + 50x^2 + 49)$, which is of class number 1 and contains $\mathbb{Q}(i)$. A model for the hyperelliptic curve with CM by $\mathcal{O}_K$ is
$$y^2 = x^7 + 1786x^5 + 44441x^3 + 278179x$$
with $\Delta = -2^{18} \cdot 7^{24} \cdot 11^{12} \cdot 19^7$. There are only two odd primes of bad reduction for the curve C, namely 7 and 11.

(2) ([Wen01, §6 - 2nd ex.]) Let $K = \mathbb{Q}[x]/(x^6 + 6x^4 + 9x^2 + 1)$, which is of class number 1 and contains $\mathbb{Q}(i)$. A model for the hyperelliptic curve with CM by $\mathcal{O}_K$ is
$$y^2 = x^7 + 6x^5 + 9x^3 + x$$
with $\Delta = -2^{18} \cdot 3^8$. The prime 3 is the only odd prime of bad reduction for the curve.

(3) ([Wen01, §6 - 1st ex.]) Let $K = \mathbb{Q}[x]/(x^6 + 5x^4 + 6x^2 + 1) = \mathbb{Q}(\zeta_7 + \zeta_7^{-1}, i)$, which is of class number 1. A model for the hyperelliptic curve with CM by $\mathcal{O}_K$ is
$$y^2 = x^7 + 7x^5 + 14x^3 + 7x$$
with $\Delta = -2^{18} \cdot 7^7$. The curve C has good reduction at each odd $p \neq 7$ and potentially good reduction at $p = 7$.

(4) Let $K = \mathbb{Q}[x]/(x^6 + 7x^4 + 14x^2 + 7) = \mathbb{Q}(\zeta_7)$, which is of class number 1 and contains $\mathbb{Q}(\sqrt{-7})$. A model for the hyperelliptic curve with CM by $\mathcal{O}_K$ is
$$y^2 = x^7 - 1$$
with $\Delta = -2^{12} \cdot 7^7$. The curve C has good reduction at each odd $p \neq 7$ and potentially good reduction at $p = 7$.

(5) Let $K = \mathbb{Q}[x]/(x^6 + 42x^4 + 441x^2 + 847)$, which is of class number 12 and contains $\mathbb{Q}(\sqrt{-7})$. A model for the hyperelliptic curve with CM by $\mathcal{O}_K$ is
$$y^2 + x^4 y = -7x^6 + 63x^4 - 140x^2 + 393x - 28$$
with $\Delta = -1 \cdot 3^8 \cdot 5^{24} \cdot 7^7$. The odd primes of bad reduction of C are 3 and 5.

(6) Let $K = \mathbb{Q}[x]/(x^6 + 29x^4 + 180x^2 + 64)$, which is of class number 4 and contains $\mathbb{Q}(i)$. A model for the hyperelliptic curve with CM by $\mathcal{O}_K$ is
$$y^2 = 1024x^7 - 12857x^5 + 731x^3 + 688x$$
with $\Delta = -2^{60} \cdot 11^{24} \cdot 43^7$. The only odd prime of bad reduction of C is 11.

(7) ([Wen01, §6 - 4th ex.]) Let $K = \mathbb{Q}[x]/(x^6 + 21x^4 + 116x^2 + 64)$, which is of class number 4 and contains $\mathbb{Q}(i)$. A model for the hyperelliptic curve with CM by $\mathcal{O}_K$ is
$$y^2 = 64x^7 - 124x^5 + 31x^3 + 31x$$
with $\Delta = -2^{44} \cdot 31^7$. The curve has potentially good reduction at 31.

(8) Let $K = \mathbb{Q}[x]/(x^6 + 42x^4 + 441x^2 + 784)$, which is of class number 4 and contains $\mathbb{Q}(i)$. A model for the hyperelliptic curve with CM by $\mathcal{O}_K$ is
$$y^2 = 16x^7 + 357x^5 - 819x^3 + 448x$$
with $\Delta = -2^{48} \cdot 3^8 \cdot 7^7$. The only odd prime of bad reduction of C is 3.

4.2. **Computation of the modular invariants.** For a given sextic CM field K, we used the available Sage code [BILV16b] to compute a period matrix for the abelian variety under consideration. This code implements the theory alluded to in Section 2.1. Once we obtained a period matrix Z, we then applied the reduction algorithm given in [KLL+17] and implemented by Kılıçer and Streng [KS16a] to obtain another period matrix that is $\mathrm{Sp}_{2g}(\mathbb{Z})$-equivalent to the first matrix obtained, but that provides faster convergence of the theta constants. Finally, using Labrande's Magma implementation for fast theta function evaluation [Lab17], we computed the 36 even theta constants for these reduced period matrices, up to 15,000 bits of precision. These theta constants were used for the computations of the modular invariants that we define below. In most cases, 10,000 bits were enough to recognize these values as algebraic numbers.[2]

[2] In fact, for CM field (6), the theta constants obtained using the Magma implementation [Lab17] for high precision (i.e. ≥ 5000 bits) were not conclusive. We therefore ran an improved implementation of the naive method to get these values up to 10,000 bits of precision, and recognized the invariants as algebraic numbers after multiplying by the expected denominators.

As illustrations of Theorem 1.1, we implemented and computed with high precision certain class invariants involving the form Σ_{140}, which is defined in (1.1), in the denominator. To defined these modular functions, we will need the following Siegel modular forms in their denominators: We first use h_4, the Eisenstein series of weight 4 that is given by

$$h_4(Z) = \frac{1}{2^3}\sum_{\xi}\theta[\xi]^8(Z), \tag{4.1}$$

where ξ ranges over all even theta characteristics. Next we present α_{12}, which is a weight 12 modular form defined by Tsuyumine [Tsu86]:

$$\alpha_{12}(Z) = \frac{1}{2^3\cdot 3^2}\sum_{(\xi_i)}(\theta[\xi_1](Z)\theta[\xi_2](Z)\theta[\xi_3](Z)\theta[\xi_4](Z)\theta[\xi_5](Z)\theta[\xi_6](Z))^4, \tag{4.2}$$

where $(\xi_1,\xi_2,\xi_3,\xi_4,\xi_5,\xi_6)$ is a maximal azygetic system of even theta characteristics. By this we mean that (ξ_i) is a sextuple of even theta characteristics such that the sum of any three among these six is odd. Notice that α_{12} is one of the 35 generators given by Tsuyumine [Tsu87] of the graded ring $A(\Gamma_3)$ of modular forms of degree 3 and cannot be written as a polynomial in Eisenstein series.

In the computations below, we consider thus the following three modular functions:

$$j_1(Z) = \frac{h_4^{35}}{\Sigma_{140}}(Z), \qquad j_2(Z) = \frac{\alpha_{12}^{35}}{\Sigma_{140}^3}(Z), \qquad j_3(Z) = \frac{h_4^5\alpha_{12}^{10}}{\Sigma_{140}}(Z). \tag{4.3}$$

The numerical data in Table 4.1 shows the tight connection between the odd primes appearing in the denominators of the Shioda invariants for a curve, the odd primes of bad reduction for the hyperelliptic curve, and the odd primes dividing the denominators of j_1, j_2 and j_3. In the denominators of j_1, j_2 and j_3, we intentionally omitted the denominators of the formulae (4.1) and (4.2), i.e. 2^3 and $2^3\cdot 3^2$. Note that we do not have a proof for the fact that h_4 and α_{12} fulfill the condition in Theorem 1.1, i.e. that their corresponding curve invariants are integral. Our results are evidence that either this condition is a reasonable one, or that the result in Theorem 1.1 may be extended to a larger class of modular forms.

Finally, the last column in Table 4.1 shows the odd primes appearing in the denominators of the Shioda invariants. Note that the Shioda invariants $J_2, J_3, \ldots, J_{10}$ are not integral and their denominators factor as products of powers of 2,3,5 and 7 (see [LR12] for a set of formulae). This is the reason why, in the last column of Table 4.1, these primes may appear in the denominators of the Shioda invariants, even when they are not primes of bad reduction. However, one can see that the primes > 7 appearing in the denominators of the Shioda invariants $\mathrm{Shioda}_{\mathrm{abs}}(C)$ are exactly the primes of bad reduction, which confirms Theorem 7.1 in [KLLG$^+$16]. All the entries marked by $-$ in the Table represent values equal to zero.

We note that because of its large weight, Σ_{140} is expensive to compute, so the modular invariants computed here may not be the most convenient to use from a computational point of view. As suggested by Lockhart [Loc94, p. 741], it might be worth finding a Siegel modular form that corresponds to a lower power of the discriminant, especially if one is to pursue further the goal of finding modular invariants having the property that the primes of geometrically bad reduction of the curve appear in the denominator.

TABLE 4.1. Denominators of invariants

CM field	curve discriminant	odd primes of bad reduction	denominators of j_1, j_2, j_3	odd primes in the denominators of $\mathrm{Shioda}_{\mathrm{abs}}(C)$
(1)	$-2^{18} \cdot 7^{24} \cdot 11^{12} \cdot 19^7$	$7, 11$	$-7^{80} \cdot 11^{40}$ $7^{240} \cdot 11^{120}$ $7^{80} \cdot 11^{40}$	$7^{31}11^{12}, -, 7^{76}11^{24}$ $-, 7^{114}11^{36}, -$ $5^7 7^{159}11^{41}, -, 5^7 7^{197}11^{60}$
(2)	$-2^{12} \cdot 3^8$	3	1 $2^3 \cdot 3^{12}$ 1	$3^8 7^7, -, 3^{23}7^{28}$ $-, 3^{38}7^{42}, -$ $3^{32}5^7 7^{63}, -, 3^{47}5^7 7^{77}$
(3)	$-2^{18} \cdot 7^7$	none	1 2^3 1	$1, -, 7^{14}$ $-, 7^{21}, -$ $5^7 7^{35}, -, 5^7 7^{42}$
(4)	$-2^{12} \cdot 7^7$	none	1 2^3 1	$-, -, -$ $-, -, 7^7$ $-, -, -$
(5)	$-3^8 \cdot 5^{24} \cdot 7^7$	3,5	$-$ $2^3 \cdot 3^{12} \cdot 5^{240}$ $-$	$3^8 \cdot 5^{31}, 5^{100}, 3^{23} \cdot 5^{41}$ $3^{12} \cdot 5^{120}, 3^{38} \cdot 5^{72}, 3^6 \cdot 5^{26}$ $3^{32} \cdot 5^{103}, 3^{72} \cdot 5^{216}, 3^{47} \cdot 5^{120}$
(6)	$-2^{60} \cdot 11^{24} \cdot 43^7$	11	$2^{125} \cdot 11^{80}$ $2^{413} \cdot 11^{240}$ $2^{135} \cdot 11^{80}$	$7^7 11^{24}, -, 7^{28}11^{48}$ $-, 7^{42}11^{72}, -$ $5^7 7^{77}11^{96}, -, 5^7 7^{77}11^{120}$
(7)	$-2^{44} \cdot 31^7$	none	2^{25} 2^{113} 2^{35}	$7^7, -, 7^{28}$ $-, 7^{42}, -$ $5^7 7^{63}, -, 5^7 7^{77}$
(8)	$-2^{48} \cdot 3^8 \cdot 7^7$	3	2^{85} $2^{293} \cdot 3^{12}$ 2^{95}	$3^8, -, 3^{23}7^{14}$ $-, 3^{38}7^{21}, -$ $3^{32}5^7 7^{35}, -, 3^{47}5^7 7^{42}$

Finally, we note that in the non-hyperelliptic curve case, one could show with similar reasoning as in Theorem 1.1 that a modular function having a power of χ_{18} in the denominator, when evaluated at a plane quartic period matrix, has denominator divisible by the primes of bad reduction or of hyperelliptic reduction of the curve associated to the period matrix. In this direction, a relationship between χ_{18} and the discriminant of the non-hyperelliptic curve was shown by Lachaud, Ritzenthaler, and Zykin [LRZ10, Theorem 4.1.2, Klein's formula].

5. Conclusion

We have displayed a connection between geometric modular forms of even weight restricted to the hyperelliptic locus and invariants of binary forms of degree $2g+2$. In his beautiful paper, Igusa [Igu67] proved that there is a homomorphism from a subring (containing forms of even weight) of the graded ring of Siegel modular forms of genus g and level 1 to the graded ring of binary forms of degree $2g+2$. Interestingly, both constructions increase the weight by a $\frac{1}{2}g$ ratio. We leave it as an open question to prove that the two constructions are equivalent.

References

[Bas15] Romain Basson. *Arithmétique des espaces de modules des courbes hyperelliptiques de genre* 3 *en caractéristique positive*. PhD thesis, Université de Rennes 1, Rennes, 2015. 2.3

[BILV16a] Jennifer S. Balakrishnan, Sorina Ionica, Kristin Lauter, and Christelle Vincent. Constructing genus-3 hyperelliptic Jacobians with CM. *LMS J. Comput. Math.*, 19(suppl. A):283–300, 2016. 2.1, 3.6, 3.6

[BILV16b] Jennifer S. Balakrishnan, Sorina Ionica, Kristin Lauter, and Christelle Vincent. Genus 3. `https://github.com/christellevincent/genus3`, 2016. 4.2

[BW17] Irene I. Bouw and Stefan Wewers. Computing L-functions and semistable reduction of superelliptic curves. *Glasg. Math. J.*, 59(1):77–108, 2017. 4.1

[Dix87] Jacques Dixmier. On the projective invariants of quartic plane curves. *Adv. in Math.*, 64:279–304, 1987. 1

[GL07] Eyal Z. Goren and Kristin E. Lauter. Class invariants for quartic CM fields. *Ann. Inst. Fourier (Grenoble)*, 57(2):457–480, 2007. 1, 3

[Ich94] Takashi Ichikawa. On Teichmüller modular forms. *Mathematische Annalen*, 299(1):731–740, 1994. 3.3

[Ich95] Takashi Ichikawa. Teichmüller modular forms of degree 3. *American Journal of Mathematics*, pages 1057–1061, 1995. 3.3

[Ich96] Takashi Ichikawa. Theta constants and Teichmüller modular forms. *journal of number theory*, 61(2):409–419, 1996. 3.3

[Ich00] Takashi Ichikawa. Generalized Tate curve and integral Teichmüller modular forms. *American Journal of Mathematics*, 122(6):1139–1174, 2000. 3.3

[Igu62] Jun-ichi Igusa. On Siegel modular forms of genus two. *American Journal of Mathematics*, 84(1):175–200, 1962. 1

[Igu67] Jun-ichi Igusa. Modular forms and projective invariants. *Amer. J. Math.*, 89:817–855, 1967. 1, 2.2, 3.5, 3.6, 5

[Kıl16] Pınar Kılıçer. *The CM class number one problem for curves*. PhD thesis, Leiden University and University of Bordeaux, 2016. 4.1

[Kıl17] Pınar Kılıçer. The CM class number one problem for curves of genus 3. In preparation, 2017. 4.1

[KLL+17] Pınar Kılıçer, Hugo Labrande, Reynald Lercier, Christophe Ritzenthaler, Jeroen Sijsling, and Marco Streng. Plane quartics over $\mathbb{Q}$ with complex multiplication. *Preprint*, 2017. 4.1, 4.2

[KLLG+16] Pınar Kılıçer, Kristin E. Lauter, Elisa Lorenzo García, Rachel Newton, Ekin Ozman, and Marco Streng. A bound on the primes of bad reduction for CM curves of genus 3. https://arxiv.org/abs/1609.05826, 2016. 3, 3.7, 4.2

[KS16a] Pınar Kılıçer and Marco Streng. Period matrices for genus 3 cm curves. `https://bitbucket.org/pkilicer/period-matrices-for-genus-3-cm-curves`, 2016. 4.2

[KS16b] Pınar Kılıçer and Marco Streng. Rational CM points and class polynomials for genus three. In preparation, 2016. 1, 4.1

[Lab17] Hugo Labrande. Code for fast theta function evaluation. `https://hlabrande.fr/math/research/`, 2017. [accessed 2017-11-17]. 4.2, 2

[Loc94] Paul Lockhart. On the discriminant of a hyperelliptic curve. *Trans. Amer. Math. Soc.*, 342(2):729–752, 1994. 1, 3, 3.6, 3.6, 3.6, 3.6, 4.2

[LR12] Reynald Lercier and Christophe Ritzenthaler. Hyperelliptic curves and their invariants: geometric, arithmetic and algorithmic aspects. *Journal of Algebra*, 372:595–636, 2012. 2.3, 4.2

[LRZ10] Gilles Lachaud, Christophe Ritzenthaler, and Alexey Zykin. Jacobians among abelian threefolds: a formula of Klein and a question of Serre. *Math. Res. Lett.*, 17(2):323–333, 2010. 1, 3, 3.1, 3.1, 3.2, 3.3, 3.4, 3.4, 3.5, 3.5, 4.2

[LV15a] Kristin Lauter and Bianca Viray. An arithmetic intersection formula for denominators of Igusa class polynomials. *Amer. J. Math.*, 137(2):497–533, 2015. 1

[LV15b] Kristin Lauter and Bianca Viray. On singular moduli for arbitrary discriminants. *Amer. J. Math.*, 19:9206–9250, 2015. 1

[Mat59] Teruhisa Matsusaka. On a characterization of a Jacobian variety. *Memo. Coll. Sci. Univ. Kyoto. Ser. A. Math.*, 32:1–19, 1959. 1

[Mum07a] David Mumford. *Tata lectures on theta. I.* Modern Birkhäuser Classics. Birkhäuser Boston, Inc., Boston, MA, 2007. With the collaboration of C. Musili, M. Nori, E. Previato and M. Stillman, Reprint of the 1983 edition. 2.2, 2.2

[Mum07b] David Mumford. *Tata lectures on theta. II.* Modern Birkhäuser Classics. Birkhäuser Boston, Inc., Boston, MA, 2007. Jacobian theta functions and differential equations, With the collaboration of C. Musili, M. Nori, E. Previato, M. Stillman, and H. Umemura, Reprint of the 1984 original. 3.6, 3.6

[Ohn05] Toshiaki Ohno. The graded ring of invariants of ternary quartics I, 2005. unpublished. 1

[Poo94] Cris Poor. The hyperelliptic locus. *Duke Math. J.*, 76(3):809–884, 1994. 3.6

[Ran81] Ziv Ran. On subvarieties of abelian varieties. *Invent. Math.*, 62(3):459–479, 1981. 1

[Shi67] Tetsuji Shioda. On the graded ring of invariants of binary octavics. *Amer. J. Math.*, 89:1022–1046, 1967. 1, 2.3

[Shi98] Goro Shimura. *Abelian varieties with complex multiplication and modular functions*, volume 46 of *Princeton Mathematical Series*. Princeton University Press, Princeton, NJ, 1998. 2.1, 4.1

[Str14] Marco Streng. Computing Igusa class polynomials. *Math. Comp.*, 83(285):275–309, 2014. `arXiv:0903.4766`. 2.1

[Tsu86] Shigeaki Tsuyumine. On Siegel modular forms of degree 3. *Amer. J. Math.*, 108:755–862, 1986. 1, 4.2

[Tsu87] Shigeaki Tsuyumine. On the Siegel modular field of degree 3. *Compos. Math.*, 63(1):83–98, 1987. 1, 4.2

[TTV91] Walter Tautz, Jaap Top, and Alain Verberkmoes. Explicit hyperelliptic curves with real multiplication and permutation polynomials. *Canad. J. Math.*, 43(5):1055–1064, 1991. 4.1

[vW99] Paul van Wamelen. Examples of genus two CM curves defined over the rationals. *Math. Comp.*, 68(225):307–320, 1999. 2.1

[Wen01] Annegret Weng. A class of hyperelliptic CM-curves of genus three. *J. Ramanujan Math. Soc.*, 16(4):339–372, 2001. 4.1

Sorina Ionica, Laboratoire MIS, Université de Picardie Jules Verne, 33 Rue Saint Leu, Amiens 80039, France
E-mail address: `sorina.ionica@u-picardie.fr`

Pinar Kiliçer, Carl von Ossietzky Universität Oldenburg, Institut für Mathematik, 26111 Oldenburg, Germany
E-mail address: `pinarkilicer@gmail.com`

Kristin Lauter, Microsoft Research, One Redmond Way, Redmond, WA 98052, USA
E-mail address: `klauter@microsoft.com`

Elisa Lorenzo García, Laboratoire IRMAR, Office 602, Université de Rennes 1, Campus de Beaulieu, 35042, Rennes Cedex
E-mail address: `elisa.lorenzogarcia@univ-rennes1.fr`

Maike Massierer, School of Mathematics and Statistics, University of New South Wales, Sydney NSW 2052, Australia
E-mail address: `maike@unsw.edu.au`

Adelina Mânzăţeanu, School of Mathematics, University of Bristol, Bristol, BS8 1JR, UK
E-mail address: `am15112@bristol.ac.uk`

Christelle Vincent, Department of Mathematics and Statistics, University of Vermont, 16 Colchester Avenue, Burlington VT 05401
E-mail address: `christelle.vincent@uvm.edu`