

# IGUSA CLASS POLYNOMIALS, EMBEDDINGS OF QUARTIC CM FIELDS, AND ARITHMETIC INTERSECTION THEORY

HELEN GRUNDMAN, JENNIFER JOHNSON-LEUNG, KRISTIN LAUTER, ADRIANA SALERNO,  
BIANCA VIRAY, ERIKA WITTENBORN

ABSTRACT. Bruinier and Yang conjectured a formula for an intersection number on the arithmetic Hilbert modular surface,  $\mathcal{CM}(K).T_m$ , where  $\mathcal{CM}(K)$  is the zero-cycle of points corresponding to abelian surfaces with CM by a primitive quartic CM field  $K$ , and  $T_m$  is the Hirzebruch-Zagier divisors parameterizing products of elliptic curves with an  $m$ -isogeny between them. In this paper, we examine fields not covered by Yang's proof of the conjecture. We give numerical evidence to support the conjecture and point to some interesting anomalies. We compare the conjecture to both the denominators of Igusa class polynomials and the number of solutions to the embedding problem stated by Goren and Lauter.

## 1. INTRODUCTION

Hilbert class polynomials are polynomials whose zeros are  $j$ -invariants of elliptic curves with complex multiplication (CM). Similarly, Igusa class polynomials are polynomials whose zeros are Igusa invariants of genus 2 curves whose Jacobians have CM by a quartic CM field  $K$ . Igusa class polynomials can be hard to compute, mostly because recovering the coefficients from approximations requires a bound on the denominators. A precise description of the denominators would greatly improve the estimated running time of current algorithms to compute Igusa class polynomials [Spa94, vW99, Wen03, EL, GHK<sup>+</sup>06].

The first attempt to understand the primes appearing in the factorization of the denominators was given in [Lau], where it was conjectured that the primes are bounded by the absolute value of the discriminant  $d_K$  of the field  $K$ , and that the primes divide  $d_K - x^2$ , for some integer  $x$ . The divisibility condition actually follows from work of Goren [Gor97] along with the observation that primes in the denominators are primes of superspecial reduction for the abelian surfaces with CM by  $K$ . In [GL07], Goren and Lauter proved a bound on the primes which appear in the factorization of the denominators. In recent work [GL], they have given a bound on the denominators (i.e. bounding the powers of the primes which appear); however, this bound is not sharp.

Igusa invariants can be expressed as rational functions in Eisenstein series and cusp forms. Using this description it can be shown that the primes dividing the denominators are (up to cancellation) the primes  $p$  such that there exists a genus 2 curve  $C$  with CM by  $K$  and a prime ideal  $\mathfrak{p}|p$  with

$$\mathrm{Jac}(C) \cong E \times E' \pmod{\mathfrak{p}}.$$

Goren and Lauter obtained the bound on such primes by showing that these primes are exactly the primes for which there is a solution to the *embedding problem*: the problem of giving an embedding  $\mathcal{O}_K \hookrightarrow \mathrm{End}(E \times E') \subset M_2(\mathbb{B}_{p,\infty})$ , where  $E, E'$  are supersingular elliptic curves over  $\overline{\mathbb{F}}_p$  and  $\mathbb{B}_{p,\infty}$  is the quaternion algebra over  $\mathbb{Q}$  ramified at only  $p$  and  $\infty$ .

Such decomposable Jacobians can be viewed as points on the Siegel moduli space where the arithmetic intersection of the  $\text{CM}(K)$ -cycle with the divisor of the cusp form  $\chi_{10}$  is nonzero at  $p$ .

This arithmetic intersection number on the Siegel moduli space can be related to a sum of intersection numbers of Hirzebruch-Zagier divisors and  $\text{CM}(K)$ -cycles on the Hilbert modular surface associated to the real quadratic subfield of  $K$ . In [BY06], Bruinier and Yang conjectured a formula for the intersection number  $\mathcal{CM}(K) \cdot \mathcal{T}_m$ , where  $\mathcal{CM}(K)$  parameterizes abelian surfaces with complex multiplication by a primitive quartic CM field  $K$ , and  $\mathcal{T}_m$  is a Hirzebruch-Zagier divisor parameterizing products of elliptic curves with an  $m$ -isogeny between them when  $m$  is split in the real quadratic subfield of  $K$ . The results of Bruinier and Yang can be viewed as a generalization of the celebrated formula of Gross and Zagier [GZ85]. Bruinier and Yang conjectured their formula for these arithmetic intersection numbers under the assumption that the real quadratic subfield of  $K$  has prime discriminant. Their formula relates the intersection numbers to the number of ideals of a certain norm in the reflex field of  $K$ . In [Yana, Yanb], Yang gives a detailed treatment of the embedding problem and uses it, along with other techniques, to prove the conjectured intersection formula under certain conditions on the CM field  $K$ .

For a given CM field  $K$ , the conjectural formula of Bruinier and Yang is straightforward to compute. Thus, if the Bruinier-Yang formula held for all  $K$ , the formula would give a way to compute the denominators precisely (up to cancellation).

In this paper, we compare the number of solutions to the embedding problem, the denominators in the Igusa class polynomials, and the conjectural formula of Bruinier and Yang for the 13 CM fields found in [vW99]. Only 6 of these fields are covered by Yang's proof of the conjecture. We give numerical evidence to support the conjecture and point to some interesting anomalies and some possible explanations for these discrepancies. Such a project was suggested in the Introduction and Section 9 of [BY06], and we give here the first numerical evidence comparing the conjecture with denominators of Igusa class polynomials and counting solutions to the embedding problem. This comparison required developing an algorithm to count the number of solutions to the embedding problem for a given primitive quartic CM field  $K$  and prime number  $p$ . The algorithm is given in Section 6.1 and the **Magma** code for computing the values is given in the Appendix.

The paper is organized as follows. Section 2 contains background on abelian surfaces with complex multiplication by a primitive quartic CM field  $K$ . Section 3 contains a description of Igusa invariants and Igusa class polynomials. It also gives a brief introduction to the algorithms for computing Igusa class polynomials and their connection with generating genus 2 hyperelliptic curves for cryptography. Section 4 introduces arithmetic intersection theory on the arithmetic Hilbert moduli space and explains how it relates to the denominators of Igusa class polynomials. In this section, we also describe the Bruinier-Yang conjecture and the cases in which it is known. Section 5 explains how the denominators of Igusa class polynomials relate to the embedding problem. Section 6 gives an algorithm to count the number of solutions to the embedding problem. Section 7 presents our numerical data and analysis of the findings.

This paper is concerned with computing these intersection numbers from three different points of view: denominators of Igusa class polynomials, arithmetic intersection numbers via the conjectured Bruinier-Yang formula, and embeddings of a CM number field into a matrix

algebra over a quaternion algebra. Thus the paper necessarily requires the introduction of a number of objects from different points of view, and the background is spread over many different references and papers. Therefore, for the readers' convenience, we have tried to include here as much background as possible. Most sections are self-contained, but Section 4 leaves some of the background material to the references.

## 2. ABELIAN SURFACES WITH CM BY $\mathcal{O}_K$

A *CM field* is a totally imaginary quadratic extension of a totally real number field of finite degree. For a CM field  $K$ , let  $K^+$  denote the totally real index 2 subfield of  $K$ . If  $\{\phi_1, \dots, \phi_{2n}\}$  are the  $2n$  complex embeddings of  $K$ , then a *CM-type*  $\Phi$  for  $K$  is a choice of  $n$  distinct complex embeddings, no two of which are complex conjugates of one another. When  $K^+ = \mathbb{Q}$ , CM fields are imaginary quadratic fields.

An *abelian variety with CM by  $K$*  is a pair  $(A, \iota)$  where  $A$  is an abelian variety and  $\iota$  is an isomorphism of  $K$  into  $\text{End}^0(A) := \text{End}(A) \otimes \mathbb{Q}$ . We say  $(A, \iota)$  has type  $(K, \Phi)$  if  $A$  has CM by  $K$  and the analytic representation of  $\text{End}^0(A)$  is equivalent to the direct sum of the  $n$  isomorphisms  $\phi_i \in \Phi$ . One can define a CM-type to be *primitive* if all of the abelian varieties over  $\mathbb{C}$  of that type are *simple*, i.e. have no abelian subvarieties other than  $\{0\}$  and itself. A CM-type  $(K, \Phi)$  is primitive if and only if  $K = K^+(\xi)$ , where  $\xi$  is an element of  $K$  such that  $\xi^2$  is totally negative and  $\text{Im}(\xi^{\phi_i}) > 0$  for  $i = 1, \dots, n$  [Shi98, p. 61]. For quartic CM fields, the only case where non-primitive CM-types arise is the case when  $K$  is biquadratic [Shi98, p. 64]. We will restrict ourselves to the primitive (i.e. non-biquadratic) case in this article.

Let  $(K, \Phi)$  denote a quartic CM field  $K$  with CM-type  $\Phi$ . Define the reflex field of  $(K, \Phi)$  to be

$$K_\Phi = \mathbb{Q} \left( \sum_{\phi \in \Phi} x^\phi \mid x \in K \right).$$

If  $K$  is Galois cyclic, then we have  $K = K_\Phi$  ([Shi98, §8.4]).

Shimura gives a construction of a principally polarized complex abelian variety of a given CM type in [Shi98, §6.1, Theorem 2]: to any ideal  $I \subseteq \mathcal{O}_K$ , associate the abelian variety  $A_I = \mathbb{C}^2 / \Phi(I)$  of dimension 2. It has endomorphism ring  $\mathcal{O}_K$  and we say it has *CM by  $\mathcal{O}_K$* . All abelian varieties with CM by  $\mathcal{O}_K$  are obtained via this construction. A *principal polarization* of  $A_I$  is an isomorphism between  $A_I$  and its dual  $\widehat{A_I} = \mathbb{C}^2 / \Phi(\bar{I}^{-1} \mathcal{D}_K^{-1})$ , where

$$\mathcal{D}_K^{-1} = \{x \in K \mid \text{Tr}_{K/\mathbb{Q}}(x\mathcal{O}_K) \subseteq \mathbb{Z}\}$$

is the inverse different. If  $\pi$  is a totally imaginary element of  $K$  which satisfies  $\Phi(\pi) \in (i\mathbb{R}_{>0})^2$  and  $\pi I \bar{I} = \mathcal{D}_K^{-1}$ , then the map  $A_I \rightarrow \widehat{A_I}$  given by

$$(z_1, z_2) \mapsto (\phi_1(\pi)z_1, \phi_2(\pi)z_2)$$

is an isomorphism ([Shi98, p. 102–104]).

Let  $K$  be a fixed primitive quartic CM-field and fix a CM-type  $\Phi : K \rightarrow \mathbb{C}^2$ . Let  $A/\mathbb{C}$  be a principally polarized abelian surface of CM-type  $(K, \Phi)$  with endomorphism ring isomorphic to  $\mathcal{O}_K$ . We define a group  $\mathfrak{C}(K) = \{(\mathfrak{a}, \alpha)\} / \sim$  where  $\mathfrak{a}$  is a fractional ideal of  $\mathcal{O}_K$  such that  $\mathfrak{a}\bar{\mathfrak{a}} = (\alpha)$ , with  $\alpha \in K^+$  totally positive. Two pairs  $(\mathfrak{a}, \alpha)$  and  $(\mathfrak{b}, \beta)$  are equivalent if and only if there exists a unit  $u \in K^*$  with  $\mathfrak{b} = u\mathfrak{a}$  and  $\beta = u\bar{u}\alpha$ . The multiplication is defined componentwise, and  $(\mathcal{O}_K, 1)$  is the identity element of  $\mathfrak{C}(K)$ .

The group  $\mathfrak{C}(K)$  naturally acts on the finite set  $S(K, \Phi)$  of isomorphism classes of principally polarized abelian surfaces that have CM by  $\mathcal{O}_K$  of a given type  $\Phi$ . Every principally polarized abelian variety with CM by  $K$  has an analytic representation  $A_I$  determined by an ideal  $I$  and a  $\Phi$ -positive element  $\pi \in K$  giving the principal polarization. We now put

$$(\mathfrak{a}, \alpha) \cdot (I, \pi) = (\mathfrak{a}I, \alpha\pi)$$

for  $(\mathfrak{a}, \alpha) \in \mathfrak{C}(K)$ . By [Shi98, §14.6], for a given  $\Phi$  the action of  $\mathfrak{C}(K)$  on  $S(K, \Phi)$  is transitive and free. In particular, we have  $|\mathfrak{C}(K)| = |S(K, \Phi)|$ , and the sets are often identified.

Abelian surfaces  $A$  of type  $(K, \Phi)$  defined by an ideal  $\mathfrak{a}$  have potentially zero, one, or two principal polarizations. There are zero principal polarizations only if there is no totally positive element  $\alpha \in \mathcal{O}_{K^+}$  with  $\mathfrak{a}\bar{\alpha} = (\alpha)$ . Otherwise there are  $[U : U_1]$  principal polarizations on  $A$ , where  $U$  is the group of all totally positive units of  $K^+$ , and  $U_1$  is the subgroup of norms of units from  $K$ .

For quartic primitive CM fields  $K$ , there are two different possible CM types up to complex conjugation. Let  $\rho$  be complex conjugation, and let  $\phi$  be a non-trivial embedding of  $K$  into  $\mathbb{C}$  other than complex conjugation. A priori, the 4 possible CM types are:  $\Phi = (1, \phi)$ ,  $\bar{\Phi} = (\rho, \rho\phi)$ ,  $\Phi' = (1, \bar{\phi})$ ,  $\bar{\Phi}' = (\rho, \rho\bar{\phi})$ . We denote by  $K_\Phi$  (resp.  $K_{\Phi'}$ , etc.) the set of principally polarized abelian varieties of CM type  $\Phi$  (resp.  $\Phi'$ , etc.).

The description above identifies isomorphism classes of principally polarized abelian varieties of a given type  $\Phi$  with the set  $\{(\mathfrak{a}, \alpha)\} / \sim$ , where  $\mathfrak{a}$  is an ideal of  $\mathcal{O}_K$  such that  $\mathfrak{a}\bar{\alpha} = (\alpha)$ ,  $\alpha$  a totally positive element of  $\mathcal{O}_{K_0}$ . The associated abelian variety is  $A = \mathbb{C}^2 / \Phi(\mathfrak{a})$  and the embedding of  $\mathcal{O}_K$  into  $\text{End}(A)$  sends  $\beta \in \mathcal{O}_K$  to the diagonal matrix with  $(\beta^{\phi_1}, \beta^{\phi_2})$  on the diagonal acting by multiplication on  $\mathbb{C}^2$ .

We can show that  $K_\Phi = K_{\bar{\Phi}}$  by sending  $(\mathfrak{a}, \alpha)$  to  $(\bar{\mathfrak{a}}, \alpha)$ . For the same reason,  $K_{\Phi'} = K_{\bar{\Phi}'}$ . If  $K$  is cyclic, then  $\phi^2$  is complex conjugation and sending  $(\mathfrak{a}, \alpha)$  to  $(\mathfrak{a}^\phi, \alpha^\phi)$  shows that  $K_\Phi = K_{\Phi'}$ .

### 3. GENUS 2 CURVES WITH CM

In cryptography, it is useful to be able to construct genus 2 curves over a finite field  $\mathbb{F}_q$  with a given number of points on its Jacobian, since they can be used to implement discrete-log cryptosystems. Many algorithms to generate such curves have been developed using complex multiplication, all of which require computing certain invariants first studied by Igusa [Igu60]. The closely related Igusa class polynomials have rational coefficients. The known algorithms for computing Igusa class polynomials all require a good bound on the primes appearing in the denominators of these invariants. One of the main goals of this project is to better understand exactly which primes appear in those denominators. In this section, we will review the definitions of the Igusa invariants and explain several algorithms for computing Igusa class polynomials.

**3.1. Generating genus 2 curves for cryptography.** To construct a genus 2 curve  $C$  over a finite field  $\mathbb{F}_q$  with a given number of points  $N$  on its Jacobian, one method is to compute a related quartic CM field  $K$  such that a curve  $C$  with  $\#J(C)(\mathbb{F}_q) = N$  has CM by  $K$ .

For an ordinary genus 2 curve  $C$  over a prime field  $\mathbb{F}_q$ , let  $N_1 = \#C(\mathbb{F}_q)$  and  $N_2 = \#C(\mathbb{F}_{q^2})$ . Then

$$(1) \quad \#J(C)(\mathbb{F}_q) = (N_1^2 + N_2)/2 - q.$$

To find a curve  $C$  over  $\mathbb{F}_q$  such that  $\#J(C) = N$ , first find  $N_1$  and  $N_2$  in the Hasse-Weil intervals for  $\mathbb{F}_q$  and  $\mathbb{F}_{q^2}$  satisfying relation (1). Next, set

$$s_1 := q + 1 - N_1$$

and

$$s_2 := \frac{1}{2} (s_1^2 + N_2 - 1 - q^2).$$

Then the quartic polynomial  $f(t) = t^4 - s_1 t^3 + s_2 t^2 - q s_1 t + q^2$  is the Weil polynomial of a genus 2 curve as long as the exceptional cases listed in [HNR09, Theorem 1.2] are avoided. Note that if  $s_2$  is prime to  $q$ , then the Jacobian is ordinary [How95, p.2366]. Under those conditions and assuming that  $f(t)$  is an irreducible polynomial in  $\mathbb{Q}[t]$ , the Jacobian of the curve has endomorphism ring equal to an order in the quartic CM field  $K = \mathbb{Q}[t]/(f(t))$ . Also, if  $K$  can be written in the form  $K = \mathbb{Q}(i\sqrt{a + b\sqrt{d}})$ , with  $a, b, d \in \mathbb{Z}$  and  $d$  and  $(a, b)$  square-free, then  $K$  is a primitive CM field if and only if  $a^2 - b^2 d$  is not a square [KW89, p.135].

To find a curve with CM by  $K$ , one method is to compute its Igusa invariants by evaluating certain Siegel modular functions at CM points associated to  $K$  in the Siegel moduli space. Igusa invariants will be explained in the next section.

**3.2. Igusa invariants and Igusa class polynomials.** Recall that the  $j$ -invariant of an elliptic curve can be calculated in two ways. One can compute it as a value of the modular  $j$ -function on a lattice defining the elliptic curve as a complex torus over  $\mathbb{C}$ , or directly from the coefficients of the equation defining the elliptic curve. Similarly, the three Igusa invariants of a genus 2 curve can be calculated in two different ways.

Let  $y^2 = f(x)$  be a hyperelliptic curve, where  $f(x)$  is a sextic with roots  $\alpha_1, \dots, \alpha_6$  and leading coefficient  $a_6$ . Igusa defined invariants  $A, B, C, D$  as certain symmetric functions of the roots [Igu60]. For example,  $D = a_6^{10} \prod_{i < j} (\alpha_i - \alpha_j)^2$  is the discriminant. The ring of rational functions of the coarse moduli space for hyperelliptic curves of genus 2 is generated by the absolute Igusa invariants, which can be defined as:

$$(2) \quad i_1 := \frac{A^5}{D}, \quad i_2 := \frac{A^3 B}{D}, \quad i_3 := \frac{A^2 C}{D}.$$

This choice of generators is not unique. These invariants are a generalization of the  $j$ -invariant for elliptic curves in the sense that, if  $i_1$  is non-zero and the characteristic is not 2 or 3, these invariants agree for two smooth genus 2 curves if and only if the two curves are isomorphic over an algebraically closed field. Note that if  $f(x)$  defines a smooth genus 2 curve, then  $i_1, i_2, i_3$  are well defined.

The invariants can also be defined in terms of modular functions on the Siegel moduli space. In [Igu62, p. 195], Igusa defined normalized Siegel modular cusp forms  $\chi_{10}$  and  $\chi_{12}$  of weights 10 and 12 in terms of the Siegel-Eisenstein series  $E_w$  for  $w = 4, 6, 10, 12$ . There he used the term *normalized* to mean that the leading coefficient of the Fourier expansion is 1. For our purposes, we will want to work with modular forms that have integral Fourier coefficients which are relatively prime. By working with  $4\chi_{10}$  and  $12\chi_{12}$ , we obtain modular forms normalized in this second sense.

In [GL07, Section 5.2], it was noted that the absolute Igusa invariants defined above,  $i_1$ ,  $i_2$ ,  $i_3$ , can also be expressed in terms of these Eisenstein series and cusp forms as follows:

$$i_1 = 2 \cdot 3^5 \frac{\chi_{12}^5}{\chi_{10}^6}, \quad i_2 = 2^{-3} \cdot 3^3 \frac{E_4 \chi_{12}^3}{\chi_{10}^4}, \quad i_3 = 2^{-5} \cdot 3 \left( \frac{E_6 \chi_{12}^2}{\chi_{10}^3} + 2^2 \cdot 3 \frac{E_4 \chi_{12}^3}{\chi_{10}^4} \right),$$

(where the parentheses in the expression for  $i_3$  were mistakenly left out in [GL07]). It was also remarked there that it follows from the formulas given by Igusa in [Igu67, p. 848] that these  $i_1$ ,  $i_2$ ,  $i_3$  coincide with the invariants defined in terms of theta functions and used for computation by [vW99, Wen03, Lau]. However, it is worth noting that in order to work with invariants which are quotients of normalized modular forms in the second sense, one should actually work with  $2^{-3}i_1$ ,  $2i_2$ ,  $2^3i_3$  as Spallek did [Spa94].

*Igusa class polynomials* are the genus 2 analogue of Hilbert class polynomials. Just as we need three Igusa invariants to define an isomorphism class instead of one  $j$ -invariant, we have a triple of Igusa class polynomials for a CM field  $K$  instead of one Hilbert class polynomial. This triple of polynomials is defined as follows.

$$(3) \quad H_\ell(X) := \prod_{\tau} (X - i_\ell(\tau)), \quad \ell = 1, 2, 3,$$

where the  $i_\ell$  are the absolute Igusa invariants defined above, and the product is taken over all  $\tau \in \mathrm{Sp}(4, \mathbb{Z}) \backslash \mathfrak{h}_2$  such that the associated principally polarized abelian variety has CM by  $\mathcal{O}_K$ . Igusa class polynomials have rational coefficients [Spa94, Satz 5.8] (as opposed to integral coefficients as in the case of Hilbert class polynomials). In the next section, we describe how this plays a key role in the difficulty of computing these polynomials.

**3.3. Algorithms for computing Igusa class polynomials.** The complex analytic method for computing genus 2 curves with a given number of points on the Jacobian is analogous to the Atkin-Morain algorithm for elliptic curves [AM93]. Recall that the Atkin-Morain algorithm computes the Hilbert class polynomial of an imaginary quadratic field  $K$  by evaluating the modular  $j$ -invariants of all elliptic curves with CM by  $K$  to high precision. The complex analytic method [Spa94, vW99, Wen03] for generating genus 2 curves takes as input a primitive quartic CM field and evaluates the Igusa invariants to high precision to form the class polynomials with coefficients in  $\mathbb{Q}$ . Computing the Igusa invariants to high precision is difficult to do efficiently. To give an algorithm requires a bound on the denominators of the class polynomials, and no such bound was known at the time of those papers.

Given a triple of roots of these polynomials, Mestre gave an algorithm to recover the equation of a genus 2 curve from its invariants [Mes91]. So to find a genus 2 curve, first find roots of the polynomials modulo a prime number  $p$  and then use Mestre's algorithm to construct a genus 2 curve over  $\mathbb{F}_p$  whose Jacobian has CM by  $K$ .

In [EL], Lauter and Eisenträger present a *CRT algorithm*, an alternative to the complex analytic algorithm to compute the Igusa class polynomials. The CRT algorithm takes as input a quartic CM field  $K$  and a constant  $c$  such that all denominators divide  $c$ . The algorithm first computes the Igusa class polynomials modulo small primes  $\ell$  by finding all curves with the right zeta function and the right endomorphism ring modulo  $\ell$ . It then forms the three polynomials whose roots are the invariants of those curves. Finally, it uses the Chinese Remainder Theorem (CRT) and the constant  $c$  to obtain the Igusa class polynomials with coefficients in  $\mathbb{Q}$ .

There is another alternative approach to computing Igusa class polynomials using  $p$ -adic arithmetic ([GHK<sup>+</sup>06]). The method is similar to the complex analytic algorithm, except the values are calculated to a high  $p$ -adic precision, instead of a complex precision. This algorithm also requires a bound on the denominators.

Notice that all three algorithms require a bound on the denominators, and their running time is directly affected by the sharpness of the bound. In the complex analytic and  $p$ -adic algorithms, it is required to bound the amount of precision needed in the approximation of the  $j_i$ -values. In the CRT algorithm, a common multiple of the denominators is needed. Thus, an exact formula for the denominators would be very useful.

#### 4. ARITHMETIC INTERSECTION THEORY AND DENOMINATORS OF IGUSA CLASS POLYNOMIALS

In this section we describe how the denominators of Igusa class polynomials are related to arithmetic intersection numbers on the Siegel moduli space of principally polarized abelian surfaces and explain how this relates to intersection numbers on the Hilbert modular surface and the conjectural formula of Bruinier and Yang for the intersection number  $\mathcal{CM}(K).\mathcal{T}_m$ .

It is a classical fact that the zero locus of  $\chi_{10}$  on the coarse moduli space of abelian surfaces consists of exactly those abelian surfaces that decompose as a product of elliptic curves with the product polarization. The arithmetic analogue of this statement was proved in [GL07, Cor 5.1.2], that if a prime  $\mathfrak{p}$  divides the denominator of  $(f/(4\chi_{10})^k)(\tau)$ , for  $\tau$  a CM point corresponding to a smooth curve  $C$  and  $f$  a Siegel modular form of weight  $10k$  with integral Fourier coefficients with  $\gcd 1$ , then  $C$  has bad reduction modulo  $\mathfrak{p}$ .

The absolute Igusa invariants are defined above as rational functions of the Siegel modular forms  $\chi_{10}$ ,  $\chi_{12}$ ,  $\psi_4$ , and  $\psi_6$ , with only powers of  $\chi_{10}$  in the denominators. Although this definition of the invariants is given in terms of genus 2 curves over  $\mathbb{C}$ , the Igusa invariants can also be defined for genus 2 curves over finite fields (as in formula 2 above). Furthermore, the Igusa invariants evaluated at CM points are algebraic numbers and can be reduced modulo suitable primes. Avoiding bad primes in the denominators, we have [EL, Thm 2]

$$i_\ell(C \bmod \mathfrak{p}) = i_\ell(C) \bmod \mathfrak{p}.$$

Thus the valuation of the denominator of the constant term of  $H_1$  at a prime  $p$  is the sum of the order of the poles of  $2 \cdot 3^5 \frac{\chi_{12}^5}{\chi_{10}^5}$  at the CM-points over  $\overline{\mathbb{F}}_p$ . We have an analogous statement for the Igusa invariants  $H_2$  and  $H_3$ . Since  $\chi_{12}$ ,  $\psi_4$ , and  $\psi_6$  have no poles, the orders of the poles of  $i_\ell$  are bounded above by suitable multiples of the order of zeros of  $\chi_{10}$ . Experimentally, we observe that usually  $\chi_{12}$ ,  $\psi_4$ , and  $\psi_6$  do not share zeros of high multiplicity with  $\chi_{10}$ , so the order of the poles should be close to the order of zeros of a suitable power of  $\chi_{10}$ . Computing the order of zeros of  $\chi_{10}$  is equivalent to computing the arithmetic intersection number  $\text{div}(\chi_{10}).\mathcal{CM}(K)$  (explained below) of the divisor of  $\chi_{10}$  with the cycle of CM points associated to  $K$ .

To compute the arithmetic intersection number  $\text{div}(\chi_{10}).\mathcal{CM}(K)$ , first note that, up to a power of 2,  $\chi_{10} = \Psi_{1,\text{Siegel}}^2$  ([BY06, Remark 9.3]), where  $\Psi_{1,\text{Siegel}}$  is the normalized Siegel-Borchers product of discriminant 1 whose divisor is  $G_1$ , the Humbert surface of discriminant 1. Thus at all primes except possibly 2, we need to compute  $2G_1.\mathcal{CM}(K)$ . The Humbert surface  $G_1$  can be pulled back to a sum of Hirzebruch-Zagier divisors  $T_m$  on the Hilbert

moduli space, and so the quantity to be computed can be expressed as a sum of intersection numbers of the form  $\mathcal{CM}(K).\mathcal{T}_m$  on the Hilbert moduli space.

We now explain all of this in more detail. The presentation in the rest of this section follows closely the treatment in [Yana, Yanb, BBGK07]. For further background, good references are the books of [vdG88, Gor02, KRY06]. In Section 4.1, we describe the Hilbert moduli space and the moduli interpretation of Hirzebruch-Zagier divisors and CM-cycles. In Section 4.2, we explain arithmetic intersection theory and the meaning of  $\mathcal{CM}(K).\mathcal{T}_m$ . In Section 4.3, we explain the relationship between the Humbert surface and Hirzebruch-Zagier divisors. In Section 4.4, we describe the Bruinier-Yang conjectural formula for these intersection numbers.

**4.1. The Hilbert moduli space and Hirzebruch-Zagier divisors.** Fix  $F$ , a real quadratic extension of  $\mathbb{Q}$  with different  $\mathcal{D}_F$ . The Hilbert moduli space parametrizes principally polarized abelian surfaces  $A$  with *real multiplication by  $\mathcal{O}_F$* , i.e. with a fixed embedding  $\iota: \mathcal{O}_F \hookrightarrow \text{End}(A)$ . More precisely, the arithmetic Hilbert moduli space  $\mathcal{M}$  is the moduli stack that associates a scheme  $S$  over  $\mathbb{Z}$  to the set of triples  $(A, \iota, \lambda)$  where

- (1)  $A$  is an abelian surface over  $S$ ,
- (2)  $\iota: \mathcal{O}_F \hookrightarrow \text{End}_S(A)$  gives the structure of real multiplication, and
- (3)  $\lambda: \mathcal{D}_F^{-1} \rightarrow \text{Hom}_{\mathcal{O}_F}(A, A^\vee)^{\text{Sym}}$  is a homomorphism of  $\mathcal{O}_F$ -modules that takes totally positive elements to  $\mathcal{O}_F$ -linear symmetric polarizations and satisfies the Deligne-Pappas condition that  $\mathcal{D}_F^{-1} \otimes A \rightarrow A^\vee$  is an isomorphism of abelian schemes.

The  $\mathbb{C}$ -points of  $\mathcal{M}$  can be identified with the usual Hilbert moduli space  $M = \text{SL}_2(\mathcal{O}_F) \backslash \mathfrak{H}^2$  described in the article of Grundman in this volume [Gru].

Now suppose that  $m$  is a prime number that splits in  $F$ . Let  $Y_0(m) = \Gamma_0(m) \backslash \mathfrak{H}$  be the modular curve parameterizing pairs of elliptic curves with an  $m$ -isogeny. Let  $\mathcal{Y}_0(m)$  be the moduli stack over  $\mathbb{Z}[1/m]$  of pairs of elliptic curves with an  $m$ -isogeny. Bruinier, Burgos Gil, and Kühn [BBGK07, Prop 5.11, 5.13] construct a map from  $\mathcal{Y}_0(m)$  into  $\mathcal{M}$ . They prove that the image of the minimal compactification of  $\mathcal{Y}_0(m)$  is the Zariski closure of the Hirzebruch-Zagier divisor,  $\mathcal{T}_m$ .

Let  $K$  be a primitive quartic CM number field with  $K^+ = F$ . Let  $\mathcal{CM}(K)$  be the moduli stack over  $\mathbb{Z}$  that represents the moduli problem assigning a base scheme  $S$  to the set of triples  $(A, \iota, \lambda)$ , where  $\iota: \mathcal{O}_K \rightarrow \text{End}_S(A)$  gives the  $\mathcal{O}_K$ -action on  $A$  such that the Rosati involution defined by  $\lambda$  induces complex conjugation on  $\mathcal{O}_K$ , and  $(A, \iota|_{\mathcal{O}_F}, \lambda) \in \mathcal{M}(S)$ . Bruinier and Yang also refer to the direct image of  $\mathcal{CM}(K)$  in  $\mathcal{M}$  by  $\mathcal{CM}(K)$ .

**4.2. Arithmetic Intersection Theory.** Following [KRY06, Chapter 2] and [Yana, Yanb], we define the arithmetic intersection number of two cycles on a Deligne-Mumford stack of dimension  $n$  that is proper and flat over  $\mathbb{Z}$ . Let  $\mathcal{Z}_1$  and  $\mathcal{Z}_2$  be two cycles that intersect properly, i.e. their codimensions are  $r_1$  and  $r_2$ , with  $r_1 + r_2 = n$ , and  $\mathcal{Z}_1 \cap \mathcal{Z}_2 = \mathcal{Z}_1 \times_{\mathcal{M}} \mathcal{Z}_2$  is a Deligne-Mumford stack of dimension 0. Then the arithmetic intersection number (written logarithmically) is

$$\begin{aligned} \mathcal{Z}_1.\mathcal{Z}_2 &= \sum_p \sum_{x \in \mathcal{Z}_1 \cap \mathcal{Z}_2(\overline{\mathbb{F}}_p)} \frac{1}{\# \text{Aut}(x)} \log \# \tilde{\mathcal{O}}_{\mathcal{Z}_1 \cap \mathcal{Z}_2, x} \\ &= \sum_p \sum_{x \in \mathcal{Z}_1 \cap \mathcal{Z}_2(\overline{\mathbb{F}}_p)} \frac{1}{\# \text{Aut}(x)} i_p(\mathcal{Z}_1, \mathcal{Z}_2, x) \log p, \end{aligned}$$



where  $\tilde{\mathcal{O}}_{\mathcal{Z}_1 \cap \mathcal{Z}_2, x}$  is the local ring of  $\mathcal{Z}_1 \cap \mathcal{Z}_2$  at  $x$ , and  $i_p(\mathcal{Z}_1, \mathcal{Z}_2, x) = \text{Length } \tilde{\mathcal{O}}_{\mathcal{Z}_1 \cap \mathcal{Z}_2, x}$  is the local intersection at  $x$ .

We are interested in the arithmetic intersection of the cycles  $\mathcal{CM}(K)$  and  $\mathcal{T}(m)$  on the moduli stack  $\mathcal{M}$ . Using the moduli interpretation of the cycles  $\mathcal{CM}(K)$  and  $\mathcal{T}_m$ , it is clear that a geometric point  $x$  in  $\mathcal{CM}(K) \cap \mathcal{T}_m = \mathcal{CM}(K) \times_{\mathcal{M}} \mathcal{T}_m$  is indexed by a pair  $(\phi: E \rightarrow E', \iota)$ , where  $\phi \in \mathcal{Y}_0(m)(\overline{\mathbb{F}}_p)$  and  $\iota: \mathcal{O}_K \rightarrow \text{End}_{\mathcal{O}_F}(B)$  is an embedding such that the Rosati involution associated to  $\lambda$  induces complex conjugation on the image of  $K$  and where  $(B, \lambda)$  is the polarized abelian surface in  $\mathcal{T}_m$  which is the image of  $\phi$ . Denote by  $i_p(\phi, \iota) = i_p(\mathcal{CM}(K), \mathcal{T}(m), x)$  the local intersection number at a point  $x = (\phi, \iota)$ . It follows from deformation theory that  $i_p(\phi, \iota) = \text{Length}(\mathbb{W}[[t, t']]/I)$ , where  $\mathbb{W}$  is the Witt ring of  $\overline{\mathbb{F}}_p$  and  $I$  is the minimal ideal such that  $\phi$  can be lifted to an isogeny modulo  $I$  and the embedding  $\iota$  can be lifted to an embedding modulo  $I$  [Yanb, Eq. (3.7)].

**4.3. The relationship between the Hilbert and Siegel moduli spaces.** Let  $M$  be the Hilbert modular surface associated to the real quadratic field of discriminant  $D$ ,  $F = \mathbb{Q}(\sqrt{D})$ . Recall that forgetting real multiplication gives a morphism  $\phi_D$  from the Hilbert moduli space  $M$  to the Siegel moduli space  $X = \text{Sp}(4, \mathbb{Z}) \backslash \mathfrak{h}_2$ . The image  $G_D \subset X$  of  $M$  is known as the Humbert surface of discriminant  $D$ . For every  $G_D$ , there is a normalized integral Siegel Borchers product  $\Psi_{D, \text{Siegel}}$  whose divisor is equal to  $G_D$  (up to multiplication by  $\pm 1$ ). Let  $\mathcal{G}_D$  denote the flat closure of  $G_D$  in the Siegel moduli stack representing principally polarized abelian surfaces.

The pullback to the Hilbert modular surface  $M$  of a Humbert surface  $G_{D'}$  under the morphism  $\phi_D$  is a linear combination of Hirzebruch-Zagier divisors [vdG88, p.215]:

$$(4) \quad \phi_D^*(G_{D'}) = \sum_{\substack{x \in \mathbb{Z}_{\geq 0} \\ x < \sqrt{DD'} \\ x^2 \equiv DD' \pmod{4}}} T_{(DD' - x^2)/4},$$

for  $D'$  a positive discriminant, and the same is true of the flat closures of these cycles in  $\mathcal{M}$ . By Theorem 2.8 in [BY06] we also know that the pullback to  $M$  of the Borchers product  $\Psi_{D', \text{Siegel}}$  is a Hilbert-Borchers product with divisor (4). In our case, the denominators of the Igusa functions are powers of  $\chi_{10}$ , and  $\chi_{10} = \Psi_{1, \text{Siegel}}^2$  up to a power of 2 and its divisor is  $2G_1$ . So we can now express the quantity that we want to compute,  $2\mathcal{G}_1 \cdot \mathcal{CM}(K)$  as a sum

$$2 \sum_{\substack{x > 0 \\ \frac{D-x^2}{4} \in \mathbb{Z}_{\geq 0}}} \mathcal{CM}(K) \cdot \mathcal{T}_{(D-x^2)/4}.$$

**4.4. Bruinier-Yang Conjecture.** Let  $K = F(\sqrt{\Delta})$  be a non-biquadratic quartic CM field  $K$ , let  $\Phi$  be a CM type, and let  $(\tilde{K}, \tilde{\Phi})$  be a fixed reflex field and type. Bruinier and Yang assume that  $F = \mathbb{Q}(\sqrt{D})$  is a real quadratic field with  $D$  a prime congruent to 1 modulo 4. The real quadratic subfield of  $\tilde{K}$  is  $\tilde{F} = \mathbb{Q}(\sqrt{\Delta\Delta'})$ , where  $\Delta'$  is the real conjugate of  $\Delta$ . Let  $\tilde{D}$  be the norm of the relative discriminant of  $K/F$  and let  $d_{\tilde{K}/\tilde{F}}$  be the relative discriminant of  $\tilde{K}/\tilde{F}$ . Bruinier and Yang's conjectural formula for the arithmetic intersection number on

the Hilbert moduli space is:

$$\mathcal{CM}(K) \cdot \mathcal{T}_m = \frac{1}{2} \sum_p b_m(p) \log p,$$

where

$$b_m(p) \log p = \sum_{\mathfrak{p}|p} \sum_{t=\frac{n+m\sqrt{\tilde{D}}}{2D} \in d_{\tilde{K}/\tilde{F}}^{-1}, |n| < m\sqrt{\tilde{D}}} B_t(\mathfrak{p}).$$

The ideals  $\mathfrak{p}|p$  are ideals of  $\mathcal{O}_{\tilde{F}}$  and

$$B_t(\mathfrak{p}) = \begin{cases} 0 & \text{if } \mathfrak{p} \text{ is split in } \tilde{K} \\ (\text{ord}_{\mathfrak{p}} t + 1) \rho(td_{\tilde{K}/\tilde{F}} \mathfrak{p}^{-1}) \log |\mathfrak{p}| & \text{if } \mathfrak{p} \text{ is not split in } \tilde{K} \end{cases}$$

where  $\rho(\mathfrak{a}) = \#\{\mathfrak{A} \subset \mathcal{O}_{\tilde{K}} \mid N_{\tilde{K}/\tilde{F}} \mathfrak{A} = \mathfrak{a}\}$ .

Yang has proved the conjecture [Yana, Yanb] under the assumptions that  $D \equiv 1 \pmod{4}$  is prime,  $\Delta\Delta' \equiv 1 \pmod{4}$  is prime, and  $\mathcal{O}_K$  is a free  $\mathcal{O}_F$ -module generated by 1 and  $\frac{1}{2}(w + \sqrt{\Delta})$ , for some  $w \in \mathcal{O}_{\tilde{F}}$ . Note that Yang sets  $\tilde{D} = \Delta\Delta'$ , which is equal to the norm of the relative discriminant of  $K/F$  under his assumptions. They are not necessarily equal in general, in particular, they differ for many of the fields listed in [vW99]. In our computations, we use the convention from [BY06], that  $\tilde{D} = N_{F/\mathbb{Q}}(\text{Disc}_{K/F})$  and we find that with this convention, the predicted arithmetic intersection number agrees with the computed values for the number of embeddings and the denominators of Igusa class polynomials in many cases.

## 5. QUATERNION ALGEBRAS AND EMBEDDINGS OF CM FIELDS

In this section, we explain the connection given in [GL07] between denominators of Igusa class polynomials and certain embeddings of the ring of integers of  $K$  into the matrix algebra  $M_2(\mathbb{B}_{p,\infty})$ , where  $p$  is a prime number and  $\mathbb{B}_{p,\infty}$  is the unique (up to isomorphism) quaternion algebra over  $\mathbb{Q}$  which is ramified at only  $p$  and  $\infty$ .

Let  $C$  be a smooth projective genus 2 curve such that  $\text{Jac}(C)$  has CM by  $\mathcal{O}_K$ . There is a number field  $L$  such that all of the endomorphisms of  $\text{Jac}(C)$  are defined over  $L$  and thus  $\text{Jac}(C)$  has everywhere good reduction. It is observed in [GL07, §4.1] that if  $K$  is a primitive CM field and  $C$  has bad reduction at a rational prime  $p$ , then for a prime  $\mathfrak{p}|p$  of  $L$ , the reduction of  $\text{Jac}(C)$  modulo  $\mathfrak{p}$  is isomorphic over  $\mathcal{O}_L/\mathfrak{p}$  to a product of supersingular elliptic curves  $E_1 \times E_2$  with the product polarization. Moreover, we have that  $E_1$  is isogenous to  $E_2$  as otherwise

$$\text{End}(E_1 \times E_2) = \text{End}(E_1) \times \text{End}(E_2)$$

contradicting  $K \hookrightarrow \text{End}^0(\text{Jac}(C))$  with  $K$  primitive. Goren and Lauter prove that in fact the existence of a smooth projective genus 2 curve  $C$  that has CM by  $\mathcal{O}_K$  and has bad reduction at  $\mathfrak{p}$  is equivalent to the existence of an embedding

$$\iota : \mathcal{O}_K \hookrightarrow \text{End}(E_1 \times E_2)$$

such that the Rosati involution coming from the product polarization induces complex conjugation on  $\mathcal{O}_K$  [GL07, Lemma 4.1.1 and Thm. 4.2.1].

**5.1. Relating  $\text{End}(E_1 \times E_2)$  to a subring of  $M_2(\mathbb{B}_{p,\infty})$ .** We view an element  $f \in \text{End}(E_1 \times E_2)$  as a matrix  $\begin{pmatrix} f_{1,1} & f_{1,2} \\ f_{2,1} & f_{2,2} \end{pmatrix}$  where  $f_{i,j} \in \text{Hom}(E_j, E_i)$ . Then the composition of endomorphisms  $f \circ g$  corresponds to multiplication of the matrices and the Rosati involution  $f \mapsto f^\vee$  corresponds to

$$\begin{pmatrix} f_{1,1} & f_{1,2} \\ f_{2,1} & f_{2,2} \end{pmatrix} \mapsto \begin{pmatrix} f_{1,1}^\vee & f_{2,1}^\vee \\ f_{1,2}^\vee & f_{2,2}^\vee \end{pmatrix}$$

Fix a supersingular elliptic curve  $E/\overline{\mathbb{F}}_p$  and an isomorphism  $\psi: \text{End}(E) \rightarrow \mathcal{O}$  where  $\mathcal{O}$  is a maximal order in  $\mathbb{B}_{p,\infty}$ . Note that by using  $\psi$  we can view elements of  $\text{End}(E) \otimes \mathbb{Q}$  as elements of  $\mathbb{B}_{p,\infty}$ . Given an element  $\phi \in \text{Hom}(E, E')$ , we obtain an embedding  $\text{Hom}(E', E) \rightarrow \text{End}(E)$  by mapping  $f \mapsto f \circ \phi$ . Thus we can view  $\text{Hom}(E', E)$  as an ideal of  $\text{End}(E)$  or, by using the isomorphism  $\psi$ , as a left ideal  $I$  of  $\mathcal{O}$ . Note that if we replace  $\phi$  by a different endomorphism  $\phi'$ , this corresponds to right multiplying  $I$  by  $\psi(\phi^{-1}\phi') \in \mathbb{B}_{p,\infty}$  (where  $\phi^{-1}\phi' = (\phi^\vee\phi') / \deg(\phi)$ ) can be viewed as an element of  $\text{End}(E) \otimes \mathbb{Q}$ ). Thus a different choice of  $\phi$  results in a different ideal, but one in the same *ideal class*. In fact, the map

$$\begin{aligned} \{\text{supersingular curves over } \overline{\mathbb{F}}_p\} &\rightarrow \{\text{left ideal classes of } \mathcal{O}\} \\ E' &\mapsto \psi(\text{Hom}(E', E)\phi) \text{ for some } \phi \in \text{Hom}(E, E') \end{aligned}$$

is a bijection. Given a morphism  $\phi$  and the ideal  $I = \psi(\text{Hom}(E', E)\phi)$ , we can also identify the group  $\text{Hom}(E, E')$  with the ideal  $I^{-1}$  by the map

$$\text{Hom}(E, E') \rightarrow \mathbb{B}_{p,\infty}, \quad g \mapsto \psi(\phi^{-1}g).$$

We would like to view  $\text{End}(E')$  as a subring of  $\mathbb{B}_{p,\infty}$  in a compatible way. Let  $\phi$  denote a fixed element of  $\text{Hom}(E, E')$ . Then we obtain a map

$$\text{End}(E') \rightarrow \mathbb{B}_{p,\infty}, \quad g \mapsto \psi(\phi^\vee g \phi) / (\deg(\phi)).$$

Since this map is an embedding, the image  $\mathcal{O}'$  is isomorphic to  $\text{End}(E')$  and therefore is a maximal order in  $\mathbb{B}_{p,\infty}$ . One can check that  $\mathcal{O}'$  is the right order of  $I := \psi(\text{Hom}(E', E)\phi)$ . Thus, given a fixed  $\phi \in \text{Hom}(E, E')$  and a fixed isomorphism  $\psi: \text{End}(E) \rightarrow \mathcal{O} \subseteq \mathbb{B}_{p,\infty}$ , we can identify  $\text{End}(E \times E')$  with the subring of  $M_2(\mathbb{B}_{p,\infty})$ ,

$$\begin{pmatrix} \mathcal{O} & I \\ I^{-1} & \mathcal{O}' \end{pmatrix},$$

where  $I$  and  $\mathcal{O}'$  are defined as above. Under this identification the Rosati involution can be described as

$$\begin{pmatrix} x & y \\ z & w \end{pmatrix}^\vee = \begin{pmatrix} x^\vee & N(I)z^\vee \\ y^\vee/N(I) & w^\vee \end{pmatrix},$$

where  $N(I) := \gcd\{\gamma\gamma^\vee \mid \forall \gamma \in I\}$  is the norm of  $I$ . From this point forward, we will refer interchangeably to elements of  $\text{End}(E \times E')$  and elements of  $\mathcal{R}_{(E, E', \phi)} := \begin{pmatrix} \mathcal{O} & I \\ I^{-1} & \mathcal{O}' \end{pmatrix}$ .

**5.2. Isomorphisms of principally polarized CM abelian varieties.** Two principally polarized abelian varieties with complex multiplication  $(A, \iota_1, \lambda_1)$ ,  $(A, \iota_2, \lambda_2)$  are isomorphic either if  $\iota_1$  and  $\iota_2$  differ by an automorphism of  $\mathcal{O}_K$  or if there exists  $\sigma \in \text{Aut}(A)$  such that  $\sigma^{-1}\iota_1\sigma = \iota_2$  and  $\lambda_1 = \sigma^\vee\lambda_2\sigma$ . We would like to describe the set of  $\sigma \in \text{Aut}(E \times E')$  such

that conjugation by  $\sigma$  preserves the polarization. Preserving the polarization is equivalent to

$$(\sigma^{-1}\psi\sigma)^\vee = \sigma^{-1}\psi^\vee\sigma \quad \text{for all } \psi \in \text{End}(E \times E').$$

Thus  $\sigma\sigma^\vee = \pm 1$ . Let  $\begin{pmatrix} p & q \\ r & s \end{pmatrix} \in \mathcal{R}_{(E,E',\phi)}$  be the element associated to  $\sigma$ . The previous condition implies that  $q = r = 0$  and both  $p$  and  $s$  are isomorphisms, or  $p = s = 0$  and  $q$  and  $r$  are isomorphisms. Note that the latter possibility only occurs if  $E$  and  $E'$  are isomorphic. Let  $\mathcal{U}_{(E,E',\phi)}$  denote the set of elements in  $\mathcal{R}_{(E,E',\phi)}$  of this form, i.e. satisfying the condition that  $\begin{pmatrix} p & q \\ r & s \end{pmatrix} \begin{pmatrix} p & q \\ r & s \end{pmatrix}^\vee = \pm 1$ .

## 6. COUNTING THE NUMBER OF EMBEDDINGS

Let  $\mathcal{O}_K$  denote the ring of integers of  $K$ . If the real quadratic subfield  $F$  of  $K$  has class number 1, then there exists an  $\eta \in \mathcal{O}_K$  such that  $\mathcal{O}_K = \mathcal{O}_F[\eta]$ . Let  $D$  denote the discriminant of  $F$  and let  $\omega := \frac{1}{2}(D + \sqrt{D})$ , a generator of  $\mathcal{O}_F$ . Denote  $\text{Tr}(\eta) = \alpha_0 + \alpha_1\omega$  and  $N(\eta) = \beta_0 + \beta_1\omega$ .

**Proposition 6.1.** *Let  $E, E'$  be supersingular curves over  $\overline{\mathbb{F}}_p$ . Fix an isomorphism  $\psi: \text{End}(E) \rightarrow \mathcal{O}$  where  $\mathcal{O}$  is a maximal order and an element  $\phi \in \text{Hom}(E, E')$ . Determining an embedding*

$$\iota: \mathcal{O}_K \hookrightarrow \text{End}(E \times E')$$

*is equivalent to giving two elements  $\Lambda_1, \Lambda_2 \in \mathcal{R}_{(E,E',\phi)}$  such that*

$$\begin{aligned} & \Lambda_1\Lambda_2 = \Lambda_2\Lambda_1 \\ & \Lambda_1^2 - D\Lambda_1 + \frac{D^2 - D}{4} = 0 \\ (*) \quad & \Lambda_2 + \Lambda_2^\vee = \alpha_0 + \alpha_1\Lambda_1 \\ & \Lambda_2\Lambda_2^\vee = \beta_0 + \beta_1\Lambda_1. \end{aligned}$$

*Proof.* Let  $\iota$  be an embedding. Then  $\Lambda_1 = \iota(\omega)$  and  $\Lambda_2 = \iota(\eta)$  satisfy the conditions above. In the other direction, it is clear that the map that sends  $\omega \mapsto \Lambda_1$  and  $\eta \mapsto \Lambda_2$  gives a well-defined homomorphism from  $\mathcal{O}_K$  to  $\mathcal{R}_{(E,E',\phi)}$ . Therefore it remains to show that the map is injective. Assume that the map is not injective and let  $J$  denote the kernel. If  $J$  is nontrivial then  $\mathcal{O}_K/J$  embeds into  $\mathcal{R}_{(E,E',\phi)}$ . However, since  $\mathcal{O}_K/J$  is a finite abelian group and  $\mathbb{B}_{p,\infty}$  is a torsion-free  $\mathbb{Z}$ -module, this is impossible.  $\square$

We note that the idea behind this lemma is similar to the ideas in [GL07] which used the embedding problem to obtain a bound on the primes dividing the denominator. Goren and Lauter studied pairs of matrices  $M_1, M_2$  in  $\mathcal{R}_{(E,E',\phi)}$  where  $M_1$  satisfies the minimal polynomial of  $\sqrt{D}$  and  $M_2$  satisfies the minimal polynomial of  $\sqrt{\Delta}$  where  $K = F(\sqrt{\Delta})$ .

In light of Proposition 6.1 and Section 5.2, the number of pairs of  $(E \times E', \iota)$ , counted up to isomorphism, is equal to

$$\sum_{\text{unordered pairs } E, E'} \# \frac{\left\{ (\Lambda_1, \Lambda_2) \in \mathcal{R}_{(E,E',\phi)}^2 \text{ satisfying } * \right\}}{(\Lambda_1, \Lambda_2) \sim (U\Lambda_1U^{-1}, U\Lambda_2U^{-1})} \quad \text{where } \phi \in \text{Hom}(E, E') \text{ and } U \in \mathcal{U}_{(E,E',\phi)}$$

We use this formula to count the number of embeddings. Our algorithm is sketched below and our implementation in **Magma** can be found in Appendix A. We make no claims on the running time of the algorithm or the implementation; the algorithm was only implemented to obtain the numerical evidence in Table 7.1.

### 6.1. Algorithm for counting solutions to the embedding problem.

- (1) (Initialize variables) Input  $p, D, \alpha_0, \alpha_1, \beta_0, \beta_1, \tilde{D}$ .
- (2) (Create representation of  $\mathbb{B}_{p,\infty}$ ) Let  $\mathbb{B}_{p,\infty} = (a, -p)$  where  $a$  is the maximal negative integer such that  $\mathbb{B}_{p,\infty}$  is ramified only at  $p$  and  $\infty$ .
- (3) (Create representations of  $\mathcal{R}_{(E,E',\phi)}$  for each unordered pair of elliptic curves  $(E, E')$ ) We represent each  $\mathcal{R}_{(E,E',\phi)}$  by a triple  $(B_1, B_2, B_3)$  where  $B_1$  is a basis for  $\mathcal{O}$ ,  $B_2$  is a basis for  $I$  and  $B_3$  is a basis for  $\mathcal{O}'$ . For each isomorphism class of supersingular elliptic curves, let  $\mathcal{O}$  be a maximal order isomorphic to the endomorphism ring. Then for each left ideal class of  $\mathcal{O}$  let  $I$  be an integral representative and let  $\mathcal{O}'$  be the right order. Take bases to give representatives of  $\mathcal{R}_{(E,E',\phi)}$  for each unordered pair  $(E, E')$ .
  - (a) (Find possibilities for  $\Lambda_1$ ) The condition on  $\Lambda_1$  implies that it is of the form

$$\begin{pmatrix} s_{1,1} & s_{1,2} \\ s_{1,2}^\vee/N(I) & D - s_{1,1} \end{pmatrix},$$

where  $s_{1,1}$  is an integer in  $[(D - \sqrt{D})/2, (D + \sqrt{D})/2]$  and  $s_{1,2}$  is an element in  $I$  with norm equal to

$$-s_{1,1}^2 + Ds_{1,1} - (D^2 - D)/4.$$

There are only finitely many possibilities for each of these, so we iterate over all of them.

- (i) (Find possibilities for  $\Lambda_2$ ) Denote the entries of  $\Lambda_2$  by  $t_{i,j}$ . The condition on  $\Lambda_2 + \Lambda_2^\vee$  implies that  $t_{2,1}$  is determined by  $t_{1,2}$  and  $\Lambda_1$  and that  $t_{1,1}$  and  $t_{2,2}$  have fixed trace. The condition on  $\Lambda_2\Lambda_2^\vee$  implies that  $t_{1,1}, t_{1,2}, t_{2,2}$  have bounded norm. This gives only finitely many possibilities for  $t_{1,1}, t_{1,2}, t_{2,2}$  and we iterate through them all, checking whether the pair  $(\Lambda_1, \Lambda_2)$  satisfies all of the conditions in  $(*)$ . If  $(*)$  is satisfied, then keep  $(\Lambda_1, \Lambda_2)$  in the list, otherwise discard the pair.
  - (ii) (Identify elements that differ by conjugation or automorphisms of  $\mathcal{O}_K$ ) There are only finitely many elements in  $\mathcal{U}_{(E,E',\phi)}$ . For a fixed pair  $(\Lambda_1, \Lambda_2)$ , iterate through all elements  $U$  in  $\mathcal{U}_{(E,E',\phi)}$  and all  $\sigma \in \text{Aut}(\mathcal{O}_K)$  and remove all pairs  $(\sigma(U\Lambda_1U^{-1}), \sigma(U\Lambda_2U^{-1}))$ .
- (4) (Count the embeddings) Count the number of pairs  $(\Lambda_1, \Lambda_2)$ .

## 7. NUMERICAL DATA

In Table 7.1 we examine the 13 fields studied by van Wamelen [vW99]. These 13 fields are the only fields  $K$  such that there exists a genus 2 curve  $C$  over  $\mathbb{Q}$  with CM by  $K$ , and they are all quartic Galois cyclic extensions of  $\mathbb{Q}$ . For each field  $K$ , we list

- (1) the factorization of the rational sixth root of the denominator of  $\frac{\chi_{12}^5}{\chi_{10}^6}(\tau)$ , where  $\tau$  is a CM-point of  $K$ ,

- (2) the conjectural value of  $2\phi^*G_1\mathcal{CM}(K)$  as predicted by the Bruinier-Yang formula (this was computed via a **Magma** program), and
- (3) the number of solutions to the embedding problem, computed using Algorithm 6.1 and the **Magma** code listed in Appendix A.

The three values listed above should agree if the number of solutions to the embedding problem is counted *with multiplicity*. Unfortunately, our representation of embeddings does not count multiplicity. However, Yang's proof suggests that the value  $(\text{ord}_{\mathfrak{p}} t + 1)/2$  is the multiplicity of an embedding, under certain conditions. We write the Bruinier-Yang values as iterated exponents, where the outer exponent denotes  $(\text{ord}_{\mathfrak{p}} t + 1)/2$ . If there is no outer exponent, then this value is 1. This is the case in most examples, so it appears that most of the embeddings have no multiplicity. We investigate the cases where the Bruinier-Yang conjecture does not agree with the numerical data for the other columns in Section 7.1.

**Remark 7.1.** *Since all of the fields in [vW99] are Galois, there is only one CM-type up to isomorphism. Therefore we multiply the Bruinier-Yang formula by  $1/2$  since the CM-cycle in [BY06] is  $CM(K, \Phi) + CM(K, \Phi')$  where  $\Phi$  is not the complex conjugate of  $\Phi'$ .*

**Remark 7.2.** *In the data we present in Table 7.1, we set  $\tilde{D} = N_{F/\mathbb{Q}}(\text{Disc}_{K/F})$  as in the original conjecture [BY06]. In his proofs, Yang sets  $\tilde{D} = \Delta\Delta'$  which is equal to the norm of the relative discriminant of  $K/F$  under his assumptions, but which is not equal in general.*

**7.1. Analysis of data.** The first remark to make is that, in every example in the table, the powers of the primes in the denominators of the Igusa invariants match the number of solutions to the embedding problem, except for the power of 2 in four examples and the power of 3 in the last row. The power of 3 in the last row appears to be accounted for by multiplicity. The power of 2 is different in the four rows 2, 4, 9, and 11, and we explain why that is accounted for by cancellation in more detail in Section 7.2.

The rest of this section is devoted to explaining the discrepancies when comparing the Bruinier-Yang conjecture with the denominators of the Igusa class polynomials. Note that the six rows which are marked with a (\*) are cases where the Bruinier-Yang conjecture is already proved by Yang, since in those cases both  $D$  and  $\tilde{D}$  are primes congruent to 1 (mod 4). The two rows with a (\*\*) in the table are not covered by the conjecture, since in those cases the real quadratic subfield has discriminant which is divisible by a power of 2. Next we remark that in all the cases which are covered by the Bruinier-Yang conjecture, that is, where  $D \equiv 1 \pmod{4}$  is prime, the numerical data confirms the conjecture and shows that the 2 quantities computed for each field match, except for the power of 2 in the examples already mentioned above and the power of 23 in row 11. We cannot explain the discrepancy in the power of 23 in row 11.

$\tilde{D}$	CM field	denominators of Igusa invariants	Bruinier-Yang formula (written multiplicatively)	Number of embeddings (written multiplicatively)
5	$\mathbb{Q}(\zeta_5)^*$	1	1	1
$2^5$	$\mathbb{Q}(\sqrt{-2 + \sqrt{2}})^{**}$	1	$(2^4)^{-1/2}(2^8)^{-3/2}$	2
13	$\mathbb{Q}(\sqrt{-13 + 2\sqrt{13}})^*$	1	1	1
$2^6 5$	$\mathbb{Q}(\sqrt{-5 + \sqrt{5}})$	1, $11^2$	$(2^2)^{3/2}11^2$	$2^2 \cdot 11^2$
$5 \cdot 13^2$	$\mathbb{Q}(\sqrt{-65 + 26\sqrt{5}})^*$	$11^2, 31^2 41^2$	$11^2 31^2 41^2$	$11^2 31^2 41^2$
29	$\mathbb{Q}(\sqrt{-29 + 2\sqrt{29}})^*$	$5^2$	$5^2$	$5^2$
$5 \cdot 17^2$	$\mathbb{Q}(\sqrt{-85 + 34\sqrt{5}})$	$71^2, 11^2 41^2 61^2$	$11^2 41^2 61^2 71^2$	$11^2 41^2 61^2 71^2$
37	$\mathbb{Q}(\sqrt{-37 + 6\sqrt{37}})^*$	$3^2 11^2$	$3^2 11^2$	$3^2 11^2$
$2^5 5^2$	$\mathbb{Q}(\sqrt{-10 + 5\sqrt{2}})^{**}$	$7^2 23^2, 7^2 17^2 23^2$	$(2^{28})^{-3/2}(2^2)^{-1}(2^{12})^{-1/2} \times (5^{32})^{1/2} 5^{14} 7^6 \times 17^4 23^4 31^2 41^2 79^2$	$2^2 7^4 17^2 23^4$
$5^2 13$	$\mathbb{Q}(\sqrt{-65 + 10\sqrt{13}})$	$3^2, 3^2 53^2$	$3^4 53^2$	$3^4 53^2$
$2^6 13$	$\mathbb{Q}(\sqrt{-13 + 3\sqrt{13}})$	$3^2 23^2, 3^2 23^2 131^2$	$(2^2)^{\frac{3}{2}} 3^4 23^2 131^2$	$2^2 3^4 23^4 131^2$
53	$\mathbb{Q}(\sqrt{-53 + 2\sqrt{53}})^*$	$17^2 29^2$	$17^2 29^2$	$17^2 29^2$
61	$\mathbb{Q}(\sqrt{-61 + 6\sqrt{61}})^*$	$3^4 5^2 41^2$	$(3^2)^2 5^2 41^2$	$3^2 5^2 41^2$

TABLE 1. Numerical data: precise descriptions of the values computed can be found in Section 7.

\* : Conjecture has been proved in this case since  $\tilde{D} \equiv 1 \pmod{4}$  is a prime

\*\* : Conjecture (as stated) does not include this case; [BY06] assumed that the real quadratic subfield has prime discriminant

Other than the power of 23, the discrepancies in the table occur in the four fields where  $\tilde{D}$  is highly divisible by 2. In those cases, negative and/or fractional powers of 2 appear in the Bruinier-Yang formula, plus other stray primes and powers in row nine. To explain that, observe that in [Yana, Yanb], Yang shows that the multiplicity is equal to

$$\frac{1}{2} \left( \text{ord}_p \frac{m^2 \tilde{D} - n^2}{4D} + 1 \right)$$

and proves under his assumptions that this value is equal to

$$\frac{1}{2} \left( \text{ord}_{\mathfrak{p}} \frac{n + m\sqrt{\tilde{D}}}{2D} + 1 \right).$$

In particular,  $\text{ord}_p \frac{m^2 \tilde{D} - n^2}{4D}$  is odd. However, these statements no longer hold for those 4 examples in the table, and this leads to the fractional exponents.

When  $D$  is also even in addition to  $\tilde{D}$  being even, Bruinier and Yang did not conjecture a formula, so the different values do not give a counterexample to the conjecture. However, in the aim of obtaining a formula for all CM-fields, we suggest a possible explanation for the differences and a possible correction. In Yang's papers, he proves that one should consider all pairs  $m, n$  such that  $\frac{m^2 \tilde{D} - n^2}{4D}$  is a positive integer divisible by  $p$ . This proof relies on the fact that  $D \equiv 1 \pmod{4}$ . Note that if one imposes the additional condition that  $8m + n \equiv 0 \pmod{16}$ , then one obtains intersection numbers 1 and  $7^4 17^2 23^4$  for the fields  $\mathbb{Q}(\sqrt{-2 + \sqrt{2}})$  and  $\mathbb{Q}(\sqrt{-10 + 5\sqrt{2}})$  respectively. Away from 2, these numbers agree with both the number of embeddings and the denominators. This suggests that when the real quadratic subfield has discriminant congruent to 0 modulo 4, additional congruence conditions on the pairs  $m, n$  are needed to correct the intersection formula.

**7.2. Powers of 2.** In four examples in the table, rows 2, 4, 9, and 11, the power of 2 in the denominator does not match the number of embeddings at the prime 2. The reason for that is cancellation of powers of 2 in the numerator and denominator of Igusa invariants. It was noted in [GL07, §6.2] that the phenomenon of cancellation could occur, especially for the prime 2. It was explained there that this is due to the fact that there are no smooth superspecial genus 2 curves in characteristic 2, despite the fact that superspecial primes are prevalent. For these four fields, the prime 2 is ramified, and so it follows from a generalization of the work of Goren [Gor97] given in [GL, Section 3] that 2 is a superspecial prime, and thus these curves have bad reduction at 2. So indeed we do find solutions to the embedding problem at 2 in those cases, and the only reason that 2 does not appear in the denominator is because of cancellation with powers of 2 in the numerator.

#### ACKNOWLEDGEMENTS

This work was started as our group project at the WIN workshop “Women In Numbers”, held at the Banff International Research Station in November 2008. We thank BIRS for hosting us and for the excellent working conditions there. We also thank the Fields Institute, PIMS, NSA, Microsoft Research, and the University of Calgary for their generous sponsorship of the conference. We thank Christophe Ritzenthaler for many detailed comments to improve the paper and the third author thanks Eyal Goren and Tonghai Yang for many discussions.



# APPENDIX A. MAGMA CODE FOR COUNTING THE NUMBER OF EMBEDDINGS

```
//Given a list of 4 rational numbers, q1, q2, q3, q4
//return the minimal positive integer N such that
//Nq1, Nq2, Nq3, Nq4 are integers
function Denom(L)

    denominators := [];
    for i := 1 to 4 do //hardcoded the length
        Append(~denominators, Denominator(L[i]));
    end for;
    return LCM(denominators);

end function;

/*****/
//Check whether the element x is in the integral span of elements
//in the basis B
function InIdeal(x, B)
    A := Matrix([Coordinates(B[1]), Coordinates(B[2]),
                  Coordinates(B[3]), Coordinates(B[4])]);
    v := Vector(Coordinates(x));
    s := Solution(A,v);

    retval := true;
    for n := 1 to 4 do
        if not IsIntegral(s[n]) then
            retval := false;
        end if;
    end for;
    return retval;

end function;

/*****/
//Return the Rosati involution of M.
//Notice this depends on the Norm of the ideal I
function Rosati(M,NI)

    return Matrix([ [ Conjugate(M[1][1]), Conjugate(M[2][1])*NI],
                    [ Conjugate(M[1][2])/NI, Conjugate(M[2][2])]]);

end function;
```

```

/*****
//Find all elements in the integral span of the basis B with
//norm = Normx and trace = Tracex
function FixedNormAndTrace(Normx, Tracex, B)

    xvals := [];
    Q := Parent(B[1]);
    isq := -Norm(Q.1);
    jsq := -Norm(Q.2);
    A := Transpose( Matrix([ Coordinates(B[1]), Coordinates(B[2]),
                             Coordinates(B[3]), Coordinates(B[4]) ]));

    denom1 := Denom(A[2]);
    denom2 := Denom(A[3]);
    denom3 := Denom(A[4]);
    x0 := Tracex/2;
    temp3 := Normx - x0^2;

    if temp3 ge 0 then
        for num3 := Ceiling(-Sqrt(Rationals()!(temp3*denom3^2/(isq*jsq)))
            to Floor(Sqrt(temp3*denom3^2/(isq*jsq))) do

            temp2 := temp3 - (num3/denom3)^2*isq*jsq;
            for num2 := Ceiling(-Sqrt(temp2*denom2^2/(-jsq)))
                to Floor(Sqrt(temp2*denom2^2/(-jsq))) do

                temp1 := temp2 - (num2/denom2)^2*(-jsq);
                for num1 := Ceiling(-Sqrt(temp1*denom1^2/(-isq)))
                    to Floor(Sqrt(temp1*denom1^2/(-isq))) do

                    x := x0 + num1/denom1*Q.1 +
                        num2/denom2*Q.2 + num3/denom3*Q.3;
                    if (Norm(x) eq Normx) and (Trace(x) eq Tracex)
                        and InIdeal(x, B) then
                        Append(~xvals, x);
                    end if;
                end for;
            end for;
        end for;
    end if;

    return xvals;
end function;

```

```

/*****/
function RemoveConjElts(solns, E, alpha0, alpha1, beta0, beta1, D)

  n := 1;
  while n le #solns do

    // Loop over automorphisms of E
    for r in FixedNormAndTrace(1, 0, E[1]) cat
      FixedNormAndTrace(1, 1, E[1]) cat
      FixedNormAndTrace(1, -1, E[1]) cat
      FixedNormAndTrace(1, 2, E[1]) cat
      FixedNormAndTrace(1, -2, E[1]) do

      // Loop over automorphisms of E'
      for s in FixedNormAndTrace(1, 0, E[3]) cat
        FixedNormAndTrace(1, 1, E[3]) cat
        FixedNormAndTrace(1, -1, E[3]) cat
        FixedNormAndTrace(1, 2, E[3]) cat
        FixedNormAndTrace(1, -2, E[3]) do

        //Calculating NormI so that we can compute Rosati involution
        I := LeftIdeal(QuaternionOrder(E[1]), E[2]);
        NormI := Norm(I);

        U := Matrix([r,0],[0,s]);
        Uinv := Matrix([[Conjugate(r), 0],[0, Conjugate(s)]]);

        //Remove embedding which is conjugate to given embedding by U
        // First check that U does not fix embedding
        if not (solns[n][1]*U eq U*solns[n][1] and
          solns[n][2]*U eq U*solns[n][2]) then

          Exclude(~solns, [U*solns[n][1]*Uinv,
            U*solns[n][2]*Uinv]);

        end if;

        //Remove embedding which is conjugate to the complex conjugate
        //of given embedding by U
        // First check that U does not fix complex conjugate of
        // embedding
        if not (solns[n][1]*U eq U*solns[n][1] and
          solns[n][2]*U eq U*Rosati(solns[n][2], NormI)) then

          size := #solns;

```

```

        Exclude(~solns, [U*solns[n][1]*Uinv,
                        U*Rosati(solns[n][2], NormI)*Uinv]);
    end if;

    //if E and E' are isomorphic then remove embedding which are
    // conjugate and have the order of E, E' switched
    if E[1] eq E[2] then

        U := Matrix([[0, r], [s, 0]]);
        Uinv := Matrix([[0, Conjugate(s)], [Conjugate(r), 0]]);

        if U*Uinv ne Matrix([[1,0],[0,1]]) or
           Uinv*U ne Matrix([[1,0],[0,1]]) then
            print "Error - Uinv incorrect!!", r, s;
        end if;

        if not (solns[n][1]*U eq U*solns[n][1] and
                solns[n][2]*U eq U*solns[n][2]) then

            size := #solns;
            Exclude(~solns, [U*solns[n][1]*Uinv,
                            U*solns[n][2]*Uinv]);

        end if;
        if not (solns[n][1]*U eq U*solns[n][1] and
                solns[n][2]*U eq U*Rosati(solns[n][2], NormI)) then
            size := #solns;
            Exclude(~solns, [U*solns[n][1]*Uinv,
                            U*Rosati(solns[n][2], NormI)*Uinv]);
        end if;
    end if;
end for;

n := n + 1;

end while;

return solns;

end function;

```

```

/*****
// find Lambda1, Lambda2 satsifying embedding conditions and such that
// entries have fixed norm
function FindSolns(E, alpha0, alpha1, beta0, beta1, D,
                  Norms12, Normt12, Normt22, Tracet22,
                  Normt11, Tracet11, s11);

    solns := [];

    R1 := QuaternionOrder(E[1]);
    R2 := QuaternionOrder(E[3]);
    I := LeftIdeal(R1, E[2]);

    // Create list of possible values in I with Norm = Norms12
    s12traces := [-Floor(Sqrt(4*Norms12))..Floor(Sqrt(4*Norms12))];
    s12vals := [];
    for T in s12traces do
        s12vals := s12vals cat FixedNormAndTrace(Norms12, T, E[2]);
    end for;

    for s12 in s12vals do

        // loop over values in R1 with Norm = Normt11 and Trace = Tracet11
        for t11 in FixedNormAndTrace(Normt11, Tracet11, E[1]) do

            // loop over values in R2 with Norm = Normt22 and Trace = Tracet22
            for t22 in FixedNormAndTrace(Normt22, Tracet22, E[3]) do

                // Create list of possible values in I with Norm = Normt12
                t12traces := [-Floor(Sqrt(4*Normt12))..Floor(Sqrt(4*Normt12))];
                t12vals := [];
                for T in t12traces do
                    t12vals := t12vals cat FixedNormAndTrace(Normt12, T, E[2]);
                end for;

                for t12 in t12vals do

                    t21 := 1/Norm(I)*(alpha1*Conjugate(s12) - Conjugate(t12));

                    //define Lambda1 = omega and Lambda2 = eta
                    omega := Matrix([[s11, s12],
                                     [Conjugate(s12)/Norm(I), D - s11]]);
                    eta := Matrix([[t11, t12], [t21, t22]]);

```

```

//check omega and eta live in correct subring
// and satisfy all of the embedding conditions
if InIdeal(s12, E[2]) and InIdeal(t12, E[2]) and
    (omega*eta eq eta*omega) and
    eta + Rosati(eta, Norm(I)) eq alpha0 + alpha1*omega and
    eta*Rosati(eta, Norm(I)) eq beta0 + beta1*omega then

    Append(~solns, [omega, eta]); //add to list of solutions
end if;
end for;
end for;
end for;
return solns;

end function;

```

```

/*****/
// Lists all possible pairs of matrices Lambda1, Lambda2 in R_{E, E'}
// such that
// Lambda1*Lambda2 = Lambda2*Lambda1
// Lambda1^2 - D*Lambda1 + 1/4*(D^2 - D) = 0
// Lambda2 + Lambda2^{\vee} = alpha0 + alpha1*Lambda1
// Lambda2*Lambda2^{\vee} = beta0 + beta1*Lambda1

```

```

function ListAllEmb(alpha0, alpha1, beta0, beta1, D, p)

```

```

    // Define constants associated to CM field
    F := QuadraticField(D);
    D := Discriminant(F);

```

```

    trw := D; //Trace(omega)
    nw := Integers()!(1/4*(D^2 - D)); //Norm(omega)

```

```

    Dtilde := 1/16*D^4*alpha1^4 + 1/2*D^3*alpha0*alpha1^3 - 1/8*D^3*alpha1^4
    - D^3*alpha1^2*beta1 + 3/2*D^2*alpha0^2*alpha1^2
    - 1/2*D^2*alpha0*alpha1^3 - 4*D^2*alpha0*alpha1*beta1
    + 1/16*D^2*alpha1^4 - 2*D^2*alpha1^2*beta0 + D^2*alpha1^2*beta1
    + 4*D^2*beta1^2 + 2*D*alpha0^3*alpha1 - 1/2*D*alpha0^2*alpha1^2
    - 4*D*alpha0^2*beta1 - 8*D*alpha0*alpha1*beta0
    + 4*D*alpha0*alpha1*beta1 - 2*D*alpha1^2*beta0 + 16*D*beta0*beta1
    - 4*D*beta1^2 + alpha0^4 - 8*alpha0^2*beta0 + 16*beta0^2;

```

```

// Give a presentation of  $B_{\{p, \infty\}}$ 
if p ne 2 then
    jsq := -p;
    isq := -1;
    while (IsSquare(FiniteField(p)!isq)) or
        (#RamifiedPrimes(QuaternionAlgebra<Rationals() | isq, jsq>)
        gt 1) do
        isq := isq - 1;
    end while;
else
    jsq := -1;
    isq := -1;
end if;

QQ := Rationals();
Q<i, j, k> := QuaternionAlgebra<QQ | isq, jsq>;
ksq := -isq*jsq;

// Orders = { O : O maximal order isomorphic to End(E) for E supersingular
// curve over  $\mathbb{F}_{p^2}$  }
// Note: if E and E' are not isomorphic, but have isomorphic endomorphism
// rings, Orders contains two different maximal orders, one is identified
// with End(E), the other with End(E')
OO := MaximalOrder(Q);
LI := LeftIdealClasses(OO);
Orders := [];
for I in LI do
    Append(~Orders, RightOrder(I));
end for;

// Ends = list of triples, one triple for each (ordered) pair (E, E')
// Let O be a maximal order which is isomorphic to End(E), I a left ideal
// of O which can be identified with Hom(E', E), and O' the right order of I
// which is identified with End(E'). Then the triple associated to (E, E')
// is (Basis(O), Basis(I), Basis(O')). The correspondence between
// (O, I, O') and (E, E') is explained more in the paper.
Ends := [];
for O in Orders do
    for I in LeftIdealClasses(O) do
        Append(~Ends, [Basis(O), Basis(I), Basis(RightOrder(I))]);
    end for;
end for;

// initialize list of solutions

```

```

solns := [];
number := 0;
//look for Lambda1, Lambda2 in R_{(E, E')} satisfying above conditions
// this is equivalent to searching for s11, t11 in 0, s12, t12 in I,
// s22, t22 in 0'. Then
// Lambda1 =
// [s11 s12]
// [s12^{\vee} s22]
// Lambda2 =
// [t11 t12]
// [t12^{\vee} t22]
for E in Ends do

    NormI := Norm(LeftIdeal(QuaternionOrder(E[1]), E[2]));

    //possible values for s11. s22 = D - s11
    s11vals := [Ceiling( (D - Sqrt(D))/2 )..Floor( (D + Sqrt(D))/2)];

    Esolns := [];

    for s11 in s11vals do

        a := s11; //remnants of old notation
        delta := -a^2 + a*trw - nw;
        m := delta;
        Tracet11 := alpha0 + alpha1*s11; //conditions from Lambda + Lambda*
        Tracet22 := alpha0 + alpha1*(D - s11);

        for n := Ceiling(-Sqrt(Max(m^2*Dtilde - 4*D, 0))) to
            Floor(Sqrt(Max(m^2*Dtilde - 4*D, 0))) do

            //parts of old notation
            Normx := 1/(2*D)*(n - (1/4*a^2*D^2*alpha1^2
            - 1/4*a*D^3*alpha1^2 + 1/16*D^4*alpha1^2 - 1/4*a^2*D*alpha1^2
            + 1/4*a*D^2*alpha1^2 - 1/8*D^3*alpha1^2
            + a^2*D*alpha1*alpha0 - a*D^2*alpha1*alpha0
            + 1/4*D^3*alpha1*alpha0 + 1/16*D^2*alpha1^2
            - 1/4*D^2*alpha1*alpha0 + a^2*alpha0^2 - a*D*alpha0^2
            + 1/4*D^2*alpha0^2 - 2*a^2*D*beta1 + 2*a*D^2*beta1
            - 1/2*D^3*beta1 - 1/4*D*alpha0^2 - 2*a*D*beta1
            + 1/2*D^2*beta1 - 4*a^2*beta0 + 4*a*D*beta0
            - D^2*beta0 - D*beta0));

            Normu := delta*(beta0 + beta1*a) - delta*Normx;

```



```

Tracexuc := beta1*delta - (D - 2*a)/delta*Normu;

Normv := delta^2*Normx + delta*(D - 2*a)*Tracexuc
        + (D - 2*a)^2*Normu;

//conditions coming from fixed n
Normt11 := Normx;
Normt12 := Normu*NormI/delta;
Normt22 := Normv/delta^2;
Norms12 := NormI*delta;

//check n can give a solution which is integral
if IsIntegral((m^2*Dtilde - n^2)/(4*D*p)) and
   IsIntegral(Normt11) and IsIntegral(Normt12) and
   IsIntegral(Normt22) then

    Esolns := Esolns cat FindSolns(E,
                                   alpha0, alpha1, beta0, beta1, D,
                                   Norms12, Normt12, Normt22, Tracet22,
                                   Normt11, Tracet11, s11);
// finds all solutions with
                                   // entries of Lambda2 having
                                   // fixed norm and fixed
                                   // trace (for some entries)
    end if;
end for;
end for;

// remove elements which are conjugate
Esolns := RemoveConjElts(Esolns, E, alpha0, alpha1, beta0, beta1, D);

if E[1] eq E[2] then
    number := number + #Esolns;
else
    number := number + #Esolns/2;
end if;
Append(~solns, Esolns);
end for;

return solns, Ends, Integers()!number;

end function;

```

## REFERENCES

- [AM93] A. O. L. Atkin and F. Morain, *Elliptic curves and primality proving*, Math. Comp. **61** (1993), no. 203, 29–68. MR **1199989** (**93m**:11136) ↑3.3
- [BBGK07] Jan H. Bruinier, José I. Burgos Gil, and Ulf Kühn, *Borcherds products and arithmetic intersection theory on Hilbert modular surfaces*, Duke Math. J. **139** (2007), no. 1, 1–88. MR **2322676** (**2008h**:11059) ↑4, 4.1
- [BY06] Jan Hendrik Bruinier and Tonghai Yang, *CM-values of Hilbert modular functions*, Invent. Math. **163** (2006), no. 2, 229–288. MR **2207018** (**2008b**:11053) ↑1, 4, 4.3, 4.4, 7.1, 7.2, 1
- [EL] Kirsten Eisenträger and Kristin Lauter, *A CRT algorithm for constructing genus 2 curves over finite fields*. SMF Séminaires et Congrès, Proceedings of Arithmetic, Geometry, and Coding Theory, AGCT-10, Marseille (2005), **21**, 161–176, [arXiv:0405305](#). ↑1, 3.3, 4
- [GHK<sup>+</sup>06] P. Gaudry, T. Houtmann, D. Kohel, C. Ritzenthaler, and A. Weng, *The 2-adic CM method for genus 2 curves with application to cryptography*, Advances in cryptology—ASIACRYPT 2006, Lecture Notes in Comput. Sci., vol. 4284, Springer, Berlin, 2006, pp. 114–129. MR **2444631** (**2009j**:94110) ↑1, 3.3
- [vdG88] 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 **930101** (**89c**:11073) ↑4, 4.3
- [Gor02] Eyal Z. Goren, *Lectures on Hilbert modular varieties and modular forms*, CRM Monograph Series, vol. 14, American Mathematical Society, Providence, RI, 2002. With the assistance of Marc-Hubert Nicole. MR **1863355** (**2003c**:11038) ↑4
- [Gor97] ———, *On certain reduction problems concerning abelian surfaces*, Manuscripta Math. **94** (1997), no. 1, 33–43. MR **1468933** (**98m**:14048) ↑1, 7.2
- [GL07] Eyal Z. Goren and Kristin E. Lauter, *Class invariants for quartic CM fields*, Ann. Inst. Fourier (Grenoble) **57** (2007), no. 2, 457–480 (English, with English and French summaries). MR **2310947** (**2008i**:11075) ↑1, 3.2, 4, 5, 6, 7.2
- [GL] ———, *Genus 2 curves with complex multiplication*, Preprint 2010, pp. 51, [arXiv:1003.4759v1](#). ↑1, 7.2
- [GZ85] Benedict H. Gross and Don B. Zagier, *On singular moduli*, J. Reine Angew. Math. **355** (1985), 191–220. MR **772491** (**86j**:11041) ↑1
- [Gru] Helen Grundman, *Hilbert Modular Variety Computations*. Preprint, 2009. ↑4.1
- [HNR09] Everett W. Howe, Enric Nart, and Christophe Ritzenthaler, *Jacobians in isogeny classes of abelian surfaces over finite fields*, Ann. Inst. Fourier **59** (2009), 239–289. ↑3.1
- [How95] Everett W. Howe, *Principally polarized ordinary abelian varieties over finite fields*, Trans. Amer. Math. Soc. **347** (1995), no. 7, 2361–2401. MR **1297531** (**96i**:11065) ↑3.1
- [Igu60] Jun-ichi Igusa, *Arithmetic Variety of Moduli for Genus Two*, Ann. Math. **72** (1960), 612–649. ↑3, 3.2
- [Igu62] ———, *On Siegel modular forms of genus two.*, Amer. J. Math. **84** (1962), 175–200. ↑3.2
- [Igu67] ———, *Modular forms and projective invariants*, Amer. J. Math. **89** (1967), 817–855. MR **0229643** (37 #5217) ↑3.2
- [KW89] Luise-Charlotte Kappe and Bette Warren, *An elementary test for the Galois group of a quartic polynomial*, Amer. Math. Monthly **96** (1989), no. 2, 133–137. MR **992075** (**90i**:12006) ↑3.1
- [KRY06] Stephen S. Kudla, Michael Rapoport, and Tonghai Yang, *Modular forms and special cycles on Shimura curves*, Annals of Mathematics Studies, vol. 161, Princeton University Press, Princeton, NJ, 2006. MR **2220359** (**2007i**:11084) ↑4, 4.2
- [Lau] Kristin Lauter, *Primes in the denominators of Igusa Class Polynomials*. Preprint 2003 [arXiv:0301240](#). ↑1, 3.2
- [Mes91] Jean-François Mestre, *Construction de courbes de genre 2 à partir de leurs modules*, Effective methods in algebraic geometry (Castiglione della Pescaia, 1990), Progr. Math., vol. 94, Birkhäuser Boston, Boston, MA, 1991, pp. 313–334 (French). MR **1106431** (**92g**:14022) ↑3.3

- [Shi98] Goro Shimura, *Abelian varieties with complex multiplication and modular functions*, Princeton Mathematical Series, vol. 46, Princeton University Press, Princeton, NJ, 1998. MR **1492449** (**99e:11076**) ↑2
- [Spa94] Anne-Monika Spallek, *Kurven vom Geschlecht 2 und ihre Anwendung in Public-Key-Kryptosystemen*, 1994. Universität Gesamthochschule Essen, Ph. D. Thesis. ↑1, 3.2, 3.2, 3.3
- [vW99] Paul van Wamelen, *Examples of genus two CM curves defined over the rationals*, Math. Comp. **68** (1999), no. 225, 307–320. MR **1609658** (**99c:11079**) ↑1, 3.2, 3.3, 4.4, 7, 7.1
- [Wen03] Annegret Weng, *Constructing hyperelliptic curves of genus 2 suitable for cryptography*, Math. Comp. **72** (2003), no. 241, 435–458 (electronic). MR **1933830** (**2003i:14029**) ↑1, 3.2, 3.3
- [Yana] Tonghai Yang, *An arithmetic intersection formula on Hilbert modular surfaces*. 2007, Preprint, to appear in *Amer. J. Math.* ↑1, 4, 4.2, 4.4, 7.1
- [Yanb] ———, *Arithmetic intersection on a Hilbert modular surface and the Faltings height*. 2007, Preprint. ↑1, 4, 4.2, 4.4, 7.1