Contemporary Mathematics

Computing Humbert Surfaces and Applications

David Gruenewald

Abstract. We describe an algorithm which computes components of Humbert surfaces in terms of Rosenhain invariants, based on Runge's method [**16**]. We demonstrate how Humbert equations can be used to improve the Eisenträger-Lauter algorithm [**6**] to compute the endomorphism ring of a genus 2 Jacobian, as well as improve aspects of the CRT method to compute Igusa class polynomials.

Introduction

In recent times, attention has been focused on improving algorithms related to hyperelliptic curves over finite fields. To construct hyperelliptic curves suitable for use in public key cryptography, it is necessary to determine the zeta function of the curve, or equivalently, the endomorphism algebra of its Jacobian. Thus determining explicit models for moduli spaces for principally polarized abelian varieties with prescribed endomorphism ring is not only of mathematical interest but an important problem with practical applications.

In this article we describe an algorithm for computing equations of Humbert surfaces — moduli spaces for principally polarized abelian surfaces (p.p.a.s) possessing real multiplication by a real quadratic order. The approach taken is to use Fourier expansions of modular forms with some level structure and apply Runge's method [**16**] to find relations among them.

We then present two applications for Humbert surface equations. The fact that every quartic CM-field contains a real quadratic field means that a CM-point can be identified as a point on a Humbert surface. This is used to great effect in both speeding up endomorphism ring computations for genus 2 Jacobians over finite fields and speeding up the CRT method for computing Igusa class polynomials.

Most of the equations of Humbert components we produce are too large to include in this article. For convenience we have made this data accessible online [**9**].

Acknowledgements. I would like to thank David Kohel for his supervision of my doctoral thesis of which this forms a part, and to the anonymous referee for providing helpful suggestions.

2010 *Mathematics Subject Classification.* Primary 11G15.
Supported by an APA scholarship at the University of Sydney.

1. Preliminaries

To begin, we describe the moduli space of principally polarized abelian surfaces (p.p.a.s) over the complex numbers. For general properties of complex abelian varieties we refer the reader to [**2**].

1.1. The Siegel modular threefold. Denote by $\mathcal{H}_2$ the Siegel upper half plane of degree 2, which by definition is the set of 2 by 2 symmetric matrices over $\mathbb{C}$ whose imaginary part is positive definite:

$$\mathcal{H}_2 = \{\tau \in \mathrm{Mat}_{2\times 2}(\mathbb{C}) \mid {}^t\tau = \tau \ , \ \mathrm{Im}\,(\tau) > 0\}\,.$$

Each $\tau \in \mathcal{H}_2$ corresponds to a principally polarized complex abelian surface A_τ with period matrix $(\tau \ I_2) \in \mathrm{Mat}_{2\times 4}(\mathbb{C})$. Two abelian surfaces A_τ and A'_τ are isomorphic if and only if there is a symplectic matrix $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{Sp}_4(\mathbb{Z})$ such that $\tau = M(\tau) := (a\tau + b)(c\tau + d)^{-1}$. Quotienting out by this action, we obtain the moduli space $\mathcal{A}_2 = \mathrm{Sp}_4(\mathbb{Z})\backslash\mathcal{H}_2$ of isomorphism classes of principally polarized abelian surfaces. It is a quasi-projective variety of dimension 3 and is called the *Siegel modular threefold*.

The sets of abelian surfaces having the same endomorphism ring form subvarieties of $\mathcal{A}_2$. Let A be a principally polarized abelian surface. Then $\mathrm{End}(A)$ is an order in $\mathrm{End}(A) \otimes \mathbb{Q}$ which is isomorphic to either a quartic CM field, an indefinite quaternion algebra, a real quadratic field or in the generic case $\mathbb{Q}$. The irreducible components of the corresponding moduli spaces in $\mathcal{A}_2$ which have "extra endomorphisms" have dimensions $0, 1, 2$ and are known as CM points, Shimura curves and Humbert surfaces respectively.

1.2. Humbert surfaces. Humbert [**13**] showed that for each positive discriminant Δ there is a unique irreducible Humbert surface H_Δ in $\mathcal{A}_2$, and any matrix $\left(\begin{smallmatrix} \tau_1 & \tau_2 \\ \tau_2 & \tau_3 \end{smallmatrix}\right) \in \mathcal{H}_2$ satisfying the equation

$$(*) \qquad k\tau_1 + \ell\tau_2 - \tau_3 = 0$$

lies on the Humbert surface H_Δ of discriminant $\Delta = 4k + \ell > 0$. For a modern account of Humbert's work the reader is referred to [**3**, §4].

The function field of $\mathcal{A}_2$ is rational, generated by three algebraically independent Siegel modular functions j_1, j_2, j_3 for $\mathrm{Sp}_4(\mathbb{Z})$ called *(absolute) Igusa invariants* [**4**, p.3]. Hence there is an irreducible polynomial $H_\Delta(j_1, j_2, j_3)$ whose zero set is the Humbert surface of discriminant Δ. Unfortunately, working with Igusa invariants directly is impractical due to the large degrees and coefficients of the polynomial. One fares better by working in a finite cover of the moduli space, adding some level structure.

Runge [**16**] constructed an algorithm to compute Humbert components in the cover $\Gamma^*(2,4)\backslash\mathcal{H}_2$ using theta functions and their Fourier expansions. Our objective is to extend this to other models; in particular to $\mathcal{A}_2(2)$, the Siegel modular threefold with level 2 structure using Rosenhain invariants.

2. Level 2 structure

Let $\mathcal{M}_2$ denote the moduli space of genus 2 curves. Torelli's theorem [**2**, Theorem 11.1.7] says that the map sending a curve C to its Jacobian variety $\mathrm{Jac}(C)$ is injective and defines a birational map $\mathcal{M}_2 \to \mathcal{A}_2$. In fact, the image of the

Torelli map is precisely the complement of the Humbert surface H_1 in $\mathcal{A}_2$ (see [**2**, Corollary 11.8.2(a)]).

Given a genus 2 curve $y^2 = \prod_{i=1}^{6}(x-u_i)$ over the complex numbers, we can send three of the u_i to $0, 1, \infty$ via a fractional linear transformation to get an isomorphic curve with a *Rosenhain model*:

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

The λ_i are called *Rosenhain invariants*.

The ordered tuple $(0, 1, \infty, \lambda_1, \lambda_2, \lambda_3)$ determines an ordering of the Weierstrass points and a level 2 structure on the corresponding Jacobian, that is, determines a point of $\mathcal{A}_2(2)$.

Let $\mathcal{M}_2(2)$ denote the moduli space of genus 2 curves together with a full level 2 structure. The points of $\mathcal{M}_2(2)$ are given by triples $(\lambda_1, \lambda_2, \lambda_3)$ where the λ_i are all distinct and different from 0 and 1. The forgetful morphism $\mathcal{M}_2(2) \to \mathcal{M}_2$ is a Galois covering of degree $720 = |S_6|$ where S_6 acts on the Weierstrass 6-tuple by permutations, followed by renormalising the first three coordinates to $(0, 1, \infty)$.

As functions on $\mathcal{M}_2(2)$, the Rosenhain invariants generate the coordinate ring of $\mathcal{M}_2(2)$ and hence generate the function field of $\mathcal{A}_2(2)$.

3. Theta constants and Rosenhain invariants

Let $\tau \in \mathcal{H}_2$ and write $m' = (a, b)$ and $m'' = (c, d)$. The *classical theta constants* (of half integral characteristic) are defined by

$$\theta_{abcd}(\tau) = \sum_{x \in \mathbb{Z}^2} \exp 2\pi i \left(\frac{1}{2}(x + \frac{m'}{2}) \cdot \tau \cdot {}^t(x + \frac{m'}{2}) + (x + \frac{m'}{2}) \cdot {}^t(\frac{m''}{2}) \right)$$

where a, b, c, d are either 0 or 1.

As a function of $\tau \in \mathcal{A}_2$ there are 720 different Rosenhain invariant triples, any of which may be used. By Thomae's formula [**15**, Ch. 8] we can express each of these in terms of theta functions. Write

$$\begin{aligned} \vartheta_1 &= \theta_{0000}(\tau) \\ \vartheta_2 &= \theta_{0011}(\tau) \\ \vartheta_3 &= \theta_{0010}(\tau) \\ \vartheta_4 &= \theta_{0001}(\tau) \\ \vartheta_8 &= \theta_{1100}(\tau) \\ \vartheta_{10} &= \theta_{1111}(\tau)\,, \end{aligned}$$

then

$$e_1 = \frac{\vartheta_1^2\vartheta_3^2}{\vartheta_2^2\vartheta_4^2},\ e_2 = \frac{\vartheta_3^2\vartheta_8^2}{\vartheta_4^2\vartheta_{10}^2},\ e_3 = \frac{\vartheta_1^2\vartheta_8^2}{\vartheta_2^2\vartheta_{10}^2}\,.$$

defines a Rosenhain triple (c.f. Gaudry [**8**, §7.5]).

4. Fourier series expansions

We now describe the Fourier expansion of even theta constants restricted to a Humbert surface of discriminant $\Delta \equiv 0$ or 1 mod 4, adapted from ideas in Runge's paper [**16**].

Write $\Delta = 4k + \ell$ where ℓ is either 0 or 1, hence the pair (k, ℓ) is uniquely determined. From equation $(*)$ the Humbert surface of discriminant Δ can be defined by the set

$$H_\Delta = \left\{ \begin{pmatrix} \tau_1 & \tau_2 \\ \tau_2 & k\tau_1 + \ell\tau_2 \end{pmatrix} \in \mathcal{H}_2 \right\}$$

modulo the usual $\mathrm{Sp}_4(\mathbb{Z})$ equivalence relation. Restrict θ_{abcd} to H_Δ to get

$$\theta_{abcd}(\tau) \quad = \quad \sum_{(x_1,x_2)\in\mathbb{Z}^2} e^{\pi i(x_1c+x_2d)} r^{(2x_1+a)^2+k(2x_2+b)^2} q^{2(2x_1+a)(2x_2+b)+\ell(2x_2+b)^2}$$

where $r = e^{2\pi i\tau_1/8}$ and $q = e^{2\pi i\tau_2/8}$. Unfortunately the exponent of q can be negative. To overcome this difficulty, make the invertible substitution $r = pq$ to produce the expansion

$$\sum_{(x_1,x_2)\in\mathbb{Z}^2} (-1)^{x_1c+x_2d} p^{(2x_1+a)^2+k(2x_2+b)^2} q^{(2x_1+a+2x_2+b)^2+(k+\ell-1)(2x_2+b)^2}$$

which is computationally more favourable, being an element of $\mathbb{Z}[p, q]$ which we call the *Fourier expansion of θ_{abcd} restricted to H_Δ*.

Addition and muliptication of restricted Fourier expansions are just the usual addition and muliptication operations in $\mathbb{Z}[[p, q]]$. To compute the expansions of Rosenhain invariants we need to know how to invert elements of $\mathbb{Q}[[p, q]]$ where possible.

It is well known fact about power series rings that $f(p, q) \in \mathbb{Q}[[p, q]]$ is a unit if and only if $f(0, 0) \neq 0$, where the inverse given by the geometric series

$$f(0,0)^{-1} \sum_{n\geq 0} \left(1 - \frac{f(p,q)}{f(0,0)}\right)^n.$$

An implementation on a computer uses truncated Fourier expansions, where arithmetic is done in $\mathbb{Q}[[p, q]]/(p^N, q^N)$ for some positive N. The truncated expansion of f^{-1} can be rapidly computed using $\lceil \log_2(N) \rceil$ iterations of Newton's method.

From the expansions we observe that $\vartheta_1, \vartheta_2, \vartheta_3, \vartheta_4$ have constant term 1, hence are invertible, but $\vartheta_8 = 2p^{1+k}q^{k+\ell-1} + \ldots$ and $\vartheta_{10} = -2p^{1+k}q^{k+\ell-1} + \ldots$ have zero constant term. Fortunately one can show that ϑ_8 and ϑ_{10} are in the ideal $(p^{1+k}q^{k+\ell-1})\mathbb{Z}[[p, q]]$ hence by cancelling out the $p^{1+k}q^{k+\ell-1}$ factors, the quotient $\vartheta_8/\vartheta_{10}$ makes sense in $\mathbb{Z}[[p, q]]$. Thus we are able to compute the Rosenhain invariants $\lambda_1, \lambda_2, \lambda_3$ as Fourier expansions restricted to a Humbert surface.

5. The algorithm

We describe an algorithm to find the equation of an irreducible component of H_Δ in a finite cover of $\mathcal{A}_2$, thus generalising Runge's method to different covering spaces. We shall then apply this to $\mathcal{A}_2(2)$ using Rosenhain invariants as coordinate functions.

Algorithm 5.1. Let $\phi : \mathcal{A}' \to \mathcal{A}_2$ be a finite cover of $\mathcal{A}_2$. Then the preimage $\phi^{-1}(H_\Delta)$ is a union of Humbert components $H_\Delta^{(i)}$. Given functions $\{f_i(\tau)\}_{i=1,\ldots,n}$ generating the function field of $\mathcal{A}'$, compute $H_\Delta^{(i)}(f_1, \ldots, f_n)$ as follows:

(1) Calculate the degree of the Humbert components $H_\Delta^{(i)}$ (given by a predetermined formula derived from Theorem 5.1 below).

(2) Compute power series representations of the $f_i(\tau)$ restricted to $H_\Delta \subset \mathcal{H}_2$.
(3) Solve $H_\Delta^{(i)}(f_1, \ldots, f_n) = 0$ in the power series ring (truncated series with large precision) using linear algebra.

In addition, if ϕ is a Galois cover and we understand the action of the Galois group explicitly, then we can compute all the $H_\Delta^{(i)}$ from the Galois orbit of one component.

5.1. Degree formula. Much arithmetic-geometric information is known regarding Humbert surfaces, and more generally Hilbert modular surfaces (see [**12**], [**17**]). We shall state a famous result of van der Geer, from which the degree of any Humbert surface component in any finite cover can be derived. But first we need to introduce some notation.

Define G_Δ to be the (level 1) Humbert surface divisor

$$G_\Delta = \sum_{\substack{x \geq 1 \\ x^2 | \Delta}} v(\Delta/x^2) H_{\Delta/x^2}$$

where [1]

$$v(\Delta) = \begin{cases} \frac{1}{2} & \text{if } \Delta = 1 \text{ or } 4, \\ 1 & \text{otherwise.} \end{cases}$$

Let $\mathscr{H}_2(z)$ be the elliptic modular form of weight $5/2$ for the group $\Gamma_0(4)$ as defined in Cohen [**5**, §3]. For $\Delta \equiv 0, 1 \pmod 4$ define a_Δ to be the coefficient of $(e^{2\pi i z})^\Delta$ in the Fourier expansion of $120\mathscr{H}_2(z)$. Below is a table listing the first few values of a_Δ:

Δ	1	4	5	8	9	12	13	16	17	20	21	24
a_Δ	10	70	48	120	250	240	240	550	480	528	480	720

TABLE 1. First few values of a_Δ.

These numbers have an elementary description [**5**, Proposition 4.1] due to a formula of Siegel,

$$a_\Delta = 24 \sum_{x \in \mathbb{Z}} \sigma_1\left(\frac{\Delta - x^2}{4}\right) + \begin{cases} 12\Delta - 2 & \text{if } \Delta \text{ is a square,} \\ 0 & \text{otherwise} \end{cases}$$

where $\sigma_1(n) = \sum_{d|n} d$, the sum of positive divisors function.

We can now state the theorem of van der Geer.

THEOREM 5.1. *([**12**, Theorem 8.10]) The Humbert surface divisor G_Δ is the zero divisor of a level* 1 *Siegel modular form of weight* $\deg(G_\Delta) = \frac{1}{2}a_\Delta$. *In particular, we have*

$$\sum_{\substack{x \geq 1 \\ x^2 | \Delta}} v(\Delta/x^2) \deg(H_{\Delta/x^2}) = \frac{1}{2} a_\Delta.$$

The Humbert surface H_Δ is the zero divisor of a Siegel modular form; its weight can be determined computing the degree of H_Δ recursively using the theorem above.

[1] $v(\Delta)$ is the *order of the isotropy subgroup* of H_Δ in $\mathrm{Sp}_4(\mathbb{Z})\backslash\mathcal{H}_2$.

5.1.1. *Degrees in* $\mathcal{A}_2(2)$. The natural map $\phi : \mathcal{A}_2(2) \to \mathcal{A}_2$ is a finite Galois cover (with Galois group S_6), hence all Humbert components in $\phi^{-1}(H_\Delta) \subset \mathcal{A}_2(2)$ are hypersurfaces of the same degree. The number of Humbert components $m(\Delta)$ in the Satake compactification $\mathcal{A}_2^*(2)$ of $\mathcal{A}_2(2)$ has been determined by Besser [**1**]:

$$m(\Delta) = \begin{cases} 10 & \text{if } \Delta \equiv 1 \bmod 8 \\ 15 & \text{if } \Delta \equiv 0 \bmod 4 \\ 6 & \text{if } \Delta \equiv 5 \bmod 8 \end{cases}.$$

With this information, the degree of an irreducible polynomial $F^*_{\Delta,i}$ defining a Humbert component in $\mathcal{A}_2^*(2)$ is given by the recursive formula [2]

$$a_\Delta = \sum_{x>0} m(\Delta/x^2) \deg(F^*_{(\Delta/x^2),i}).$$

This provides an upper bound on the degree of the polynomials $F_{\Delta,i}(e_1, e_2, e_3)$. From computational evidence it appears $\deg F_\Delta = \deg F^*_\Delta$ for nonsquare discriminants Δ and that $\deg F_{n^2} = (1 - \frac{1}{n}) \deg F^*_{n^2}$ for all n.

Δ	1	4	5	8	9	12	13	16	17	20	21	24
$\deg(F^*_{\Delta,i})$	1	4	8	8	24	16	40	32	48	32	80	48

TABLE 2. Table of degrees

5.2. Algebraic relations and optimizations. From the previous sections we can write down Rosenhain invariants e_1, e_2, e_3 represented as truncated power series. We know the degree of the relation we are searching for. To find an algebraic relation of degree d, compute all monomials in e_1, e_2, e_3 of degree atmost d and use linear algebra to find linear dependencies between the monomials.

We now illustrate our algorithm by computing a Humbert component of H_5.

EXAMPLE 5.2. ($\Delta = 5$). The Fourier expansions of the Rosenhain invariants restricted to H_5 begin with the terms

$$\begin{aligned} e_1 &= 1 + 16p^4q^8 + O(p^{12}q^{12}), \\ e_2 &= 1 + 4q^4 + 8q^8 - 8p^4q^4 - 24p^4q^8 + 4p^8q^8 + 48p^8q^8 + O(p^{12}q^{12}), \\ e_3 &= 1 + 4q^4 + 8q^8 + 8p^4q^4 + 40p^4q^8 + 4p^8q^8 + 48p^8q^8 + O(p^{12}q^{12}). \end{aligned}$$

From the degree formula, the defining polynomial has degree 8. Using power series with precision 65, we compute the Humbert polynomial:

$$\begin{aligned} &e_2^2e_3^2 - 2e_2^2e_3^3 + e_2^2e_3^4 + 2e_1e_2e_3^3 - 2e_1e_2e_3^4 - 2e_1e_2^2e_3 - 2e_1e_2^2e_3^2 + 4e_1e_2^2e_3^3 + 2e_1e_2^3e_3 \\ &-2e_1e_2^3e_3^3 + e_1^2e_3^4 - 2e_1^2e_2e_3^3 + e_1^2e_2^2 + 4e_1^2e_2^2e_3 - 4e_1^2e_2^2e_3^2 - 2e_1^2e_2^3 - 2e_1^2e_2^3e_3 \\ &+4e_1^2e_2^3e_3^2 + e_1^2e_2^4 - 2e_1^2e_2^4e_3 + e_1^2e_2^4e_3^2 - 2e_1^3e_3^3 - 2e_1^3e_2e_3 + 4e_1^3e_2e_3^2 + 2e_1^3e_2e_3^3 \\ &-2e_1^3e_2^2e_3^2 + 2e_1^3e_2^3e_3 - 2e_1^3e_2^3e_3^2 + e_1^4e_3^2 - 2e_1^4e_2e_3^2 + e_1^4e_2^2e_3^2. \end{aligned}$$

Once one component has been determined, the others can easily be found by looking at the Rosenhain S_6-orbit of a component.

[2]By working with the polynomial degree rather than the component degree, we avoid the annoyance of H_1 having multiplicity 2 which would otherwise complicate the formula.

EXAMPLE 5.3. ($\Delta = 1$). Points of H_1 are not Jacobians of hyperelliptic curves so they cannot have a valid Weierstrass model. Applying Runge's method we find two components $e_1 = e_2$ and $e_2 = e_3$ and permuting the roots we obtain nine relations in total:

$$e_i - e_j = 0,\ i \neq j, \quad e_i = 0, \quad e_i - 1 = 0, \quad i, j \in \{1, 2, 3\}.$$

These are the necessary and sufficient conditions for a Rosenhain model to be degenerate.

5.2.1. *Symmetries.* The fixed groups of the Humbert components in this model can be computed [**10**, §3.5]. As we know, S_6 acts on the Rosenhain invariants via the natural action on $(0, 1, \infty, e_1, e_2, e_3)$. Let h_Δ be the Humbert component computed using the above algorithm. The fixed group of h_Δ for even discriminant splits into two cases,

$$\mathrm{Fix}_{S_6}(h_{4k}) = \begin{cases} G & \text{if } k \text{ is odd} \\ g^{-1}Gg & \text{if } k \text{ is even} \end{cases}$$

where $G \subset S_6$ is a group of order 48 generated by three elements

$$(0, e_1, e_3, \infty, e_2, 1),\ (e_1, e_2) \text{ and } (1, e_1, e_3, e_2);$$

the conjugating element is $g = (1, \infty)(e_1, e_2, e_3)$. Ignoring discriminant 1 which is a degenerate case, the fixed group of $\Delta \equiv 1 \pmod 8$ is a group of order 72 generated by

$$(0, e_1)(1, e_2)(\infty, e_3),\ (e_1, e_2) \text{ and } (e_2, e_3).$$

For $\Delta \equiv 5 \pmod 8$ the fixed group is a group of order 120 generated by

$$(0, e_1)(1, e_2)(\infty, e_3),\ (1, e_3, e_2, e_1, \infty) \text{ and } (\infty, e_1, e_3, e_2).$$

By making use of some of the simpler fixed group symmetries, we can reduce the size of the linear algebra computation. For example, the discriminant 12 component h_{12} satisfies $h_{12}(e_2, e_1, e_3) = h_{12}(e_1, e_2, e_3)$ which means we only need roughly half the number of evaluated power series since $e_1^a e_2^b e_3^c$ and $e_1^b e_2^a e_3^c$ have the same coefficient.

5.3. Runtime analysis. The runtime of the algorithm is greatly affected by the $O(\binom{d+3}{3}) = O(d^3)$ monomials that need to be evaluated. The linear algebra solution requires finding the kernel of a matrix with $O(\binom{d+3}{3})$ rows and in the order of $(N/4)^2$ columns where N is the precision of the power series, which gives a runtime cost of order $O(d^6 N^2)$. To have any chance of finding a unique relation, the number of monomials must be less than the precision used, so that the runtime is at least of order $O(d^9)$.

From the table it is evident that the degree increases with the discriminant, so as it stands this algorithm can only find equations with small degrees. Besides discriminant 21, we managed to produce Rosenhain Humbert components for all the discriminants listed in the above table (see [**9**]). This extends the equations found in the literature ([**13**],[**11**]) which go up to discriminant 8. See the Appendix for the equation of the discriminant 12 Humbert component we found.

6. Applications

In this section we show how Humbert surface equations can be used to speed up endomorphism ring calculations and improve the CRT method of computing Igusa class polynomials [**6**].

6.1. Computing endomorphism rings. Let J be a genus 2 Jacobian defined over $\mathbb{F}_p$ which is geometrically simple and ordinary. Then the endomorphism algebra $\mathrm{End}(J) \otimes \mathbb{Q}$ is a primitive quartic CM-field $K = \mathbb{Q}(\pi)$ where π is the Frobenius endomorphism, and we have that

$$\mathbb{Z}[\pi, \overline{\pi}] \subseteq \mathrm{End}(J) \subseteq \mathcal{O}_K \,.$$

Currently, the best deterministic methods of computing $\mathrm{End}(J)$ are based on the Eisenträger-Lauter algorithm [**6**]. The complexity for calculating $\mathrm{End}(J)$ is determined by the index of largest known suborder of $\mathrm{End}(J)$, namely $\mathbb{Z}[\pi, \overline{\pi}]$. Write $[\mathcal{O}_K : \mathbb{Z}[\pi, \overline{\pi}]] = \prod \ell_i^{e_i}$. Computing $\mathrm{End}(J)$ relies on computing a basis for the $\ell_i^{e_i}$-torsion over its splitting field for each prime $\ell_i \neq p$, an expensive calculation.

We can improve the situation by using Humbert equations. In the case where the Igusa invariants for J lie on the Humbert surface $H_{\mathrm{disc}(K^+)}$, it follows that J has real multiplication by $\mathcal{O}_{K^+}$ and so

$$\mathbb{Z}[\pi, \overline{\pi}] \subseteq \mathcal{O}_{K^+}[\pi, \overline{\pi}] \subseteq \mathrm{End}(J) \subseteq \mathcal{O}_K$$

and the index $[\mathcal{O}_K : \mathcal{O}_{K^+}[\pi, \overline{\pi}]]$ will be *smaller* in many cases.

6.2. Computing Igusa class polynomials mod p. Effective algorithms for computing $\mathrm{End}(J)$ are needed in CM constructions for the cryptographical application of constructing abelian surfaces with a prescribed number of points, over a large prime field. Here one makes use of precomputed polynomials called *Igusa class polynomials*

$$P_K^{(i)} = \prod_{\{A/\mathbb{C} \text{ p.p.a.s} \,|\, \mathrm{End}(A)=\mathcal{O}_K\}/\cong} (X - j_i(A)) \in \mathbb{Q}[X], \ i = 1, 2, 3,$$

where the j_i are Igusa invariants of A.

The CRT method of computing Igusa class polynomials computes the reductions $P_{K,p}^{(i)}$ modulo primes p and combines the information using the Chinese remainder theorem (CRT) to reconstruct the rational coefficients. Let p be a prime for which the Igusa class polynomials split completely. Then

$$P_{K,p}^{(i)} = \prod_{\{A/\mathbb{F}_p \text{ p.p.a.s} \,|\, \mathrm{End}(A)=\mathcal{O}_K\}/\cong_{\mathbb{F}_p}} (X - j_i(A))$$

where the Igusa invariants (j_1, j_2, j_3) for each A are in $\mathbb{F}_p^3$. Hence to compute $P_{K,p}^{(i)}$ we must find all $\overline{\mathbb{F}}_p$-isomorphism classes of principally polarized abelian surfaces A over $\mathbb{F}_p$ having the maximal order $\mathcal{O}_K$ as its endomorphism ring.

We briefly outline the procedure in [**6**, §5.3] used to find Igusa invariants $(j_1, j_2, j_3) \in \mathbb{F}_p^3$ of the genus 2 curves over $\mathbb{F}_p$ whose Jacobian has endomorphism algebra K. For each candidate triple, one constructs the associated hyperelliptic curve C using Mestre's algorithm ([**14**],[**4**]) then counts points on $\mathrm{Jac}(C)$ to determine whether its Frobenius endomorphism is compatible with an ordinary p-Weil number of K. If it passes this test one computes the cardinality of C, thereby determining the endomorphism algebra. If it equals K, we proceed to compute the endomorphism ring. The runtime is dominated by the size of the search space $\mathbb{F}_p^3$.

An order of magnitude improvement is achieved using Humbert surfaces. From the identity $\mathcal{O}_K \cap K^+ = \mathcal{O}_{K^+}$ it follows that the Igusa invariants of p.p.a.s's having endomorphism ring $\mathcal{O}_K$ must lie on H_Δ where $\Delta = \mathrm{disc}(K^+)$. Thus in the case where we have a model for the Humbert surface of discriminant Δ, the search space

is reduced from p^3 triples to the $|H_\Delta(\mathbb{F}_p)| = O(p^2)$ points on the Humbert surface mod p.

We remark that since there are infinitely many primitive quartic CM fields whose maximal order contains $\mathcal{O}_{K^+}$, our improvements can be applied to *all* of these fields.

6.3. Example. Take the cyclic CM field $K = \mathbb{Q}(i\sqrt{2+\sqrt{2}})$ having class number 1, also considered in [**7**, Example 9.1]. The Igusa class polynomials have degree 1 so there is one triple of Igusa invariants having maximal endomorphism ring. Using Freeman and Lauter's implementation of the CRT method, more than 40% of the running time was spent on generating all 1281 genus 2 Jacobians over $\mathbb{F}_{113}$ having endomorphism algebra K (see [**7**, Table 1]). We shall demonstrate our improvements to computing the Igusa class polynomials mod 113.

The real quadratic subfield is $K^+ = \mathbb{Q}(\sqrt{2})$ so the maximal order has discriminant 8. With our improvements, we check each triple of Igusa invariants first to see if it lies on H_8 to avoid unnecessary point counting. This step is simply amounts to evaluating a polynomial in three variables over $\mathbb{F}_{113}$. There are $12665 = 113^2 - 104$ points on $H_8(\mathbb{F}_{113})$, far less than the total 113^3 curves.

Once we have a point on H_8 over $\mathbb{F}_{113}$, we do point counting determine whether its endomorphism algebra is K. The first point we encounter on H_8 having endomorphism algebra K is $(1, 67, 37) \in \mathbb{F}_{113}$ corresponding to a genus 2 Jacobian J with Frobenius endomorphism π satisfying

$$\pi^4 + 4\pi^3 + 102\pi^2 + 452\pi + 12769 = 0.$$

We find that $\mathrm{End}(J)$ is an index 14 suborder of the maximal order. The index of $\mathbb{Z}[\pi, \overline{\pi}]$ in $\mathcal{O}_K$ is $3584 = 2^9 \cdot 7$, but as we know the endomorphism ring is contained in $\mathcal{O}_{K^+}[\pi, \overline{\pi}]$ which has smaller index $[\mathcal{O}_K : \mathcal{O}_{K^+}[\pi, \overline{\pi}]] = 2^3 \cdot 7$, the computation is faster than for a random genus 2 Jacobian over $\mathbb{F}_{113}$ with endomorphism algebra K.

References

[1] Amnon Besser, *Elliptic fibrations of K3 surfaces and QM Kummer surfaces*, Math. Z. **228** (1998), no. 2, 283–308. MR MR1630575 (99f:14047)

[2] Christina Birkenhake and Herbert Lange, *Complex abelian varieties*, second ed., Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 302, Springer-Verlag, Berlin, 2004. MR MR2062673 (2005c:14001)

[3] Christina Birkenhake and Hannes Wilhelm, *Humbert surfaces and the Kummer plane*, Trans. Amer. Math. Soc. **355** (2003), no. 5, 1819–1841 (electronic). MR MR1953527 (2003m:14064)

[4] Gabriel Cardona and Jordi Quer, *Field of moduli and field of definition for curves of genus 2*, Computational aspects of algebraic curves, Lecture Notes Ser. Comput., vol. 13, World Sci. Publ., Hackensack, NJ, 2005, pp. 71–83. MR MR2181874 (2006h:14036)

[5] Henri Cohen, *Sums involving the values at negative integers of L-functions of quadratic characters*, Math. Ann. **217** (1975), no. 3, 271–285. MR MR0382192 (52 #3080)

[6] K. Eisenträger and K. Lauter, *A CRT algorithm for constructing genus* 2 *curves over finite fields*, To appear in Proceedings of 'Arithmetic, Geometry, and Coding Theory', (AGCT-10), Marseille (2005).

[7] D. Freeman and K. Lauter, *Computing endomorphism rings of jacobians of genus 2 curves over finite fields*, Symposium on algebraic geometry and its applications, World Scientific, 2008, pp. 29–66.

[8] Pierrick Gaudry, *Fast genus 2 arithmetic based on theta functions*, Preprint, 2005.

[9] David Gruenewald, *Humbert surface data*, http://sites.google.com/site/humbertequations/.

[10] David Gruenewald, *Explicit algorithms for humbert surfaces*, Ph.D. thesis, University of Sydney, 2008.
[11] Ki-ichiro Hashimoto and Naoki Murabayashi, *Shimura curves as intersections of Humbert surfaces and defining equations of QM-curves of genus two*, Tohoku Math. J. (2) **47** (1995), no. 2, 271–296. MR MR1329525 (96b:14023)
[12] Friedrich Hirzebruch and Gerard van der Geer, *Lectures on Hilbert modular surfaces*, Séminaire de Mathématiques Supérieures [Seminar on Higher Mathematics], vol. 77, Presses de l'Université de Montréal, Montreal, Que., 1981, Based on notes taken by W. Hausmann and F. J. Koll. MR MR639898 (83i:10037)
[13] Georges Humbert, *Sur les fonctions abéliennes singulières*, Œuvres **II** (1936), 297–401.
[14] Jean-François Mestre, *Construction de courbes de genre* 2 *à partir de leurs modules*, Effective methods in algebraic geometry (Castiglioncello, 1990), Progr. Math., vol. 94, Birkhäuser Boston, Boston, MA, 1991, pp. 313–334. MR MR1106431 (92g:14022)
[15] David Mumford, *Tata lectures on theta. II*, Progress in Mathematics, vol. 43, Birkhäuser Boston Inc., Boston, MA, 1984, Jacobian theta functions and differential equations, With the collaboration of C. Musili, M. Nori, E. Previato, M. Stillman and H. Umemura. MR MR742776 (86b:14017)
[16] Bernhard Runge, *Endomorphism rings of abelian surfaces and projective models of their moduli spaces*, Tohoku Math. J. (2) **51** (1999), no. 3, 283–303. MR MR1707758 (2000g:14056)
[17] Gerard van der Geer, *Hilbert modular surfaces*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], vol. 16, Springer-Verlag, Berlin, 1988. MR MR930101 (89c:11073)

Appendix: Equation for discriminant 12

$$
\begin{aligned}
0 \;=\;& e_2^4e_3^4 - 4e_2^4e_3^5 + 6e_2^4e_3^6 - 4e_2^4e_3^7 + e_2^4e_3^8 - 4e_1e_2^3e_3^4 - 16e_1e_2^3e_3^5 + 40e_1e_2^3e_3^6 - \\
& 16e_1e_2^3e_3^7 - 4e_1e_2^3e_3^8 + 160e_1e_2^4e_3^4 - 160e_1e_2^4e_3^5 - 160e_1e_2^4e_3^6 + 160e_1e_2^4e_3^7 - \\
& 132e_1e_2^5e_3^3 - 272e_1e_2^5e_3^4 + 808e_1e_2^5e_3^5 - 272e_1e_2^5e_3^6 - 132e_1e_2^5e_3^7 + 384e_1e_2^6e_3^3 - \\
& 384e_1e_2^6e_3^4 - 384e_1e_2^6e_3^5 + 384e_1e_2^6e_3^6 - 256e_1e_2^7e_3^3 + 512e_1e_2^7e_3^4 - 256e_1e_2^7e_3^5 + \\
& 6e_1^2e_2^2e_3^4 + 40e_1^2e_2^2e_3^5 + 164e_1^2e_2^2e_3^6 + 40e_1^2e_2^2e_3^7 + 6e_1^2e_2^2e_3^8 - 160e_1^2e_2^3e_3^4 - \\
& 352e_1^2e_2^3e_3^5 - 352e_1^2e_2^3e_3^6 - 160e_1^2e_2^3e_3^7 - 272e_1^2e_2^4e_3^3 + 1344e_1^2e_2^4e_3^4 - 608e_1^2e_2^4e_3^5 + \\
& 1344e_1^2e_2^4e_3^6 - 272e_1^2e_2^4e_3^7 + 384e_1^2e_2^5e_3^2 - 416e_1^2e_2^5e_3^3 - 480e_1^2e_2^5e_3^4 - 480e_1^2e_2^5e_3^5 - \\
& 416e_1^2e_2^5e_3^6 + 384e_1^2e_2^5e_3^7 - 762e_1^2e_2^6e_3^2 + 1064e_1^2e_2^6e_3^3 - 348e_1^2e_2^6e_3^4 + 1064e_1^2e_2^6e_3^5 - \\
& 762e_1^2e_2^6e_3^6 + 384e_1^2e_2^7e_3^2 - 384e_1^2e_2^7e_3^3 - 384e_1^2e_2^7e_3^4 + 384e_1^2e_2^7e_3^5 - 4e_1^3e_2e_3^4 - \\
& 16e_1^3e_2e_3^5 + 40e_1^3e_2e_3^6 - 16e_1^3e_2e_3^7 - 4e_1^3e_2e_3^8 - 160e_1^3e_2^2e_3^4 - 352e_1^3e_2^2e_3^5 - \\
& 352e_1^3e_2^2e_3^6 - 160e_1^3e_2^2e_3^7 + 808e_1^3e_2^3e_3^3 - 608e_1^3e_2^3e_3^4 + 3696e_1^3e_2^3e_3^5 - 608e_1^3e_2^3e_3^6 + \\
& 808e_1^3e_2^3e_3^7 - 384e_1^3e_2^4e_3^2 - 480e_1^3e_2^4e_3^3 - 2208e_1^3e_2^4e_3^4 - 2208e_1^3e_2^4e_3^5 - 480e_1^3e_2^4e_3^6 - \\
& 384e_1^3e_2^4e_3^7 - 256e_1^3e_2^5e_3 + 1064e_1^3e_2^5e_3^2 - 608e_1^3e_2^5e_3^3 + 3696e_1^3e_2^5e_3^4 - 608e_1^3e_2^5e_3^5 + \\
& 1064e_1^3e_2^5e_3^6 - 256e_1^3e_2^5e_3^7 + 384e_1^3e_2^6e_3 - 416e_1^3e_2^6e_3^2 - 480e_1^3e_2^6e_3^3 - 480e_1^3e_2^6e_3^4 - \\
& 416e_1^3e_2^6e_3^5 + 384e_1^3e_2^6e_3^6 - 132e_1^3e_2^7e_3 - 272e_1^3e_2^7e_3^2 + 808e_1^3e_2^7e_3^3 - 272e_1^3e_2^7e_3^4 - \\
& 132e_1^3e_2^7e_3^5 + e_1^4e_3^4 - 4e_1^4e_3^5 + 6e_1^4e_3^6 - 4e_1^4e_3^7 + e_1^4e_3^8 + 160e_1^4e_2e_3^4 - 160e_1^4e_2e_3^5 - \\
& 160e_1^4e_2e_3^6 + 160e_1^4e_2e_3^7 - 272e_1^4e_2^2e_3^3 + 1344e_1^4e_2^2e_3^4 - 608e_1^4e_2^2e_3^5 + 1344e_1^4e_2^2e_3^6 - \\
& 272e_1^4e_2^2e_3^7 - 384e_1^4e_2^3e_3^2 - 480e_1^4e_2^3e_3^3 - 2208e_1^4e_2^3e_3^4 - 2208e_1^4e_2^3e_3^5 - \\
& 480e_1^4e_2^3e_3^6 - 384e_1^4e_2^3e_3^7 + 512e_1^4e_2^4e_3 - 348e_1^4e_2^4e_3^2 + 3696e_1^4e_2^4e_3^3 + 1496e_1^4e_2^4e_3^4 + \\
& 3696e_1^4e_2^4e_3^5 - 348e_1^4e_2^4e_3^6 + 512e_1^4e_2^4e_3^7 - 384e_1^4e_2^5e_3 - 480e_1^4e_2^5e_3^2 - 2208e_1^4e_2^5e_3^3 - \\
& 2208e_1^4e_2^5e_3^4 - 480e_1^4e_2^5e_3^5 - 384e_1^4e_2^5e_3^6 - 272e_1^4e_2^6e_3 + 1344e_1^4e_2^6e_3^2 - 608e_1^4e_2^6e_3^3 + \\
& 1344e_1^4e_2^6e_3^4 - 272e_1^4e_2^6e_3^5 + 160e_1^4e_2^7e_3 - 160e_1^4e_2^7e_3^2 - 160e_1^4e_2^7e_3^3 + 160e_1^4e_2^7e_3^4 + \\
& e_1^4e_2^8 - 4e_1^4e_2^8e_3 + 6e_1^4e_2^8e_3^2 - 4e_1^4e_2^8e_3^3 + e_1^4e_2^8e_3^4 - 132e_1^5e_2e_3^3 - 272e_1^5e_2e_3^4 + \\
& 808e_1^5e_2e_3^5 - 272e_1^5e_2e_3^6 - 132e_1^5e_2e_3^7 + 384e_1^5e_2^2e_3^2 - 416e_1^5e_2^2e_3^3 - 480e_1^5e_2^2e_3^4 - \\
& 480e_1^5e_2^2e_3^5 - 416e_1^5e_2^2e_3^6 + 384e_1^5e_2^2e_3^7 - 256e_1^5e_2^3e_3 + 1064e_1^5e_2^3e_3^2 - 608e_1^5e_2^3e_3^3 + \\
& 3696e_1^5e_2^3e_3^4 - 608e_1^5e_2^3e_3^5 + 1064e_1^5e_2^3e_3^6 - 256e_1^5e_2^3e_3^7 - 384e_1^5e_2^4e_3 - 480e_1^5e_2^4e_3^2 - \\
& 2208e_1^5e_2^4e_3^3 - 2208e_1^5e_2^4e_3^4 - 480e_1^5e_2^4e_3^5 - 384e_1^5e_2^4e_3^6 + 808e_1^5e_2^5e_3 - 608e_1^5e_2^5e_3^2 + \\
& 3696e_1^5e_2^5e_3^3 - 608e_1^5e_2^5e_3^4 + 808e_1^5e_2^5e_3^5 - 160e_1^5e_2^6e_3 - 352e_1^5e_2^6e_3^2 - 352e_1^5e_2^6e_3^3 - \\
& 160e_1^5e_2^6e_3^4 - 4e_1^5e_2^7 - 16e_1^5e_2^7e_3 + 40e_1^5e_2^7e_3^2 - 16e_1^5e_2^7e_3^3 - 4e_1^5e_2^7e_3^4 + 384e_1^6e_2e_3^3 - \\
& 384e_1^6e_2e_3^4 - 384e_1^6e_2e_3^5 + 384e_1^6e_2e_3^6 - 762e_1^6e_2^2e_3^2 + 1064e_1^6e_2^2e_3^3 - 348e_1^6e_2^2e_3^4 + \\
& 1064e_1^6e_2^2e_3^5 - 762e_1^6e_2^2e_3^6 + 384e_1^6e_2^3e_3 - 416e_1^6e_2^3e_3^2 - 480e_1^6e_2^3e_3^3 - 480e_1^6e_2^3e_3^4 - \\
& 416e_1^6e_2^3e_3^5 + 384e_1^6e_2^3e_3^6 - 272e_1^6e_2^4e_3 + 1344e_1^6e_2^4e_3^2 - 608e_1^6e_2^4e_3^3 + 1344e_1^6e_2^4e_3^4 - \\
& 272e_1^6e_2^4e_3^5 - 160e_1^6e_2^5e_3 - 352e_1^6e_2^5e_3^2 - 352e_1^6e_2^5e_3^3 - 160e_1^6e_2^5e_3^4 + 6e_1^6e_2^6 + \\
& 40e_1^6e_2^6e_3 + 164e_1^6e_2^6e_3^2 + 40e_1^6e_2^6e_3^3 + 6e_1^6e_2^6e_3^4 - 256e_1^7e_2e_3^3 + 512e_1^7e_2e_3^4 - \\
& 256e_1^7e_2e_3^5 + 384e_1^7e_2^2e_3^2 - 384e_1^7e_2^2e_3^3 - 384e_1^7e_2^2e_3^4 + 384e_1^7e_2^2e_3^5 - 132e_1^7e_2^3e_3 - \\
& 272e_1^7e_2^3e_3^2 + 808e_1^7e_2^3e_3^3 - 272e_1^7e_2^3e_3^4 - 132e_1^7e_2^3e_3^5 + 160e_1^7e_2^4e_3 - 160e_1^7e_2^4e_3^2 - \\
& 160e_1^7e_2^4e_3^3 + 160e_1^7e_2^4e_3^4 - 4e_1^7e_2^5 - 16e_1^7e_2^5e_3 + 40e_1^7e_2^5e_3^2 - 16e_1^7e_2^5e_3^3 - 4e_1^7e_2^5e_3^4 + \\
& e_1^8e_2^4 - 4e_1^8e_2^4e_3 + 6e_1^8e_2^4e_3^2 - 4e_1^8e_2^4e_3^3 + e_1^8e_2^4e_3^4
\end{aligned}
$$

Groupe de Recherche ERISCS; Parc Scientifique de Luminy-ESIL; 13288 Marseille, France

E-mail address: davidg@maths.usyd.edu.au