Publications mathématiques de Besançon – 2014/2, 5-30

DENOMINATORS OF IGUSA CLASS POLYNOMIALS

by

Kristin Lauter and Bianca Viray

Abstract. — In [22], the authors proved an explicit formula for the arithmetic intersection number $(\mathrm{CM}(K).G_1)$ on the Siegel moduli space of abelian surfaces, under some assumptions on the quartic CM field K. These intersection numbers allow one to compute the denominators of Igusa class polynomials, which has important applications to the construction of genus 2 curves for use in cryptography. One of the main tools in the proof was a previous result of the authors [21] generalizing the singular moduli formula of Gross and Zagier. The current paper combines the arguments of [21, 22] and presents a direct proof of the main arithmetic intersection formula. We focus on providing a stream-lined account of the proof such that the algorithm for implementation is clear, and we give applications and examples of the formula in corner cases.

Résumé. — *Dénominateurs des polynômes des classes d'Igusa.*
Cet article donne une demonstration directe de la formule explicite du nombre d'intersection $(\mathrm{CM}(K).G_1)$ sur l'espace des modules de Siegel pour un corps K à multiplication complexe quartique. Cette formule permet de calculer, d'une manière effective, les denominateurs des polynômes des classes d'Igusa ce qui est utile pour construire des courbes de genre 2 pour la cryptographie Cette formule a ete demontree dans l'article [22], avec une forte dependance, dans la demonstration, d'une formule donnee dans [21] qui généeralise la formule de Gross et Zagier. Notre présentation ici est plus transparante et plus adaptée pour écrire un algorithme pour la calculer. Nous donnons aussi des exemples et des applications.

1. Introduction

Igusa defined a collection of invariants for genus 2 curves and proved expressions for them in terms of quotients of Siegel modular forms. For genus 2 curves with complex multiplication (CM) by a primitive quartic CM field K, these invariants lie in the Hilbert class field of the reflex field of K, and their minimal polynomials, *Igusa class polynomials*, have coefficients which are rational, not necessarily integral as is the case for Hilbert class polynomials related to invariants of elliptic curves.

Ignoring cancellation with numerators, the primes which appear in the denominators of Igusa class polynomials are those which appear in $(\mathrm{CM}(K).G_1)$, the arithmetic intersection on the Siegel moduli space of the divisor of the Siegel modular form χ_{10} with the CM points of

Mathematical subject classification (2010). — To be completed.
Keywords. — Gross-Zagier's formula, intersection number, complex multiplication, Igusa class polynomials.

The second author was partially supported by Microsoft Research and NSF grant DMS-1002933.

K. In [10], it was proved that these primes are those p for which there is a solution to an *Embedding Problem*, that is, there exists an embedding of $\mathcal{O}_K$ into $M_2(\mathbb{B}_{p,\infty})$ with certain properties. Studying this embedding problem, [10] gave a bound on the primes which can appear, and [11] gave a bound on the powers to which they can appear.
At the same time, Bruinier and Yang, using methods from Arakelov intersection theory, gave a conjectural exact formula for the factorization of the denominators under certain conditions on the ramification in the primitive quartic CM field K [1]. They assume that the discriminant of K is p^2q, where p and q are both primes congruent to 1 (mod 4). In [33, 34], Yang gave a detailed treatment of the Embedding Problem and used it, along with other techniques, to prove the conjectured intersection formula assuming the ring integers of K is generated by one element over the ring of integers of the real quadratic subfield. Yang's proof uses results of Gross-Keating, and then computes local densities by evaluating certain local integrals over the quaternions.
In practice, very few primitive quartic CM fields have ramification of such restricted form. In [16], the authors studied all 13 quartic cyclic CM fields in van Wamelen's tables of CM genus 2 curves defined over $\mathbb{Q}$, compared denominators with the number of solutions to the Embedding Problem and Bruinier and Yang's formula, and found that the assumptions on the ramification of K are necessary for the Bruinier-Yang formula to hold. For applications to the computation of genus 2 curves for cryptography, it is important to have a precise formula for the denominators of Igusa class polynomials which holds for general primitive quartic CM fields.
An arithmetic intersection formula for $(\mathrm{CM}(K).G_1)$ was proved in [22], extending the conjecture of Bruinier and Yang to general primitive quartic CM fields K with almost no assumptions on K. Furthermore, for *all* primitive quartic CM fields K, the formula proved in [22] gives an upper bound on prime powers in the denominator which is very accurate for the purpose of efficiently computing Igusa class polynomials. This solves the problem of estimating or clearing denominators of Igusa class polynomials from a practical point of view, for any primitive quartic CM field K, and gives strong motivation for an effective algorithm for computing the formula in practice.
One of the main tools in [22] is earlier work of the two authors that generalizes the singular moduli formula of Gross and Zagier [15]. As [22] cites only the results of [21], the algorithmic nature of the proof of the formula for $(\mathrm{CM}(K).G_1)$ may not be readily apparent.
The present paper combines the results of [21, 22] and presents a direct proof of the main arithmetic intersection formula. The proof is more explicit than what is given in those two papers, but relies on the same building blocks. Here we revisit those ideas, and include all details necessary for implementing an algorithm to compute the formula. The main new content is in Section 5, where the direct proof is presented. We focus on providing a streamlined account of the proof such that the algorithm for implementation is clear, and we give applications and examples of the formula in corner cases in Sections 8, 9.
The statement of the theorem and an outline of the proof is given in Section 2, and a summary pulling all the steps of the proof together is given in Section 7. The strategy of our proof is as follows: to study and characterize solutions to the Embedding Problem, we first fix the embedding of the real quadratic subfield, as Yang did in [33, 34]. Then through a series of calculations explained in Section 2 it becomes possible to see that solutions can be parameterized by pairs of endomorphisms of a supersingular elliptic curve E, $x, u \in \mathrm{End}(E)$

with a fixed norm and trace. This in turn is related to the counting problem studied by Gross and Zagier [15] in their formula for the factorization of differences of singular moduli: counting simultaneous embeddings of maximal orders from two distinct imaginary quadratic fields, $\mathbb{Q}(\sqrt{d_1})$ and $\mathbb{Q}(\sqrt{d_2})$, into a maximal order in the quaternion algebra $\mathbb{B}_{p,\infty}$.
To solve this problem Gross and Zagier gave an explicit description of all maximal orders in $\mathbb{B}_{p,\infty}$ with an optimal embedding of the maximal order in $\mathbb{Q}(\sqrt{-p})$, for p prime. In follow-up work, Dorman [5] extended their description to work for maximal orders in $\mathbb{B}_{p,\infty}$ with an optimal embedding of a *maximal* order in an imaginary quadratic field that is unramified at 2. To solve the Embedding Problem, explicit descriptions of maximal orders in the quaternion algebra with an optimal embedding of arbitrary quadratic orders are needed. The fact that the quadratic orders which arise may have even discriminant makes the genus theory required for our formula considerably more difficult. The explicit descriptions of maximal orders in the quaternion algebra were given in [21], where a broad generalization of Gross and Zagier's theorem on singular moduli was proved as a consequence. In Section 4 we repeat the definitions and statements about the maximal orders in $\mathbb{B}_{p,\infty}$ with an optimal embedding of a non-maximal quadratic order without proof, since the notation is needed for the proof of the main theorem.
A solution to the embedding problem is actually given by a pair of supersingular elliptic curves E_1 and E_2 modulo p, an embedding of the ring of integers of the real quadratic subfield of K into $\mathrm{End}(E_1 \times E_2)$, along with a pair of endomorphisms $x \in \mathrm{End}(E_1)$ and $z \in \mathrm{End}(E_2)$ and an isogeny y between them satisfying certain properties. In order to convert pairs of solutions $x, u \in \mathrm{End}(E_1)$ into an actual solution to the Embedding Problem, there is another counting problem to be solved, namely counting ideals with certain properties in a quaternion algebra. The counting formula which solves this problem is stated in Theorem 6.1.1, and was proved in [22].
Finally, in §8, we explain how this intersection number gives a sharp bound for the denominators of Igusa class polynomials, and we give several concrete examples in Section 9. These examples illustrate various complexities that arise in the formulae for corner cases.

2. Main Theorem

Let K be a primitive quartic CM field, let F denote its real quadratic subfield, and let D denote the discriminant of $\mathcal{O}_F$. We assume that $\mathcal{O}_K$ is generated over $\mathcal{O}_F$ by one element, say η, so $\mathcal{O}_K = \mathcal{O}_F[\eta]$. If this assumption does not hold, then Theorem 2.3 in [22] gives an upper bound on the intersection number. Let $\tilde{D}$ denote $\mathrm{N}_{F/\mathbb{Q}}\left(\mathrm{Disc}_{K/F}(\mathcal{O}_K)\right)$ and let $\alpha_0, \alpha_1, \beta_0, \beta_1 \in \mathbb{Z}$ be such that

$$\mathrm{Tr}_{K/F}(\eta) = \alpha_0 + \alpha_1 \frac{D+\sqrt{D}}{2}, \quad \mathrm{N}_{K/F}(\eta) = \beta_0 + \beta_1 \frac{D+\sqrt{D}}{2}.$$

For any positive integer δ such that $D - 4\delta = \square$, we define

$$c_K(\delta) := \delta\left(\alpha_0^2 + \alpha_0\alpha_1 D + \alpha_1^2 \frac{D^2-D}{4} - 4\beta_0 - 2\beta_1 D\right),$$

and let $a := \frac{1}{2}\left(D - \sqrt{D-4\delta}\right)$, where we take the non-negative square root. Then for any integer n such that $2D \mid (n + c_K(\delta))$, we define

$$\begin{aligned}
d_u(n) &= (\alpha_1\delta)^2 + 4\frac{(n+c_K(\delta))\delta}{2D},\\
t_x &= \alpha_0 + a\alpha_1,\\
d_x(n) &= (\alpha_0 + a\alpha_1)^2 - 4\left(\beta_0 + a\beta_1 + \frac{(n+c_K(\delta))}{2D}\right),\\
t_{xu^\vee}(n) &= \beta_1\delta + (D-2a)\frac{(n+c_K(\delta))}{2D}\\
s'(n) &= t_x\alpha_1\delta - 2t_{xu^\vee}(n),\\
t_w(n) &= \alpha_0 + (D-a)\alpha_1,\\
n_w(n) &= \beta_0 + (D-a)\beta_1 + \frac{(n+c_K(\delta))}{2D}.
\end{aligned}$$

Our main theorem gives a counting formula for an arithmetic intersection number, which is defined as a weighted sum of lengths of local rings at points in the intersection as follows:

$$\frac{(\mathrm{CM}(K).G_1)_\ell}{\log \ell} = \sum_{P \in (\mathrm{CM}(K)\cap G_1)(\overline{\mathbb{F}}_\ell)} \frac{1}{\#\operatorname{Aut}(P)} \cdot \operatorname{length} \widetilde{\mathcal{O}}_{G_1\cap \mathrm{CM}(K),P} \tag{2.1}$$

where $\widetilde{\mathcal{O}}_{G_1\cap \mathrm{CM}(K),P}$ is the local ring of $G_1 \cap \mathrm{CM}(K)$ at P.
Our counting formula is stated in terms of the quantities $M(\delta, n, f)$ and $\mathfrak{I}(\delta, n, f)$. The precise definition of $M(\delta, n, f)$ is given in Definition 5.4.1: it is a weighted ideal count of certain invertible ideals of norm N in the imaginary quadratic order of discriminant d, where N and d are determined by (δ, n, f), and the sum is weighted by multiplicity and a factor which determines the genus class.
The definition of $\mathfrak{I}(\delta, n, f)$ is given in Theorem 6.1.1, and it counts the number of left integral ideals of a maximal order in a quaternion algebra with special properties defined by (δ, n, f). Let

$$B(\delta, n, f) = \mathfrak{I}(\delta, n, f) M(\delta, n, f).$$

Theorem 2.0.1. — *Let ℓ be a prime different from 2. If $\ell\delta$ for any positive integer δ of the form $\frac{D-\square}{4}$, then*

$$\frac{(\mathrm{CM}(K).G_1)_\ell}{\log \ell} = \sum_{\substack{\delta\in\mathbb{Z}_{>0}\\ \delta=\frac{D-\square}{4}}} C_\delta \sum_{\substack{n\in\mathbb{Z}\\ \frac{\delta^2\widetilde{D}-n^2}{4D}\in\ell\mathbb{Z}_{>0}\\ 2D\mid(n+c_K(\delta))}} \varepsilon(n) \sum_{\substack{f\in\mathbb{Z}_{>0}\\ \frac{\delta^2\widetilde{D}-n^2}{4Df^2}\in\ell\mathbb{Z}_{>0}}} B(\delta, n, f),$$

otherwise,

$$\frac{(\mathrm{CM}(K).G_1)_\ell}{\log \ell} \leq 2 \sum_{\substack{\delta \in \mathbb{Z}_{>0} \\ \delta = \frac{D-\square}{4}}} C_\delta \sum_{\substack{n \in \mathbb{Z} \\ \frac{\delta^2 \widetilde{D} - n^2}{4D} \in \ell\mathbb{Z}_{>0} \\ 2D \mid (n + c_K(\delta))}} \varepsilon(n) \sum_{\substack{f \in \mathbb{Z}_{>0} \\ \frac{\delta^2 \widetilde{D} - n^2}{4Df^2} \in \ell\mathbb{Z}_{>0}}} B(\delta, n, f),$$

where $C_\delta = \begin{cases} \frac{1}{2} & \text{if } 4\delta = D \\ 1 & \text{otherwise,} \end{cases}$ $\varepsilon(n) = \begin{cases} 0 & \text{if } v_\ell(d_u(n)) > 1 \text{ and } v_\ell(d_x(n)) > 1 \\ 1 & \text{otherwise.} \end{cases}$

Remark 2.0.2. — *If $\mathcal{O}_K$ is not generated by a single element over $\mathcal{O}_F$, then the proof instead gives an upper bound. For any integral element $\eta \in K \setminus F$, let $\widetilde{D}_\eta := \mathrm{N}_{F/\mathbb{Q}}(\mathrm{Disc}_{K/F}(\eta))$ and let*

$$c_\eta(\delta) := \delta \left(\alpha_0^2 + \alpha_0 \alpha_1 D + \alpha_1^2 \frac{D^2 - D}{4} - 4\beta_0 - 2\beta_1 D \right),$$

where α_i and β_i are defined in terms of η as above. Then

$$\frac{(\mathrm{CM}(K).G_1)_\ell}{\log \ell} \leq \sum_{\substack{\delta \in \mathbb{Z}_{>0} \\ \delta = \frac{D-\square}{4}}} 2C_\delta \cdot \min_{\substack{\eta \in \mathcal{O}_K \setminus \mathcal{O}_F \\ \gcd([\mathcal{O}_K : \mathcal{O}_F[\eta]], \ell\delta) = 1}} \left(\sum_{\substack{n \in \mathbb{Z} \\ \frac{\delta^2 \widetilde{D}_\eta - n^2}{4D} \in \ell\mathbb{Z}_{>0} \\ 2D \mid (n + c_\eta(\delta))}} \varepsilon(n) \sum_{\substack{f \in \mathbb{Z}_{>0} \\ \frac{\delta^2 \widetilde{D}_\eta - n^2}{4Df^2} \in \ell\mathbb{Z}_{>0}}} B(\delta, n, f) \right),$$

where the factor of 2 can be removed if $\ell\delta$.

Proof of Main Theorem. — G_1 parametrizes products of elliptic curves with the product polarization, so a point $P \in (G_1 \cap \mathrm{CM}(K))(\overline{\mathbb{F}}_\ell)$ corresponds to an isomorphism class of a pair of elliptic curves E_1, E_2, and an embedding $\iota \colon \mathcal{O}_K \hookrightarrow \mathrm{End}(E_1 \times E_2)$. In addition, the embedding must be such that the action of complex conjugation agrees with the Rosati involution induced by the product polarization, i.e.,

$$\text{if } \iota(\alpha) = \begin{pmatrix} g_{1,1} & g_{1,2} \\ g_{2,1} & g_{2,2} \end{pmatrix} \text{ where } g_{i,j} \in \mathrm{Hom}(E_j, E_i), \text{ then } \iota(\overline{\alpha}) = \begin{pmatrix} g_{1,1}^\vee & g_{2,1}^\vee \\ g_{1,2}^\vee & g_{2,2}^\vee \end{pmatrix},$$

where $g^\vee$ denotes the dual isogeny of g (see [10, p. 462]).
Two tuples $(E_1, E_2, \iota \colon \mathcal{O}_K \hookrightarrow \mathrm{End}(E_1 \times E_2))$ and $(E_1', E_2', \iota' \colon \mathcal{O}_K \hookrightarrow \mathrm{End}(E_1' \times E_2'))$ are isomorphic if there exists an isomorphism $\psi \colon E_1 \times E_2 \xrightarrow{\sim} E_1' \times E_2'$ such that

$$\psi \circ \iota(\alpha) = \iota'(\alpha) \circ \psi \ \ \forall \alpha \in \mathcal{O}_K, \ \text{ and } \ \psi \circ g^\vee \circ \psi^{-1} = \left(\psi \circ g \circ \psi^{-1} \right)^\vee \ \ \forall g \in \mathrm{End}(E_1 \times E_2).$$

We study the isomorphism classes by first fixing elliptic curves in each isomorphism class and then ranging over isomorphism classes of embeddings. When $E_i = E_i'$, then the tuples are isomorphic if there exists a $\psi \in \mathrm{Aut}(E_1 \times E_2)$ such that $\psi \circ \iota(\alpha) = \iota'(\alpha) \circ \psi$ for all $\alpha \in \mathcal{O}_K$ and $\psi\psi^\vee = 1$; this last condition is equivalent to the condition on the Rosati involution that is described at the beginning of the paragraph.
Given two elliptic curves E_1, E_2 over $\overline{\mathbb{F}}_\ell$, the deformation space of E_1, E_2 is $\mathbb{W}[[t_1, t_2]]$, where $\mathbb{W}$ denotes the Witt ring of $\overline{\mathbb{F}}_\ell$. Let $\mathbb{E}_1, \mathbb{E}_2$ be the universal curves over this space and let $I_{E_1, E_2, \iota} \subset$

$\mathbb{W}[[t_1,t_2]]$ denote the minimal ideal such that there exists an $\widetilde{\iota}\colon \mathcal{O}_K \hookrightarrow \mathrm{End}_{\mathbb{W}[[t_1,t_2]]/I_{E_1,E_2,\iota}}$ that agrees with ι after reducing modulo the maximal ideal of $\mathbb{W}[[t_1,t_2]]$. Then we have

$$\text{length } \widetilde{\mathcal{O}}_{G_1\cap \mathrm{CM}(K),P} = \text{length } \mathbb{W}[[t_1,t_2]]/I_{E_1,E_2,\iota},$$

for any point $P \leftrightarrow (E_1,E_2,\iota) \in (G_1 \cap \mathrm{CM}(K))\,(\overline{\mathbb{F}}_\ell)$.
Thus, (2.1) can be rewritten as

$$\frac{(\mathrm{CM}(K).G_1)_\ell}{\log \ell} = \sum_{\substack{\text{iso. classes } E_1,E_2\\ \iota\colon \mathcal{O}_K\hookrightarrow \mathrm{End}(E_1\times E_2)\\ \text{as above}}} \frac{1}{\#\,\mathrm{Aut}(E_1,E_2,\iota)} \cdot \text{length } \frac{\mathbb{W}[[t_1,t_2]]}{I_{E_1,E_2,\iota}}, \tag{2.2}$$

where $\mathrm{Aut}(E_1,E_2,\iota) := \{\sigma \in \mathrm{Aut}(E_1\times E_2) : \sigma\iota(\alpha)\sigma^\vee = \iota(\alpha)\ \forall \alpha \in \mathcal{O}_K \text{ and } \sigma\sigma^\vee = 1\}$. The condition that $\sigma\sigma^\vee = 1$ ensures that σ preserves the product polarization.
Since $\mathcal{O}_K = \mathcal{O}_F[\eta]$, giving an embedding $\iota \hookrightarrow \mathrm{End}(E_1\times E_2)$ is equivalent to giving two elements $\Lambda_1,\Lambda_2 \in \mathrm{End}(E_1\times E_2)$ such that

$$\begin{aligned} \Lambda_1\Lambda_2 &= \Lambda_2\Lambda_1,\\ \Lambda_2 + \Lambda_2^\vee &= \alpha_0 + \alpha_1\Lambda_1,\\ \Lambda_2\Lambda_2^\vee &= \beta_0 + \beta_1\Lambda_1, \text{ and}\\ \Lambda_1^2 - D\Lambda_1 + \frac{D^2-D}{4} &= 0. \end{aligned}$$

The equivalence is obtained by letting $\Lambda_1 = \iota\left(\frac{D+\sqrt{D}}{2}\right), \Lambda_2 = \iota(\eta)$. This equivalence is a more precise reformulation of the Embedding Problem than the version used in [10, p. 463], where the elements from $\mathcal{O}_K$ being embedded were of a simpler form and were not necessarily generators of $\mathcal{O}_K$. By representing elements in $\mathrm{End}(E_1\times E_2)$ as 2×2 matrices $(g_{i,j})$ where $g_{i,j} \in \mathrm{End}(E_j,E_i)$ and expanding the above relations, we see that

$$\Lambda_1 = \begin{pmatrix} a & b\\ b^\vee & D-a\end{pmatrix}, \quad \Lambda_2 = \begin{pmatrix} x & y\\ \alpha_1 b^\vee - y^\vee & z\end{pmatrix},$$

where $a\in\mathbb{Z},\ b,y \in \mathrm{Hom}(E_2,E_1),\ x\in\mathrm{End}(E_1)$, and $z\in\mathrm{End}(E_2)$ satisfy

$$\delta := \mathrm{N}(b) = \frac{D-(D-2a)^2}{4}, \tag{2.3}$$

$$\mathrm{Tr}(x) = \alpha_0 + a\alpha_1, \tag{2.4}$$

$$\mathrm{Tr}(z) = \alpha_0 + (D-a)\alpha_1, \tag{2.5}$$

$$\mathrm{Tr}(yb^\vee) = \mathrm{Tr}(y^\vee b) = \mathrm{N}(b)\alpha_1, \tag{2.6}$$

$$\mathrm{N}(x) + \mathrm{N}(y) = \beta_0 + a\beta_1, \tag{2.7}$$

$$\mathrm{N}(z) + \mathrm{N}(y) = \beta_0 + (D-a)\beta_1, \tag{2.8}$$

$$\beta_1 b = \alpha_1 xb - xy + yz^\vee \tag{2.9}$$

$$bz = xb + (D-2a)y \tag{2.10}$$

After possibly conjugating Λ_1, Λ_2 by $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and interchanging E_1, E_2, we may assume that $2a \leq D$. Then a is uniquely determined by δ. Thus for a fixed δ, the embedding ι is determined by a tuple (x, y, b, z) satisfying the above relations.
Motivated by the definition of isomorphism of triples (E_1, E_2, ι) given above, we say that such two tuples $(x, y, b, z), (x', y', b', z')$ are isomorphic if

$$x\phi_1 = \phi_1 x',\ b\phi_2 = \phi_1 b',\ y\phi_2 = \phi_1 y',\ z\phi_2 = \phi_2 z', \quad \text{for some } \phi_i \in \mathrm{Aut}(E_i).$$

In particular,

$$\mathrm{Aut}(x, y, b, z) := \{\phi_i \in \mathrm{Aut}(E_i) : x\phi_1 = \phi_1 x,\ b\phi_2 = \phi_1 b,\ y\phi_2 = \phi_1 y,\ z\phi_2 = \phi_2 z\}.$$

If $4\delta \neq D$, then (x, y, b, z) is isomorphic to (x', y', b', z') if and only if the corresponding embeddings are isomorphic and $\#\,\mathrm{Aut}(x, y, b, z) = \#\,\mathrm{Aut}(E_1, E_2, \iota)$.
If $4\delta = D$, then the situation is more complicated. If $E_1 \neq E_2$, then (x, y, b, z) and $(z, y^\vee, b^\vee, x)$ correspond to the same embedding, although we do not say that they are isomorphic as tuples. If $E_1 = E_2$, then for each tuple (x, y, b, z) we have two possibilities. Either there exists an (x', y', b', z') that is *not* isomorphic to (x, y, b, z) but corresponds to an isomorphic embedding, or $2\#\,\mathrm{Aut}(x, y, b, z) = \#\,\mathrm{Aut}(E_1, E_2, \iota)$, where ι is the corresponding embedding. In either case, we see that the number of isomorphism classes of tuples (x, y, b, z) weighted by $\frac{1}{\#\,\mathrm{Aut}}$ is double the number of embeddings also weighted by $\frac{1}{\#\,\mathrm{Aut}}$. This discussion shows that (2.2) can be rewritten in terms of tuples (x, y, b, z), namely

$$\frac{(\mathrm{CM}(K).G_1)_\ell}{\log \ell} = \sum_{\substack{\delta \in \mathbb{Z}_{>0} \\ \delta = \frac{D-\square}{4}}} C_\delta \sum_{E_1} \sum_{E_2} \sum_{\substack{x,y,b,z \\ \text{up to iso. as above}}} \frac{1}{\#\,\mathrm{Aut}(x, y, b, z)} \mathrm{length}\ \frac{\mathbb{W}[[t_1, t_2]]}{I_{x,y,b,z}}, \tag{2.11}$$

where $C_\delta = \frac{1}{2}$ if $4\delta = D$ and 1 otherwise, and where $I_{x,y,b,z} \subseteq \mathbb{W}[[t_1, t_2]]$ is the minimal ideal such that there exists

$$\widetilde{x} \in \mathrm{End}_{\mathbb{W}[[t_1,t_2]]/I_{x,y,b,z}}(\mathbb{E}_1),\ \widetilde{y}, \widetilde{b} \in \mathrm{Hom}_{\mathbb{W}[[t_1,t_2]]/I_{x,y,b,z}}(\mathbb{E}_2, \mathbb{E}_1),\ \widetilde{z} \in \mathrm{End}_{\mathbb{W}[[t_1,t_2]]/I_{x,y,b,z}}(\mathbb{E}_2)$$

that reduce to x, y, b, z respectively, modulo the maximal ideal of $\mathbb{W}[[t_1, t_2]]$.
Fix δ, E_1, E_2, and assume that there exists a tuple (x, y, b, z) as above. Then, there exists $x, u := yb^\vee \in \mathrm{End}(E_1)$ satisfying

$$\mathrm{Tr}(x) = \alpha_0 + a\alpha_1, \tag{2.12}$$

$$\mathrm{Tr}(u) = \delta\alpha_1, \tag{2.13}$$

$$\delta\,\mathrm{N}(x) + \mathrm{N}(u) = \delta\,(\beta_0 + \beta_1 a)\,, \tag{2.14}$$

$$(D - 2a)\,\mathrm{N}\,(u) + \delta\,\mathrm{Tr}\,(xu^\vee) = \beta_1\delta^2, \tag{2.15}$$

where $a \in \mathbb{Z}$ is such that $a \leq D/2$ and $(D - 2a)^2 = D - 4\delta$. This is easy to check using the relations (2.4)–(2.10) on (x, y, b, z).
We will complete the proof of the theorem in two steps in sections 5 and 6, respectively,

1. Calculate the number of (E_1, x, u) satisfying (2.12)–(2.15)(§5), and
2. For a fixed (E_1, x, u) determine the number of (E_2, y, b, z) such that $u = yb^\vee$ and (x, y, b, z), satisfy (2.4)–(2.10) (§6).

As it is not necessarily obvious how the arguments in sections 2 through 6 come together, we summarize the argument in §7.
In the next two sections we present the necessary background to continue with these steps of the proof. These notation and statements are taken from [21] and the proofs are omitted.

3. Background: quadratic imaginary orders

This section is taken from Section 5 of [21].
Let $\mathcal{O}$ be an order in a quadratic imaginary field, and let d be the discriminant of $\mathcal{O}$. Let $\mathfrak{a}$ be an ideal in $\mathcal{O}$. If $\mathcal{O}$ is not maximal, then we can not necessarily write $\mathfrak{a}$ uniquely as a product of primes. However, we can always write $\mathfrak{a}$ uniquely as a product of primary ideals where no two ideals in the factorization are supported at the same prime. Precisely, for any prime $\mathfrak{p}$, define $\mathfrak{a}_\mathfrak{p} := \mathcal{O} \cap \mathfrak{a}\mathcal{O}_\mathfrak{p}$. Then $\mathfrak{a} = \bigcap_\mathfrak{p} \mathfrak{a}_\mathfrak{p}$, and since for any 2 distinct primes $\mathfrak{p}, \mathfrak{q}$, $\mathfrak{a}_\mathfrak{p}$ and $\mathfrak{a}_\mathfrak{q}$ are co-maximal, we have that

$$\mathfrak{a} = \prod_\mathfrak{p} \mathfrak{a}_\mathfrak{p}.$$

(See [24, Prop 12.3] for more details.) If there is a unique prime $\mathfrak{p} \subseteq \mathcal{O}$ lying over p, then we will often write $\mathfrak{a}_p$ instead of $\mathfrak{a}_\mathfrak{p}$.
We will often be concerned with the special case where $\mathfrak{a} = \mathfrak{D} := \sqrt{d}\mathcal{O}$. If $p|d$ is odd, then for $a, b \in \mathcal{O}$, the difference $a - b \in \mathfrak{D}_p$ if and only if $\mathrm{Tr}(a) \equiv \mathrm{Tr}(b) \pmod{p^{v_p(d)}}$. If $p = 2|d$, then $a - b \in \mathfrak{D}_2$ if and only if $a_0 \equiv b_0 \pmod{2^{v_2(d)-1}}$ and $a_1 \equiv b_1 \pmod 2$, where $a = a_0 + a_1\frac{d+\sqrt{d}}{2}$ and $b = b_0 + b_1\frac{d+\sqrt{d}}{2}$.

3.1. The Picard group. — The Picard group of $\mathcal{O}$, denoted $\mathrm{Pic}(\mathcal{O})$, is the group of invertible fractional ideals modulo fractional principal ideals. It is isomorphic to the form class group $C(d)$, the group of classes of primitive positive definite forms of discriminant d [4, §7]. We will use this isomorphism to determine whether there exists an ideal in $2\,\mathrm{Pic}(\mathcal{O})$ of a certain norm. For more information on genus theory, i.e., the study of $\mathrm{Pic}(\mathcal{O})/2\,\mathrm{Pic}(\mathcal{O})$, see [4].
Let $p_1, \ldots, p_j$ be the distinct odd primes dividing d. Define

$$k = \begin{cases} j & \text{if } d \equiv 1 \pmod 4 \text{ or } d \equiv 4 \pmod{16}, \\ j+1 & \text{if } d \equiv 8, 12 \pmod{16} \text{ or } d \equiv 16 \pmod{32}, \\ j+2 & \text{if } d \equiv 0 \pmod{32}. \end{cases}$$

For $i = 1, \ldots, j$, we define $\chi_{p_i}(a) := \left(\frac{a}{p_i}\right)$ for a coprime to p_i. For a odd, we also define $\chi_{-4}(a) := (-1)^{\frac{a-1}{2}}$, $\chi_8(a) := (-1)^{\frac{a^2-1}{8}}$. Then we define $\Psi\colon (\mathbb{Z}/d\mathbb{Z})^\times \to \{\pm 1\}^k$ as follows.

$$\Psi = \begin{cases} (\chi_{p_1}, \ldots, \chi_{p_j}) & \text{if } d \equiv 1 \pmod 4 \text{ or } d \equiv 4 \pmod{16}, \\ (\chi_{p_1}, \ldots, \chi_{p_j}, \chi_{-4}) & \text{if } d \equiv 12 \pmod{16} \text{ or } d \equiv 16 \pmod{32}, \\ (\chi_{p_1}, \ldots, \chi_{p_j}, \chi_8) & \text{if } d \equiv 8 \pmod{32}, \\ (\chi_{p_1}, \ldots, \chi_{p_j}, \chi_{-4}\chi_8) & \text{if } d \equiv 24 \pmod{32}, \\ (\chi_{p_1}, \ldots, \chi_{p_j}, \chi_{-4}, \chi_8) & \text{if } d \equiv 0 \pmod{32}. \end{cases}$$

For a prime p that divides d, but does not divide the conductor f of $\mathcal{O}$, we define

$$\Psi_p = \begin{cases} \chi_{p_i} & \text{if } p = p_i, \\ \chi_{-4} & \text{if } p = 2 \text{ and } d \equiv 12 \pmod{16}, \\ \chi_8 & \text{if } p = 2 \text{ and } d \equiv 8 \pmod{32}, \\ \chi_{-4} \cdot \chi_8 & \text{if } p = 2 \text{ and } d \equiv 24 \pmod{32}. \end{cases}$$

Let $\widehat{\Psi}_p$ be the projection of Ψ on the components that are complementary to the one that appears in Ψ_p.
If pf, then for n relatively prime to d one may check that $\Psi_p = (d, n)_p$ where $(d, n)_p$ denotes the Hilbert symbol at p. We may use this equality to extend Ψ to $(\mathbb{Z}/f\mathbb{Z})^\times$, by defining $\Psi_p(n) := (d, n)_p$.
This map Ψ can be used to test when an ideal $\mathfrak{a}$ is a square in the Picard group.

Theorem 3.1.1 **([4]*§§3&7).** — *For any positive integer m prime to the conductor f of $\mathcal{O}_d$, there exists an invertible ideal $\mathfrak{a}$ such that $\mathrm{N}(\mathfrak{a}) = m$ and $[\mathfrak{a}] \in 2\operatorname{Pic}(\mathcal{O}_d)$ if and only if $m \in \ker \Psi$.*

From this theorem, we can easily obtain the following corollary.

Corollary 3.1.2. — *Let ℓ be a prime that divides d, but does not divide the conductor f. Let $\mathfrak{a}$ be an invertible integral ideal that is prime to the conductor. Then $[\mathfrak{a}] \in 2\operatorname{Pic}(\mathcal{O})$ if and only if $\mathrm{N}(\mathfrak{a}) \in \ker \widehat{\Psi}_\ell$.*

Unfortunately, the map Ψ cannot be extended to all integers while still retaining the properties described in Theorem 3.1.1 and Corollary 3.1.2. This is because it is possible to have two invertible ideals $\mathfrak{a}, \mathfrak{b} \subseteq \mathcal{O}_d$ with the same norm, such that $\mathfrak{a}\mathfrak{b}^{-1} \notin 2\operatorname{Pic}(\mathcal{O}_d)$. This can only occur when the ideals are not prime to f.
Let $\mathfrak{a}$ be an integral invertible ideal that is supported at a single prime p that divides the conductor, i.e. $\mathfrak{a}_\mathfrak{q} = \langle 1 \rangle$ for all $\mathfrak{q}p$. Let $\alpha \in \mathcal{O}$ be a generator for $\mathfrak{a}\mathcal{O}_p$ such that $\gcd(\mathrm{N}(\alpha), f)$ is supported only at p. Then $\mathfrak{a} \sim \widetilde{\mathfrak{a}}$ in $\operatorname{Pic}(\mathcal{O})$, where

$$\widetilde{\mathfrak{a}} := \mathcal{O}_p \cap \bigcap_{\mathfrak{q}p} (\alpha \mathcal{O}_\mathfrak{q}),$$

and $\mathrm{N}(\widetilde{\mathfrak{a}})$ is coprime to the conductor. Thus, the genus of $\mathfrak{a}$ is equal to $\Psi(\mathrm{N}(\widetilde{\mathfrak{a}}))$. Since every ideal can be factored uniquely into comaximal primary ideals, this gives a method of computing the genus class of any ideal.

4. Parametrizing endomorphism rings of supersingular elliptic curves

This section is taken from Section 6 of [21] with proofs omitted.
Let ℓ be a fixed prime and let $\mathcal{O}$ be a quadratic imaginary order of discriminant d such that $\ell f := \mathrm{cond}(d)$. We assume that ℓ is not split in $\mathcal{O}$. Let $\mathbb{W}$ be the ring of integers in $\mathbb{Q}_\ell^{\mathrm{unr}}(\sqrt{d})$, and write π for the uniformizer. By the theory of complex multiplication [19, §10.3], the isomorphism classes of elliptic curves that have CM by $\mathcal{O}$ are in bijection with $\operatorname{Pic}(\mathcal{O})$, and every elliptic curve E with CM by $\mathcal{O}$ has a model defined over $\mathbb{W}$. Moreover, by [25, Cor. 1], we may assume that E has good reduction.

Fix a presentation $\mathbb{B}_{\ell,\infty}$ of the quaternion algebra ramified at ℓ and ∞, and fix an embedding $L := \mathrm{Frac}(\mathcal{O}) \hookrightarrow \mathbb{B}_{\ell,\infty}$. The goal of this section is to define, for every $[\mathfrak{a}] \in \mathrm{Pic}(\mathcal{O})$, a maximal order $R(\mathfrak{a}) \subset \mathbb{B}_{\ell,\infty}$ such that

1. $R(\mathfrak{a}) \cap L = \mathcal{O}$,

2. $R(\mathfrak{a})$, together with the optimal embedding $\mathcal{O} \hookrightarrow R(\mathfrak{a})$ is isomorphic to the embedding $\mathrm{End}(E(\mathfrak{a})) \hookrightarrow \mathrm{End}(E(\mathfrak{a}) \bmod \pi)$, where $E(\mathfrak{a})$ is the elliptic curve with CM by $\mathcal{O}$ that corresponds to $\mathfrak{a}$, and

3. $\mathfrak{b}^{-1}R(\mathfrak{a})\mathfrak{b} = R(\mathfrak{a}\mathfrak{b})$.

Our construction of these maximal orders $R(\mathfrak{a})$ generalizes the work of Gross-Zagier [15] and Dorman [5], where they defined maximal orders with these properties under the assumption that $-d$ is prime [15] or d is squarefree [5]. We give the statements and definitions for arbitrary discriminants d and include the ramified case; for proofs we refer you to [21, §6].
Note that Goren and the first author have given a different generalization of Dorman's work [12] to higher dimensions, which works for CM fields K, characterizing superspecial orders in a quaternion algebra over the totally real field K^+ with an optimal embedding of $\mathcal{O}_{K^+}$. That work also corrects the proofs of [5], but in a slightly different way than we do here, and does not handle the ramified case or non-maximal orders.

4.0.1. *Outline.* — In §4.1, we give an explicit presentation of $\mathbb{B}_{\ell,\infty}$ that we will use throughout. The construction of the maximal orders $R(\mathfrak{a})$ depends on whether ℓ is inert (§4.2) or ramified (§4.3) in $\mathcal{O}$.

4.1. Representations of quaternion algebra. — Given a fixed embedding $\iota\colon L \hookrightarrow \mathbb{B}_{\ell,\infty}$, the quaternion algebra $\mathbb{B}_{\ell,\infty}$ can be written uniquely as $\iota(L) \oplus \iota(L)j$, where $j \in \mathbb{B}_{\ell,\infty}$ is such that $j\iota(\alpha)j^{-1} = \iota(\overline{\alpha})$, for all $\alpha \in L$. Thus j^2 defines a unique element in $\mathbb{Q}^\times / \mathrm{N}(L^\times)$. From now on, we will represent $\mathbb{B}_{\ell,\infty}$ as a sub-algebra of $\mathrm{M}_2(L)$ as follows.

$$\mathbb{B}_{\ell,\infty} = \left\{ [\alpha : \beta] := \begin{pmatrix} \alpha & \beta \\ j^2\overline{\beta} & \overline{\alpha} \end{pmatrix} : \alpha, \beta \in L \right\}. \tag{4.1}$$

Under this representation, $\iota\colon L \hookrightarrow \mathbb{B}_{\ell,\infty}, \quad \iota(\alpha) = [\alpha, 0]$.
If ℓ is unramified in $\mathcal{O}$ then we may assume that $j^2 = -\ell q$, where q is a prime such that $-\ell q \in \ker \Psi$ and qd. If ℓ is ramified, then we may assume that $j^2 = -q$ where $-q \in \ker \widehat{\Psi}_\ell$, $-q \notin \ker \Psi_\ell$ and qd. (The functions Ψ, $\widehat{\Psi}_\ell$ and Ψ_ℓ were defined in Section 3 above.) In both cases, these conditions imply that q is split in $\mathcal{O}$.

4.2. The inert case. — Let $\mathfrak{a} \subseteq \mathcal{O}$ be an integral invertible ideal such that $\gcd(f, \mathrm{N}(\mathfrak{a})) = 1$. Let $\mathfrak{q}$ be a prime ideal of $\mathcal{O}$ lying over q. For any $\lambda \in \mathcal{O}$ such that

1. $\lambda\mathfrak{q}^{-1}\overline{\mathfrak{a}}\mathfrak{a}^{-1} \subseteq \mathcal{O}$, and

2. $\mathrm{N}(\lambda) \equiv -\ell q \pmod{d}$,

we define

$$R(\mathfrak{a},\lambda) := \left\{[\alpha,\beta] : \alpha \in \mathfrak{D}^{-1}, \beta \in \mathfrak{q}^{-1}\ell^{n-1}\mathfrak{D}^{-1}\overline{\mathfrak{a}}\mathfrak{a}^{-1}, \alpha - \lambda\beta \in \mathcal{O}\right\}.$$

From this definition, it is clear that if λ' satisfies (1) and (2) and $\lambda \equiv \lambda' \pmod{\mathfrak{D}}$, then $R(\mathfrak{a},\lambda) = R(\mathfrak{a},\lambda')$. We claim that, for any $\mathfrak{a}$ and λ, $R(\mathfrak{a},\lambda)$ is a maximal order.

Remark 4.2.1. — *Although Dorman* [5] *does not include condition* (1) *in his definition, it is, in fact, necessary. Without this assumption $R(\mathfrak{a},\lambda)$ is not closed under multiplication, even if d is squarefree. This was already remarked on in* [12].

Remark 4.2.2. — *Write $\lambda = \lambda_0 + \lambda_1\frac{d+\sqrt{d}}{2}$. If d is odd, then the congruence class of $\lambda \bmod \mathfrak{D}$ is determined by $\lambda_0 \bmod d$. In addition, the condition that $\mathrm{N}(\lambda) \equiv -\ell q \pmod{d}$ is equivalent to the condition that $\lambda_0^2 \equiv -\ell q \pmod{d}$. Therefore, if d is odd, then we may think of λ as an integer, instead of as an element of $\mathcal{O}$. This was the point of view taken in* [15, 5].

Lemma 4.2.3. — *$R(\mathfrak{a},\lambda)$ is an order with discriminant ℓ^2, and so it is maximal.*
Proof. — [21, Section 6] □

Given an ideal $\mathfrak{a}$, we will now construct a $\lambda = \lambda_{\mathfrak{a}}$ satisfying conditions (1) and (2). Since we want our orders $R(\mathfrak{a}) := R(\mathfrak{a},\lambda_{\mathfrak{a}})$ to satisfy

$$R(\mathfrak{a})\mathfrak{b} = \mathfrak{b}R(\mathfrak{a}\mathfrak{b})$$

the relationship between $\lambda_{\mathfrak{a}}$ and $\lambda_{\mathfrak{a}\mathfrak{b}}$ will be quite important. In fact, the relation

$$R(\mathcal{O})\mathfrak{a} = \mathfrak{a}R(\mathfrak{a})$$

shows that $R(\mathfrak{a})$ is determined from $R(\mathcal{O})$ and so $\lambda_{\mathfrak{a}} \bmod \mathfrak{D}$ is determined by $\lambda_{\mathcal{O}} \bmod \mathfrak{D}$.

4.2.1. *Defining $\lambda_{\mathfrak{a}}$.* — For all regular ramified primes p, fix two elements $\lambda^{(p)}, \widetilde{\lambda}^{(p)} \in \mathcal{O}$ with norm congruent to $-\ell q \bmod p^{v(d)}$ such that $\lambda^{(p)} \not\equiv \widetilde{\lambda}^{(p)} \pmod{\mathfrak{D}_p}$. For all irregular ramified primes p, fix $\lambda^{(p)} \in \mathcal{O}$ such that $\mathrm{N}(\lambda^{(p)}) \equiv -\ell q \pmod{p^{v(d)}}$.
For any prime ideal $\mathfrak{p}$ of $\mathcal{O}$ that is prime to $\mathfrak{D}$, let $M(\mathfrak{p})$ denote a fixed integer that is divisible by $\mathrm{N}(\mathfrak{p})$ and congruent to 1 $\pmod{d}$. For any product of regular ramified primes $\mathfrak{b}_d := \prod_{\substack{\mathfrak{p} \text{ regular} \\ \mathfrak{p}\mid\mathfrak{D}}} \mathfrak{p}^{e_{\mathfrak{p}}}$, we write $\lambda_{\mathfrak{b}_d}$ for any element in $\mathcal{O}$ such that

$$\lambda_{\mathfrak{b}_d} \bmod \mathfrak{D}_p \equiv \begin{cases} \lambda^{(p)} & \text{if } e_p \equiv 0 \pmod 2 \\ \widetilde{\lambda}^{(p)} & \text{if } e_p \equiv 1 \pmod 2 \end{cases}$$

for all regular primes $\mathfrak{p}$ and $\lambda_{\mathfrak{b}} \equiv \lambda^{(p)} \pmod{\mathfrak{D}_p}$ for all irregular primes. These conditions imply that $\lambda_{\mathfrak{b}_d}$ is well-defined modulo $\mathfrak{D}$.
Let $\mathfrak{a}$ be an invertible integral ideal $\mathcal{O}$ such that $\gcd(\mathrm{N}(\mathfrak{a}), f) = 1$. Then we may factor $\mathfrak{a}$ as $\mathfrak{a}'\mathfrak{a}_d$, where $\mathfrak{a}'$ is prime to the discriminant and $\mathfrak{a}_d$ is supported only on regular ramified primes. We define $\lambda_{\mathfrak{a}} := \left(\prod_{\mathfrak{p}\mid\mathfrak{a}'} M(\mathfrak{p})^{v_{\mathfrak{p}}(\mathfrak{a}')}\right) M(\mathfrak{q})\lambda_{\mathfrak{a}_d}$. Note that it follows from this definition that $\lambda_{\mathfrak{a}}$ is well-defined modulo $\mathfrak{D}$ and, importantly, that $\lambda_{\mathfrak{a}}$ satisfies $\lambda_{\mathfrak{a}}\mathfrak{q}^{-1}\overline{\mathfrak{a}}\mathfrak{a}^{-1} \subset \mathcal{O}$ and $\mathrm{N}(\lambda_{\mathfrak{a}}) \equiv -\ell q \mod d$.

Lemma 4.2.4. — *Let $\mathfrak{a}, \mathfrak{b}$ be two invertible ideals in $\mathcal{O}$ that are prime to the conductor. Assume that $\mathfrak{a}$ and $\mathfrak{ab}$ are both integral. Then*

$$R(\mathfrak{a}, \lambda_{\mathfrak{a}})\mathfrak{b} = \mathfrak{b}R(\mathfrak{ab}, \lambda_{\mathfrak{ab}}).$$

Proof. — [21, Section 6] □

4.3. The ramified case. — Let $\mathfrak{a} \subseteq \mathcal{O}$ be an integral invertible ideal such that $\gcd(f, \mathrm{N}(\mathfrak{a})) = 1$. Let $\mathfrak{q}$ be a prime ideal of $\mathcal{O}$ lying over q. For any $\lambda \in \mathcal{O}$ such that

1. $\lambda\mathfrak{q}^{-1}\overline{\mathfrak{a}}\mathfrak{a}^{-1} \subseteq \mathcal{O}$, and
2. $\mathrm{N}(\lambda) \equiv -q \pmod{d/\ell}$,

we define

$$R(\mathfrak{a}, \lambda) := \left\{[\alpha, \beta] : \alpha \in \mathfrak{l}\mathfrak{D}^{-1}, \beta \in \mathfrak{q}^{-1}\mathfrak{l}\mathfrak{D}^{-1}\overline{\mathfrak{a}}\mathfrak{a}^{-1}, \alpha - \lambda\beta \in \mathcal{O}\right\}.$$

From this definition, it is clear that if λ' satisfies (1) and (2) and $\lambda \equiv \lambda' \pmod{\mathfrak{D}\mathfrak{l}^{-1}}$, then $R(\mathfrak{a}, \lambda) = R(\mathfrak{a}, \lambda')$. We claim that, for any $\mathfrak{a}$ and λ, $R(\mathfrak{a}, \lambda)$ is a maximal order.

Lemma 4.3.1. — *$R(\mathfrak{a}, \lambda)$ is an order of discriminant ℓ^2, and so it is maximal.*

Proof. — This proof is exactly the same as in the inert case after replacing q with q/ℓ ([21, Section 6]). □

4.3.1. *Defining $\lambda_{\mathfrak{a}}$.* — For all regular ramified primes p, fix two elements $\lambda^{(p)}, \widetilde{\lambda}^{(p)} \in \mathcal{O}$ with norm congruent to $-q \bmod p^{v(d/\ell)}$ such that $\lambda^{(p)} \not\equiv \widetilde{\lambda}^{(p)} \pmod{\mathfrak{D}_p}$. If $p = \ell$ and $\ell \neq 2$, then in addition we assume that $\lambda_{\ell,0} = -\lambda_{\ell,1}$. For all irregular ramified primes p, fix $\lambda^{(p)} \in \mathcal{O}$ such that $\mathrm{N}(\lambda^{(p)}) \equiv -q \pmod{p^{v(d/\ell)}}$.
For any prime ideal $\mathfrak{p}$ of $\mathcal{O}$ that is coprime to $\mathfrak{D}$, let $M(\mathfrak{p})$ denote a fixed integer that is divisible by $\mathrm{N}(\mathfrak{p})$ and congruent to 1 $(\bmod\, d)$. For any product of regular ramified primes $\mathfrak{b}_d := \prod_{\substack{\mathfrak{p} \text{ regular} \\ \mathfrak{p}|\mathfrak{D}}} \mathfrak{p}^{e_{\mathfrak{p}}}$, we write $\lambda_{\mathfrak{b}_d}$ for any element in $\mathcal{O}$ such that

$$\lambda_{\mathfrak{b}_d} \bmod \mathfrak{D}_p \equiv \begin{cases} \lambda^{(p)} & \text{if } e_p \equiv 0 \pmod 2 \\ \widetilde{\lambda}^{(p)} & \text{if } e_p \equiv 1 \pmod 2 \end{cases}$$

for all regular primes $\mathfrak{p}$ and $\lambda_{\mathfrak{b}} \equiv \lambda^{(p)} \pmod{\mathfrak{D}_p}$ for all irregular primes. These conditions imply that $\lambda_{\mathfrak{b}_d}$ is well-defined modulo $\mathfrak{D}$.
Let $\mathfrak{a}$ be an invertible integral ideal $\mathcal{O}$ such that $(\mathrm{N}(\mathfrak{a}), f) = 1$. Then we may factor $\mathfrak{a}$ as $\mathfrak{a}'\mathfrak{a}_d$, where $\mathfrak{a}'$ is coprime to the discriminant and $\mathfrak{a}_d$ is supported only on regular ramified primes. We define $\lambda_{\mathfrak{a}} := \left(\prod_{\mathfrak{p}|\mathfrak{a}'} M(\mathfrak{p})^{v_{\mathfrak{p}}(\mathfrak{a}')}\right) M(\mathfrak{q})\lambda_{\mathfrak{a}_d}$. Note that $\lambda_{\mathfrak{a}}$ is well-defined modulo $\mathfrak{D}$ and that $\lambda_{\mathfrak{a}}$ satisfies $\lambda_{\mathfrak{a}}\mathfrak{q}^{-1}\overline{\mathfrak{a}}\mathfrak{a}^{-1} \subset \mathcal{O}$ and $\mathrm{N}(\lambda_{\mathfrak{a}}) \equiv -q \mod d/\ell$.

Remark 4.3.2. — *Since $\lambda_{\mathfrak{a}} \equiv \lambda_{\mathfrak{a}\mathfrak{l}} \pmod{\mathfrak{D}\mathfrak{l}^{-1}}$ for any integral invertible ideal $\mathfrak{a}$, the corresponding orders $R(\mathfrak{a})$, $R(\mathfrak{a}\mathfrak{l})$ are equal. This is not surprising, since $E(\mathfrak{a}) \cong E(\mathfrak{a}\mathfrak{l})$ modulo π.*

Lemma 4.3.3. — *Let $\mathfrak{a}, \mathfrak{b}$ be two invertible ideals in $\mathcal{O}$ that are coprime to the conductor. We assume that $\mathfrak{a}$ and $\mathfrak{ab}$ are integral. Then*

$$R(\mathfrak{a}, \lambda_{\mathfrak{a}})\mathfrak{b} = \mathfrak{b}R(\mathfrak{ab}, \lambda_{\mathfrak{ab}}).$$

Proof. — [21, Section 6] □

4.4. Elliptic curves with complex multiplication. —

Theorem 4.4.1. — *Let R be a maximal order of $\mathbb{B}_{\ell,\infty}$ such that $R \cap L = \mathcal{O}$, where the intersection takes place using the embedding of $\mathbb{B}_{\ell,\infty} \subset \mathrm{M}_2(L)$ given in* (4.1)*. Then there is an integral invertible ideal $\mathfrak{a} \subseteq \mathcal{O}$ coprime to the conductor such that R is conjugate to $R(\mathfrak{a}, \lambda_\mathfrak{a})$ by an element of $L^\times$.*
Proof. — [21, Section 6]

□

Fix an element $[\tau^{(0)}]$ of discriminant d, and let $E = E(\tau^0)$ be an elliptic curve over $\mathbb{W}$ with $j(E) = j(\tau^{(0)})$ and good reduction at π. Then we have an optimal embedding of $\mathcal{O} \cong \mathrm{End}(E)$ into $\mathrm{End}_{\mathbb{W}/\pi}(E)$, a maximal order in $\mathbb{B}_{\ell,\infty}$. Thus, by Theorem 4.4.1, there is an element $[\mathfrak{a}_0] \in \mathrm{Pic}(\mathcal{O})$ such that the pair

$$(\mathrm{End}(E \bmod \mathfrak{l}), \iota \colon \mathcal{O} = \mathrm{End}(E) \hookrightarrow \mathrm{End}(E \bmod \mathfrak{l}))$$

is conjugate to $R(\mathfrak{a}_0)$ with the diagonal embedding $\mathcal{O} \hookrightarrow R(\mathfrak{a}_0)$. Now let $\sigma \in \mathrm{Gal}(H/L)$ and consider the pair

$$(\mathrm{End}(E^\sigma \bmod \mathfrak{l}), \iota \colon \mathcal{O} \hookrightarrow \mathrm{End}(E^\sigma \bmod \mathfrak{l}))\,.$$

By class field theory, $\mathrm{Gal}(H/L) \cong \mathrm{Pic}(\mathcal{O})$; let $\mathfrak{a} = \mathfrak{a}_\sigma$ be an invertible ideal that corresponds to σ; note that $\mathfrak{a}$ is unique as an element of $\mathrm{Pic}(\mathcal{O})$. We assume that $\mathfrak{a}$ is integral and coprime to the conductor. Since $\mathrm{Hom}(E^\sigma, E)$ is isomorphic to $\mathfrak{a}$ as a left $\mathrm{End}(E)$-module, we have $\mathrm{End}(E^\sigma \bmod \mathfrak{l}) = \mathfrak{a}\,\mathrm{End}(E)\mathfrak{a}^{-1}$[2, Chap. XIII]. Thus, by Lemmas 4.2.4 and 4.3.3, the pair corresponding to E^σ is conjugate to $R(\mathfrak{a}_0\overline{\mathfrak{a}})$.
We define

$$R_n(\mathfrak{a}) := \left\{[\alpha,\beta] : \alpha \in \mathfrak{D}^{-1}, \beta \in \mathfrak{q}^{-1}\ell^{n-1}\mathfrak{D}^{-1}\overline{\mathfrak{a}}\mathfrak{a}^{-1}, \alpha - \lambda_\mathfrak{a}\beta \in \mathcal{O}\right\}, \quad \text{if } \ell d$$

$$R_n(\mathfrak{a}) := \left\{[\alpha,\beta] : \alpha \in \mathfrak{D}^{-1}, \beta \in \mathfrak{q}^{-1}\mathfrak{l}^{n}\mathfrak{D}^{-1}\overline{\mathfrak{a}}\mathfrak{a}^{-1}, \alpha - \lambda_\mathfrak{a}\beta \in \mathcal{O}\right\}, \quad \text{if } \ell | d$$

One can easily check that $R_1(\mathfrak{a}) = R(\mathfrak{a})$, that $\bigcap_n R_n(\mathfrak{a}) = \mathcal{O}$ and that

$$R_n(\mathfrak{a}) = \begin{cases} \mathcal{O} + \ell^{n-1}R_1(\mathfrak{a}) & \text{if } \ell d, \\ \mathcal{O} + \mathfrak{l}^{n-1}R_1(\mathfrak{a}), & \text{if } \ell | d \end{cases} \tag{4.2}$$

Then by [13, Prop. 3.3], $\mathrm{End}_{W/\pi^n}(E^\sigma) \cong R_n(\mathfrak{a}_0\overline{\mathfrak{a}})$.

5. Calculating the number of (E, x, u)

Proposition 5.1. — *Let E be an elliptic curve over $\overline{\mathbb{F}}_\ell$ and assume that there exists $x, u \in \mathrm{End}(E)$ satisfying* (2.12)–(2.15)*. Then E must be supersingular and there exists an $n \in \mathbb{Z}$ such that*

$$\frac{\delta^2\widetilde{D} - n^2}{4D} \in \ell\mathbb{Z}_{>0}, \text{ and } n + c_\delta(K) \equiv 0 \pmod{2D}, \tag{5.1}$$

where $c_K(\delta) := \delta\left(\alpha_0^2 + \alpha_0\alpha_1 D + \alpha_1^2\frac{D^2-D}{4} - 4\beta_0 - 2\beta_1 D\right)$.

Proof. — [22, Prop 3.1] □

Proposition 5.1 shows that the tuples (E, x, u) satisfying (2.12)–(2.15) can be partitioned by integers n satisfying (5.1). By the proof of Proposition 5.1, fixing such an n implies that $\mathrm{N}(u) = n_u(n), \mathrm{N}(x) = n_x(n)$, and $\mathrm{Tr}(xu^\vee) = t_{xu^\vee}(n)$ where

$$n_u(n) := \frac{-\delta(n + c_K\delta)}{2D}, \quad n_x(n) := \beta_0 + a\beta_1 - \frac{n_u(n)}{\delta}, \quad \& \quad t_{xu^\vee}(n) := \beta_1\delta - (D - 2a)\frac{n_u(n)}{\delta}.$$

The trace of x and u are already determined by δ, so we define

$$d_u(n) := (\alpha_1\delta)^2 - 4n_u(n) \quad \text{and} \quad d_x(n) := (\alpha_0 + a\alpha_1)^2 - 4n_x(n).$$

For the rest of the section, we assume that n is a fixed integer satisfying (5.1). We define

$$\mathcal{E}(n) := \left\{ [(E, x, u)] : \begin{array}{l} \mathrm{Tr}(x) = \alpha_0 + a\alpha_1, \mathrm{Tr}(u) = \alpha_1\delta, \\ \mathrm{N}(u) = n_u(n), \mathrm{N}(x) = n_x(n), \mathrm{Tr}(xu^\vee) = t_{xu^\vee}(n) \end{array} \right\},$$

where $[(E, x, u)]$ denotes the isomorphism class of (E, x, u).

5.1. Counting pairs of endomorphisms for a fixed n. — Fix a prime ℓ.
Let $t_x, t_u, t_{xu^\vee}, n_x, n_u$ be integers such that either $d_x := t_x^2 - 4n_x$ or $d_u := t_u^2 - 4n_u$ is a quadratic discriminant fundamental at ℓ and such that $d_xd_u - (t_xt_u - 2t_{xu^\vee})^2$ is nonzero. In the rest of this section we will count triples (E, x, u) where E is a supersingular elliptic curve over $\overline{\mathbb{F}}_\ell$ and $x, u \in \mathrm{End}(E)$ satisfy $\mathrm{Tr}(x) = t_x, \mathrm{Tr}(u) = t_u, \mathrm{Tr}(xu^\vee) = t_{xu^\vee}, \mathrm{N}(x) = n_x$, and $\mathrm{N}(u) = n_u$.
The formula for the number of such triples and the proof become significantly more technical if $t_xt_u - 2t_{xu^\vee}$ has a common factor prime to ℓ with either the conductor of d_x or the conductor of d_u. For the sake of exposition, we will first give the formula and proof in a less technical case (§5.1.1), and then we will consider the general case (§5.1.2).

5.1.1. *A simpler case.* — Let $t_x, t_u, t_{xu^\vee}, n_x, n_u, d_x, d_u$ be as above. We also assume that

$$\mathrm{GCD}(t_xt_x - 2t_{xu^\vee}, \mathrm{cond}(d_u))$$

is a power of ℓ, where $1 = \ell^0$ is considered to be a power of ℓ. Let $v := v_\ell(\mathrm{cond}(d_u))$.

Theorem 5.1.1. — *The number of triples (E, x, u) where $E/\overline{\mathbb{F}}_\ell$ is a supersingular elliptic curve, and x, u are endomorphisms satisfying*

$$\deg(x) = n_x, \deg(u) = n_u, \mathrm{Tr}(x) = t_x, \mathrm{Tr}(u) = t_u, \mathrm{Tr}(xu^\vee) = t_{xu^\vee}$$

is equal to

$$\mathfrak{A}_d\left(\frac{d_xd_u - (t_xt_u - 2t_{xu^\vee})^2}{4\ell^{1+2v}}\right)\rho_{d,\ell}\left(\frac{d_xd_u - (t_xt_u - 2t_{xu^\vee})^2}{4\ell^{1+2v}}\right),$$

where $d = d_u/\ell^{2v}$, $\mathfrak{A}_d(N) := \#\{\mathfrak{b} \subset \mathcal{O}_d : \mathrm{N}(\mathfrak{b}) = N,\ \mathfrak{b} \text{ invertible }\}$, and

$$\rho_{d,\ell}(N) := \begin{cases} 0 & \text{if } \Psi_d(N) \neq \Psi_d(-\ell) \\ 2^{\#\{p : p \mid (N,d), p \neq \ell\}} & \text{otherwise.} \end{cases}$$

Proof. — Since E is a supersingular elliptic curve, $\mathrm{End}(E)$ is a maximal order in the quaternion algebra $\mathbb{B}_{\ell,\infty}$. Since $\mathrm{End}(E)$ contains u, $\mathbb{Q}[u] \cap \mathrm{End}(E)$ is an order in $\mathbb{Q}(\sqrt{d_u})$ of discriminant $d = d_u/f^2$ for some integer f. In addition, d must be fundamental at ℓ [29, Chap. 2, Lemma 1.5], so ℓ^v must divide f.

Fix such a d. Then, by Theorem 4.4.1, $\mathrm{End}(E) \cong R(\mathfrak{a})$, $u \mapsto \left[\frac{t_u + f\sqrt{d}}{2}, 0\right]$, where $\mathfrak{a}$ is an invertible ideal in $\mathcal{O}_d$. By [13], if ℓ is inert in $\mathcal{O}_d$, then $\mathfrak{a}$ is well-defined as an element in $\mathrm{Pic}(\mathcal{O}_d)$, and if ℓ is ramified then there are 2 choices for $\mathfrak{a} \in \mathrm{Pic}(\mathcal{O}_d)$.

Now we have to count the number of elements $[\alpha, \beta]$ in $R(\mathfrak{a})$ such that $\mathrm{Tr}([\alpha,\beta]) = t_x$, $\mathrm{N}([\alpha,\beta]) = n_x$, and $\mathrm{Tr}([\alpha,\beta] \cdot [\frac{t_u + \sqrt{d_u}}{2}, 0]) = t_{xu^\vee}$; such $[\alpha,\beta]$ will correspond to the endomorphism x. The trace conditions imply that $\alpha = \frac{(t_x t_u - 2t_{xu^\vee}) + t_x f\sqrt{d}}{2f\sqrt{d}}$. Since α must be contained in $\mathfrak{D}^{-1}$, we must have $\frac{t_x t_u - 2t_{xu^\vee}}{f} \in \mathbb{Z}$. Using our assumption on the GCD of d and $t_x t_u - 2t_{xu^\vee}$, we must have that $f = \ell^v$.

So we have reduced to counting pairs $(\beta, [\mathfrak{a}])$ where $c_\beta := \left[\frac{(t_x t_u - 2t_{xu^\vee}) + t_x f\sqrt{d}}{2f\sqrt{d}}, \beta\right] \in R(\mathfrak{a})$, $\mathrm{N}(c_\beta) = n_x$ and $\mathfrak{a} \subseteq \mathcal{O}_d$, an invertible ideal, under the assumption that

$$N := \frac{d_x d_u - (t_x t_u - 2t_{xu^\vee})^2}{4\ell^{2v+1}} = \frac{d_x d_u - (t_x t_u - 2t_{xu^\vee})^2}{4f^2\ell}$$

is prime to the conductor of d. Since each pair $(\beta, [\mathfrak{a}])$ will correspond to a distinct (E, x, u) if ℓ is inert, and, if ℓ is ramified, then exactly 2 pairs $(\beta, [\mathfrak{a}])$ will correspond to the same (E, x, u). This combined with the following proposition shows that the number of triples (E, x, u) is $\mathfrak{A}(N)\rho_{d,\ell}(N)$ as desired. □

Proposition 5.2. — *Let $t_x, t_u, t_{xu^\vee}, n_x, n_u \in \mathbb{Z}$ be as defined at the beginning of the section. Let $v = v_\ell(\mathrm{cond}(t_u^2 - 4n_u))$, set $f = \ell^v$, $d = d_u/f^2$ and set $N := \frac{d_x d_u - (t_x t_u - 2t_{xu^\vee})^2}{4f^2\ell}$. Assume that N is prime to the conductor of d. Then there is an $e \cdot \rho_{d,\ell}(N)$-to-1 map*

$$\begin{array}{rcl} \{(\beta, [\mathfrak{a}]) : c_\beta \in R(\mathfrak{a}), \mathrm{N}(c_\beta) = n_x, \mathfrak{a} \subseteq \mathcal{O}_d \text{ invertible}\} & \to & \{\mathfrak{b} \subseteq \mathcal{O}_d : \mathrm{N}(\mathfrak{b}) = N, \mathfrak{b} \text{ invertible}\}, \\ (\beta, \mathfrak{a}) & \mapsto & \beta\mathfrak{q}\mathfrak{D}\mathfrak{a}\bar{\mathfrak{a}}^{-1} \quad \text{if } \ell \text{ is inert in } \mathcal{O}_d, \\ (\beta, \mathfrak{a}) & \mapsto & \beta\mathfrak{l}^{-1}\mathfrak{q}\mathfrak{D}\mathfrak{a}\bar{\mathfrak{a}}^{-1} \quad \text{if } \ell \text{ is ramified in } \mathcal{O}_d. \end{array}$$

where $c_\beta := \left[\frac{(t_x t_u - 2t_{xu^\vee}) + t_x f\sqrt{d}}{2f\sqrt{d}}, \beta\right]$, and $\mathfrak{q}$ is as defined in §4, and e is the ramification index of ℓ in $\mathcal{O}_d$.

Proof. — First we show that the map is well-defined if ℓ is inert in $\mathcal{O}_d$. By the definition of $R(\mathfrak{a})$, $\beta \in \mathfrak{q}^{-1}\mathfrak{D}^{-1}\overline{\mathfrak{a}}\mathfrak{a}^{-1}$ so $\beta\mathfrak{q}\mathfrak{D}\mathfrak{a}\overline{\mathfrak{a}}^{-1}$ is integral. Since $\mathrm{N}(c_\beta) = n_x$, we have

$$\begin{aligned}\mathrm{N}(\beta\mathfrak{q}\mathfrak{D}\mathfrak{a}\overline{\mathfrak{a}}^{-1}) = -\mathrm{N}(\beta)qd &= \frac{-d}{\ell}\left(n_x - \mathrm{N}\left(\frac{(t_x t_u - 2t_{xu^\vee}) + t_x f\sqrt{d}}{2f\sqrt{d}}\right)\right)\\ &= \frac{-d}{\ell}\left(n_x - \frac{(t_x t_u - 2t_{xu^\vee})^2 - t_x^2 f^2 d}{-4f^2 d}\right)\\ &= \frac{1}{4\ell f^2}\left(f^2 d(t_x^2 - 4n_x) - (t_x t_u - 2t_{xu^\vee})^2\right)\\ &= N.\end{aligned}$$

Since $\mathfrak{a}$ and $\mathfrak{q}$ are invertible and $\mathfrak{D}$ is principal, $\beta\mathfrak{q}\mathfrak{D}\mathfrak{a}\overline{\mathfrak{a}}^{-1}$ is invertible. A similar computation shows that the map is well-defined in the ramified case.

Assume that N is coprime to the conductor of d. We first consider the case where $\Psi_{d,p}(N) \neq \Psi_{d,p}(-\ell)$ for some $p \neq \ell$. First we assume that ℓ is inert in $\mathcal{O}_d$. Since q was chosen such that $\Psi_{d,p}(-\ell q) = 1$ for all $p \neq \ell$, $\Psi_{d,p}(N) \neq \Psi_{d,p}(q)$ for some prime p. Thus, by Theorem 3.1.1, there is no ideal $\mathfrak{b} \subseteq \mathcal{O}_d$ such that $[\mathfrak{b}\mathfrak{q}^{-1}] \in 2\operatorname{Pic}(\mathcal{O}_d)$ and $\mathrm{N}(\mathfrak{b}) = N$ so the domain must be empty. Now assume that ℓ is ramified. In this case q was chosen such that $\Psi_{d,p}(-q) = 1$ for all $p \neq \ell$ so there is some $p \neq \ell$ such that $\Psi_{d,p}(N) \neq \Psi_{d,p}(\ell q)$. Therefore, again by Theorem 3.1.1, there is no ideal $\mathfrak{b} \subseteq \mathcal{O}_d$ such that $[\mathfrak{b}\mathfrak{l}\mathfrak{q}^{-1}] \in 2\operatorname{Pic}(\mathcal{O}_d)$ and $\mathrm{N}(\mathfrak{b}) = N$ so again the domain must be empty.

Now assume that $\Psi_{d,p}(N) = \Psi_{d,p}(-\ell)$ for all $p \neq \ell$. Then by our assumptions on q, $\widehat{\Psi}_\ell(N) = \widehat{\Psi}_\ell(q)$ if ℓ is inert, or such that $\widehat{\Psi}_\ell(N) = \widehat{\Psi}_\ell(\ell q)$ if ℓ is ramified. Fix an integral invertible ideal $\mathfrak{b}$ in the codomain. By [21, Cor. 5.2], if ℓ is inert, $\mathfrak{b} = \gamma_{\mathfrak{a}}\mathfrak{q}\mathfrak{a}\overline{\mathfrak{a}}^{-1}$ for some invertible ideal $\mathfrak{a}$ and $\gamma_{\mathfrak{a}} \in \mathbb{Q}(\sqrt{d})^\times$ ($\gamma_{\mathfrak{a}}$ is uniquely determined by $\mathfrak{a}$). Similarly, if ℓ is ramified then $\mathfrak{b} = \gamma_{\mathfrak{a}}\mathfrak{l}^{-1}\mathfrak{q}\mathfrak{a}\overline{\mathfrak{a}}^{-1}$ for some invertible ideal $\mathfrak{a}$ and $\gamma_{\mathfrak{a}} \in \mathbb{Q}(\sqrt{d})^\times$ (again $\gamma_{\mathfrak{a}}$ is uniquely determined by $\mathfrak{a}$). Note that for every $\mathfrak{c} \in \operatorname{Pic}(\mathcal{O})[2]$, $\mathfrak{b}$ can also be written as $\gamma_{\mathfrak{a}\mathfrak{c}}\mathfrak{q}\mathfrak{a}\mathfrak{c}(\overline{\mathfrak{a}\mathfrak{c}})^{-1}$ if ℓ is inert, and as $\gamma_{\mathfrak{a}\mathfrak{c}}\mathfrak{l}^{-1}\mathfrak{q}\mathfrak{a}\mathfrak{c}(\overline{\mathfrak{a}\mathfrak{c}})^{-1}$ if ℓ is ramified, where $\gamma_{\mathfrak{a}\mathfrak{c}} = \gamma_{\mathfrak{a}}\epsilon_{\overline{\mathfrak{c}}^2}/\mathrm{N}(\mathfrak{c})$ and $\overline{\mathfrak{c}}^2 = (\epsilon_{\overline{\mathfrak{c}}^2})$.

Let $\beta_{\mathfrak{a}\mathfrak{c}} := \gamma_{\mathfrak{a}\mathfrak{c}}/\sqrt{d}$ so that $\mathfrak{b} = \beta_{\mathfrak{a}\mathfrak{c}}\mathfrak{q}\mathfrak{D}\mathfrak{a}\mathfrak{c}(\overline{\mathfrak{a}\mathfrak{c}})^{-1}$ in the inert case, and $\mathfrak{b} = \beta_{\mathfrak{a}\mathfrak{c}}\mathfrak{l}^{-1}\mathfrak{q}\mathfrak{D}\mathfrak{a}\mathfrak{c}(\overline{\mathfrak{a}\mathfrak{c}})^{-1}$ in the ramified case. One can easily check that $\mathrm{N}(c_{\beta_{\mathfrak{a}\mathfrak{c}}}) = n_x$ and that $\beta_{\mathfrak{a}\mathfrak{c}} \in \mathfrak{q}^{-1}\mathfrak{D}^{-1}\overline{\mathfrak{a}\mathfrak{c}}(\mathfrak{a}\mathfrak{c})^{-1}$ in the inert case, and $\beta_{\mathfrak{a}\mathfrak{c}} \in \mathfrak{q}^{-1}\mathfrak{l}\mathfrak{D}^{-1}\overline{\mathfrak{a}\mathfrak{c}}(\mathfrak{a}\mathfrak{c})^{-1}$ in the ramified case. Since N is an integer, $t_x t_u - 2t_{xu^\vee} \equiv 0 \pmod f$, so $\frac{(t_x t_u - 2t_{xu^\vee}) + t_x f\sqrt{d}}{2f\sqrt{d}} \in \mathfrak{D}^{-1}$. In the case ℓ is ramified, one can show that $\frac{(t_x t_u - 2t_{xu^\vee}) + t_x f\sqrt{d}}{2f\sqrt{d}} \in \mathfrak{l}\mathfrak{D}^{-1}$. Therefore $(\beta_{\mathfrak{a}\mathfrak{c}}, \mathfrak{a}\mathfrak{c})$ is in the pre-image of $\mathfrak{b}$ if and only if

$$\frac{(t_x t_u - 2t_{xu^\vee}) + t_x f\sqrt{d}}{2f\sqrt{d}} - \lambda_{\mathfrak{a}\mathfrak{c}}\beta_{\mathfrak{a}\mathfrak{c}} \in \mathcal{O},$$

or equivalently,

$$\frac{t_x t_u - 2t_{xu^\vee}}{2f} + \frac{t_x}{2}\sqrt{d} - \lambda_{\mathfrak{a}\mathfrak{c}}\gamma_{\mathfrak{a}\mathfrak{c}} \in \mathfrak{D}. \tag{5.2}$$

Fix $\mathfrak{c}_1, \ldots, \mathfrak{c}_{2^{\mu-1}}$ representatives for $\operatorname{Pic}(\mathcal{O})[2]$, that are prime to the discriminant. To calculate the size of the pre-image of $\mathfrak{b}$, we need to determine for which $\mathfrak{c}_i$ (5.2) holds. Since $\mathfrak{c}_i$ is prime to the discriminant, we may rewrite $\lambda_{\mathfrak{a}\mathfrak{c}_i}\gamma_{\mathfrak{a}\mathfrak{c}_i} = (M(\mathfrak{c}_i)\epsilon_{\overline{\mathfrak{c}}_i^2}/\mathrm{N}(\mathfrak{c}_i))\lambda_{\mathfrak{a}}\gamma_{\mathfrak{a}}$, where $M(\mathfrak{c}_i)$ is as in

subsection 4.3.1. Applying [21, Lemmas 7.5 and 7.6] with $a := \frac{t_x t_u - 2t_{xu^\vee}}{2f} + \frac{t_x}{2}\sqrt{d}$ and $b := \lambda_{\mathfrak{a}}\gamma_{\mathfrak{a}}$ completes the proof. □

5.1.2. *The general case.* — Now we would like to consider the case where N and $\mathrm{cond}(d_u)$ share common factors different from ℓ.

Theorem 5.1.2. — *The number of triples (E, x, u) where $E/\overline{\mathbb{F}}_\ell$ is a supersingular elliptic curve, and x, u are endomorphisms satisfying*

$$\deg(x) = n_x, \deg(u) = n_u, \mathrm{Tr}(x) = t_x, \mathrm{Tr}(u) = t_u, \mathrm{Tr}(xu^\vee) = t_{xu^\vee}$$

is equal to

$$\sum_{\substack{f\in\mathbb{Z} \\ d:=d_u/f^2\in\mathbb{Z} \\ \text{fundamental at } \ell}} \widetilde{\mathfrak{A}}_d\left(\frac{d_x d_u - (t_x t_u - 2t_{xu^\vee})^2}{4f^2\ell}\right)\widetilde{\rho}_{d,\ell}\left(\frac{t_x t_u - 2t_{xu^\vee}}{2f}, t_x\right),$$

where

$$\mathfrak{r} := \begin{cases} \mathfrak{q} & \text{if } \ell \text{ inert in } \mathcal{O}_d, \\ \mathfrak{l}^{-1}\mathfrak{q} & \text{otherwise.} \end{cases}$$

$$\widetilde{\rho}_d^{(2)}(s,t) := \left\{\begin{array}{ll} 2 & \text{if } d \equiv 12 \bmod 16, s \equiv t \bmod 2 \\ & \text{or if } 8 \mid d, v_2(s) \geq v_2(d) - 2 \\ 1 & \text{otherwise} \end{array}\right\} \cdot \left\{\begin{array}{ll} 2 & \text{if } 32 \mid d, 4 \mid (s-2t) \\ 1 & \text{otherwise} \end{array}\right\}$$

$$\widetilde{\rho}_{d,\ell}(s,t) := \begin{cases} \widetilde{\rho}_d^{(2)}(s,t) \cdot 2^{\#\{p : v_p(s) \geq v_p(d), p \neq 2, \ell\}} & \text{for } \ell \neq 2 \\ 2^{\#\{p : v_p(s) \geq v_p(d), p \neq 2, \ell\}} & \text{for } \ell = 2, \end{cases}$$

and

$$\begin{aligned} \widetilde{\mathfrak{A}}_d(N) := \#\{\mathfrak{b} \subset \mathcal{O}_d : \mathrm{N}(\mathfrak{b}) = N, \mathfrak{b} \text{ invertible }, \mathfrak{b} \sim \mathfrak{r} \bmod 2\,\mathrm{Pic}(\mathcal{O}_d) \\ \exists \mathfrak{a} \subset \mathcal{O}_d \text{ prime to } d, \epsilon \in \mathcal{O}_d \\ \text{such that } \langle\gamma\rangle = \mathfrak{b}\mathfrak{r}^{-1}\bar{\mathfrak{a}}\mathfrak{a}^{-1}, \mathrm{N}(\epsilon) \equiv 1 \pmod{d}, \text{ and} \\ \epsilon M(\mathfrak{q})M(\mathfrak{a})\gamma \equiv \frac{t_x t_u - 2t_{xu^\vee}}{2f} + \frac{t_x}{2}\sqrt{d} \pmod{\sqrt{d}}\}\}, \end{aligned}$$

Moreover, there is an algorithm to compute $\widetilde{\mathfrak{A}}_d(N)$ and $\widetilde{\mathfrak{A}}_d(N)$ is always bounded above by $\mathfrak{A}_d(N)$. In addition, if N and the conductor of d, $\mathrm{cond}(d)$, share no common factors, $\widetilde{\mathfrak{A}}_d(N)\widetilde{\rho}_{d,\ell}(N) = \mathfrak{A}_d(N)\rho_{d,\ell}(N)$.

Proof. — We will follow the proof of Theorem 5.1.1. Until the invocation of Proposition 5.2, the only place the GCD assumption is used is in concluding that $f = \ell^v$. In the general case, we are only able to conclude that $\ell^v | f | \mathrm{GCD}(t_x t_u - 2t_{xu^\vee}, \mathrm{cond}(d_u))$. So to count the tuples (E, x, u), we will sum over f as above, and try to follow the proof Proposition 5.2.
It is still a necessary condition that $\Psi_{d,p}(N) = \Psi_{d,p}(-\ell)$ for every prime $p | d, p(\mathrm{cond}(d), N)$ ($\Psi_{d,p}(N)$ is undefined if $p | (\mathrm{cond}(d), N)$). However, as mentioned in §3, this is no longer sufficient. Thus instead of considering all ideals of norm N, as we do in the case where N is prime to the conductor, we must only consider ideals of norm N *in a fixed genus.*

The rest of the proof can be applied in this more general case, until we cite [21, Lemma 7.5 and 7.6]. Lemma 7.6 of [21] no longer guarantees the existence of an ideal $\mathfrak{c}$ such that (5.2) holds. However, once the existence of such an ideal $\mathfrak{c}$ is known, Lemmas 7.5 and 7.6 in [21] still give the exact number of ideal classes $\mathfrak{c}$ for which (5.2) holds. Thus the proof of the formula is complete.
The proof of Proposition 5.2 gives an algorithm to compute $\widetilde{\mathfrak{A}}_d(N)$, and it is clear from the definition that $\widetilde{\mathfrak{A}}_d(N) \leq \mathfrak{A}_d(N)$. The statement about equality follows from the above discussion. □

5.2. Multiplicity of pairs of endomorphisms. —

Proposition 5.3. — *Let E be a supersingular elliptic curve over $\overline{\mathbb{F}}_\ell$, and let $x, u \in \mathrm{End}(E)$ be elements such that at least one of $\mathrm{Disc}(x), \mathrm{Disc}(u)$ is fundamental at ℓ and that the two orders $\mathbb{Q}(x) \cap \mathrm{End}(E)$, $\mathbb{Q}(u) \cap \mathrm{End}(E)$ have different discriminants. Then*

$$\text{length } (\mathbb{W}_{\overline{\mathbb{F}}_\ell}[[t]]/I_{x,u}) = \mu_{\mathrm{Disc}(x),\mathrm{Disc}(u)}(N) := \begin{cases} v_\ell(N) + 1 & \text{if } \ell \mid d \\ \frac{1}{2}(v_\ell(N) + 2) & \text{otherwise,} \end{cases}$$

where $N := \frac{1}{4\ell}\left(\mathrm{Disc}(x)\,\mathrm{Disc}(u) - (\mathrm{Tr}(x)\,\mathrm{Tr}(u) - 2\,\mathrm{Tr}(xu^\vee))^2\right)$, and $d \in \{\mathrm{Disc}(x), \mathrm{Disc}(u)\}$ is chosen so that it is a discriminant fundamental at ℓ.

Proof. — [22, Theorem 3.3] □

In fact, it is always the case that if $\mathcal{E} \neq$ then at least one of $d_u(n), d_x(n)$ is the discriminant of a quadratic imaginary order that is maximal at ℓ.

Lemma 5.2.1. — *Let E be a supersingular elliptic curve over $\overline{\mathbb{F}}_\ell$ and let $x, u \in \mathrm{End}(E)$ be endomorphisms satisfying* (2.12)–(2.15)*. Then the indices*

$$[\mathbb{Q}(x) \cap \mathrm{End}(E) : \mathbb{Z}[x]] \text{ and } [\mathbb{Q}(u) \cap \mathrm{End}(E) : \mathbb{Z}[u]]$$

are relatively prime. In particular, at least one of $\mathbb{Z}[x]$, $\mathbb{Z}[u]$ is a quadratic imaginary order maximal at ℓ.

Proof. — [22, Lemma 3.4] □

5.3. Automorphisms of triples (E, x, u). — Fix a supersingular elliptic curve E, and two endomorphisms x, u such that the $\mathbb{Z}$-algebra generated by x, u has rank 4. This is equivalent to the assumption that $d_x d_u$ is not a square. We define

$$\mathrm{Aut}((E, x, u)) = \{\phi \in \mathrm{Aut}(E) : \phi x = x\phi, \phi u = u\phi\}.$$

Since x, u generate a rank 4 module, if ϕ commutes with x, u, then ϕ is in the center of $\mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$. Since E is supersingular, $\mathrm{End}(E)$ is a maximal order in a quaternion algebra, so the center of $\mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$ is exactly $\mathbb{Q}$. Therefore, for any (E, x, u) as above, $\mathrm{Aut}((E, x, u)) = \{\pm 1\}$.

5.4. Summary. — Fix an odd prime ℓ.
To count solutions x, u, to the embedding problem for a fixed δ, we will range over the integers n which arise in Equation 5.1. Then for a fixed δ and n, the trace and norm of x and u are expressed as above directly in terms of δ, n, and the generators for the quartic CM field K.
Let $t_x, t_u, t_{xu^\vee}, n_x, n_u \in \mathbb{Z}$ be such that $d_x := t_x^2 - 4n_x$ and $d_u := t_u^2 - 4n_u$ are quadratic imaginary discriminants, and at least one of d_x, d_u is fundamental at ℓ. Let $f \in \mathbb{Z}$ be such that $d := d_u/f^2$ is still a quadratic imaginary discriminant.

Definition 5.4.1. — *We define the quantity $M(\delta, n, f)$ as a weighted ideal count of certain invertible ideals of norm N in the order of discriminant d, weighted by the multiplicity and a factor which determines the genus class:*

$$M(\delta, n, f) := \frac{1}{2}\widetilde{\mathfrak{A}}_d(N)\widetilde{\rho}_{d,\ell}(s, t_x)\mu_{d_u,d_x}(Nf^2).$$

where $N = \frac{1}{4f^2\ell}\left(d_x d_u - (t_x t_u - 2t_{xu^\vee})^2\right)$, and $s = \frac{1}{f}\left(t_x t_u - 2t_{xu^\vee}\right)$.

Theorem 5.4.2. — *Define*

$$\begin{aligned}\mathcal{E} &= \mathcal{E}(t_x, t_u, t_{xu^\vee}, n_x, n_u, d)\\ &:= \left\{(E, x, u) : \begin{array}{c} E/\overline{\mathbb{F}}_\ell \text{ supersingular elliptic curve }; x, u \in \operatorname{End} E \text{ such that} \\ \operatorname{Tr}(x) = t_x, \operatorname{Tr}(u) = t_u, \operatorname{Tr}(xu^\vee) = t_{xu^\vee}, \mathrm{N}(x) = n_x, \mathrm{N}(u) = n_u, \\ \text{and such that the order } \mathbb{Q}(u) \cap \operatorname{End}(E) \text{ has discriminant } d \end{array}\right\}.\end{aligned}$$

Then

$$\sum_{(E,x,u)\in\mathcal{E}} \frac{1}{\#\operatorname{Aut}(E, x, u)} \cdot \operatorname{length} \frac{\mathbb{W}[[t]]}{I_{x,u}} = M(\delta, n, f).$$

Proof. — This is just a restated summary of the results in this section. □

6. Determining the pre-image of (E, x, u)

This section is taken from [22, Section 6] with proofs omitted.
Fix an (E, x, u) satisfying (2.12)–(2.15). Assume that there exists an elliptic curve E', $b, y \in \operatorname{Hom}(E', E)$, and $z \in \operatorname{End}(E')$ such that $u = yb^\vee$, $bz = xb + (D - 2a)y$. Then there is a left integral ideal $I := \operatorname{Hom}(E', E) \circ b^\vee$ of $R := \operatorname{End}(E)$ which has the following properties:

1. $\mathrm{N}(I) = \delta$,
2. $\delta, u \in I$, and
3. $w := x + (D - 2a)\frac{u}{\delta} \in R(I)$, where $R(I)$ denotes the right order of I.

In addition, Deuring's correspondence between isogenies and ideals shows that a left ideal satisfying the above three properties uniquely determines E', $b, y \in \operatorname{Hom}(E', E)$, and $z \in \operatorname{End}(E')$, up to isomorphisms of E and E'.

6.1. Formula for counting ideals. — Using Deuring's correspondence, we have:

Proposition 6.1. — *For a fixed triple (E, x, u) satisfying* (2.12)–(2.15),

$$\begin{aligned}&\#\left\{(E', y, b, z) : u = yb^\vee, (x, y, b, z) \text{ satisfying } \ (2.4)-(2.10)\right\}\\ &\qquad = \#\left\{I := \mathrm{Hom}(E', E)\circ b^\vee : \text{ satisfying } (1),(2),(3)\right\}.\end{aligned}$$

The following Theorem gives a formula for the number of left ideals satisfying properties (1), (2), and (3).

Theorem 6.1.1. — *Let E be a supersingular elliptic curve and assume there exists $x, u \in \mathrm{End}(E)$ satisfying* (2.12)–(2.15). *Let $f \in \mathbb{Z}_{>0}$ be such that $\mathbb{Q}(u) \cap \mathrm{End}(E)$ is an order of discriminant $d := \frac{\mathrm{Disc}(u)}{f^2}$. Then*

$$\begin{aligned}\mathfrak{I}(\delta, n, f) &:= \#\left\{(E', y, b, z) : u = yb^\vee, (x, y, b, z) \text{ satisfying } \ (2.4)-(2.10)\right\}\\ &= \prod_{p\mid\delta, p\neq\ell}\left(\sum_{\substack{j=0\\ j\equiv v_p(\delta) \bmod 2}}^{v_p(\delta)} \mathfrak{I}^{(p)}_{j-r_p}(t_w, n_w)\right),\end{aligned}$$

where

$$\begin{aligned}t_w &= \alpha_0 + (D-a)\alpha_1\\ n_w &= \beta_0 + (D-a)\beta_1 + \frac{(n + c_K(\delta))}{2D}\\ r_p &= \max\left(v_p(\delta) - \left\lfloor \frac{1}{2} v_p\left(\mathrm{GCD}(t_w^2, n_w, f^2)\right)\right\rfloor, 0\right)\\ \mathfrak{I}_C(a_1, a_0) = \mathfrak{I}^{(p)}_C(a_1, a_0) &= \begin{cases}\#\{\widetilde{t} \bmod p^C : \widetilde{t}^2 - a_1\widetilde{t} + a_0 \equiv 0 \pmod{p^C}\} & \text{if } C \geq 0,\\ 0 & \text{if } C < 0.\end{cases}\end{aligned}$$

7. Concluding the proof of Main Theorem

Now we resume our proof of Theorem 2.0.1. Recall that we had shown that

$$\frac{(\mathrm{CM}(K).G_1)_\ell}{\log \ell} = \sum_{\substack{\delta\in\mathbb{Z}_{>0}\\ \delta=\frac{D-\square}{4}}} C_\delta \sum_{E_1}\sum_{E_2} \sum_{\substack{x,y,b,z\\ \text{up to iso.}\\ \text{as above}}} \frac{1}{\#\,\mathrm{Aut}(x, y, b, z)} \text{length } \frac{\mathbb{W}[[t_1, t_2]]}{I_{x,y,b,z}}.$$

The arguments in [22, Lemma 3.10] show that $\#\,\mathrm{Aut}(x, y, b, z) = 2$ and [22, Proposition 3.11] shows that the length of $\frac{\mathbb{W}[[t_1,t_2]]}{I_{x,y,b,z}}$ is bounded above by $2\left(\text{length } \frac{\mathbb{W}[[t_1]]}{I_{x,u}}\right)$, and if $\ell\delta$, then

$$\text{length } \frac{\mathbb{W}[[t_1, t_2]]}{I_{x,y,b,z}} = \text{length } \frac{\mathbb{W}[[t_1]]}{I_{x,u}}.$$

Thus it follows that the intersection number can be rewritten as

$$\frac{(\mathrm{CM}(K).G_1)_\ell}{\log \ell} = \sum_{\substack{\delta\in\mathbb{Z}_{>0}\\ \delta=\frac{D-\square}{4}}} C_\delta \sum_{E_1}\sum_{E_2} \sum_{\substack{x,y,b,z\\ \text{up to iso.}\\ \text{as above}}} \frac{1}{\#\,\mathrm{Aut}(x, yb^\vee)} \cdot \text{length } \frac{\mathbb{W}[[t_1]]}{I_{x,yb^\vee}},$$

as long as $\ell\delta$ for any δ, and that

$$\frac{(\mathrm{CM}(K).G_1)_\ell}{\log \ell} \leq \sum_{\substack{\delta\in\mathbb{Z}_{>0}\\ \delta=\frac{D-\square}{4}}} C_\delta \sum_{E_1}\sum_{E_2} \sum_{\substack{x,y,b,z\\ \text{up to iso.}\\ \text{as above}}} \frac{1}{\#\operatorname{Aut}(x, yb^\vee)} \cdot 2\text{length } \frac{\mathbb{W}[[t_1]]}{I_{x,yb^\vee}},$$

for any δ. Using the results from §§5,6 we will rearrange the terms as follows

$$\begin{aligned} I_\ell &:= \sum_{\substack{\delta\in\mathbb{Z}_{>0}\\ \delta=\frac{D-\square}{4}}} C_\delta \sum_{E_1}\sum_{E_2} \sum_{\substack{x,y,b,z\\ \text{up to iso.}\\ \text{as above}}} \frac{1}{\#\operatorname{Aut}(x, yb^\vee)} \cdot \text{length } \frac{\mathbb{W}[[t_1]]}{I_{x,yb^\vee}} \\ &= \sum_{\substack{\delta\in\mathbb{Z}_{>0}\\ \delta=\frac{D-\square}{4}}} C_\delta \sum_{\substack{(E_1,x,u)\\ \text{up to iso.}\\ \text{as above}}} \frac{1}{\#\operatorname{Aut}(x, u)} \text{length } \frac{\mathbb{W}[[t_1]]}{I_{x,u}} \cdot \#\left\{(E', y, b, z) \text{ as above} : u = yb^\vee\right\} \\ &= \sum_{\substack{\delta\in\mathbb{Z}_{>0}\\ \delta=\frac{D-\square}{4}}} C_\delta \sum_{\substack{n\in\mathbb{Z} \text{ s.t.}\\ \frac{\delta^2\widetilde{D}-n^2}{4D}\in\ell\mathbb{Z}_{>0}\\ -n\equiv c_K(\delta) \pmod{2D}}} \varepsilon(n) \sum_{\substack{f\in\mathbb{Z}_{>0}\\ \frac{\delta^2\widetilde{D}-n^2}{4Df^2}\in\ell\mathbb{Z}_{>0}}} \sum_{\substack{(E_1,x,u)\\ \mathrm{Disc}(u)=d_u(n)\\ \mathbb{Q}(u)\cap\mathrm{End}(E)=\mathcal{O}_{d_u(n)/f^2}}} \\ &\qquad \frac{1}{\#\operatorname{Aut}(x, u)} \cdot \text{length } \frac{\mathbb{W}[[t_1]]}{I_{x,u}} \cdot \#\left\{(E', y, b, z) \text{ as above} : u = yb^\vee\right\} \end{aligned}$$

Recall from §6 that

$$\#\left\{(E', y, b, z) \text{ as above} : u = yb^\vee\right\} = \prod_{p\mid\delta, p\neq\ell} \left(\sum_{\substack{j=0\\ j\equiv v_p(\delta) \bmod 2}}^{v_p(\delta)} \mathfrak{I}^{(p)}_{j-r_p}(\mathrm{Tr}(w), \mathrm{N}(w)) \right).$$

By the definition of w and Proposition 5.1, we see that all of the quantities on the right-hand side can be defined in terms of δ, n and f. Thus I_ℓ can be rewritten as

$$\begin{aligned} &= \sum_{\substack{\delta\in\mathbb{Z}_{>0}\\ \delta=\frac{D-\square}{4}}} C_\delta \sum_{\substack{n\in\mathbb{Z} \text{ s.t.}\\ \frac{\delta^2\widetilde{D}-n^2}{4D}\in\ell\mathbb{Z}_{>0}\\ -n\equiv c_K(\delta) \pmod{2D}}} \varepsilon(n) \sum_{\substack{f\in\mathbb{Z}_{>0}\\ \frac{\delta^2\widetilde{D}-n^2}{4Df^2}\in\ell\mathbb{Z}_{>0}}} \mathfrak{I}(\delta, n, f) \cdot \\ &\qquad \left(\sum_{\substack{(E_1,x,u)\,\mathrm{Disc}(u)=d_u(n)\\ \mathbb{Q}(u)\cap\mathrm{End}(E)=\mathcal{O}_{d_u(n)/f^2}}} \frac{1}{\#\operatorname{Aut}(x, u)} \cdot \text{length } \frac{\mathbb{W}[[t_1]]}{I_{x,u}} \right) \end{aligned}$$

By Theorem 5.4.2, this is equal to

$$= \sum_{\substack{\delta\in\mathbb{Z}_{>0}\\ \delta=\frac{D-\square}{4}}} C_\delta \sum_{\substack{n\in\mathbb{Z}\text{ s.t.}\\ \frac{\delta^2\widetilde{D}-n^2}{4D}\in\ell\mathbb{Z}_{>0}\\ -n\equiv c_K(\delta)\pmod{2D}}} \varepsilon(n) \sum_{\substack{f\in\mathbb{Z}_{>0}\\ \frac{\delta^2\widetilde{D}-n^2}{4Df^2}\in\ell\mathbb{Z}_{>0}}} \mathfrak{I}(\delta,n,f)M(\delta,n,f),$$

which completes the proof. □

8. Relationship to Igusa class polynomials

8.1. Igusa invariants and Igusa class polynomials. — One of the immediate applications of the arithmetic intersection formula we have proved is to improve algorithms for computing Igusa class polynomials for generating genus 2 curves for use in cryptography. Roots of Igusa class polynomials are Igusa invariants of genus 2 curves whose Jacobians have CM by a primitive quartic CM field K. Igusa class polynomials can be hard to compute, mostly because provably recovering the rational coefficients from approximations requires a bound on the denominators. Recognizing algebraic numbers, either in $\mathbb{Q}$ or in a number field, is harder than recognizing algebraic integers. Our formula can be used to clear denominators in complex analytic approximations to the Igusa class polynomials, reducing the problem to recognizing integer coefficients. Analogous techniques apply to improving the CRT approach to computing class polynomials, where a multiple of the denominator is needed [7], and to the p-adic approach [9].
Igusa invariants can be defined in terms of modular functions on the Siegel moduli space:

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

where χ_{10} and χ_{12} are Siegel modular cusp forms of weights 10 and 12 which can be expressed in terms of the Siegel-Eisenstein series E_w for $w = 4, 6, 10, 12$ (see [17],[18]).
Igusa class polynomials are the genus 2 analogue of Hilbert class polynomials, defined as follows:

$$H_\ell(X) := \prod_\tau (X - i_\ell(\tau)),\quad \ell = 1, 2, 3, \tag{8.1}$$

where the product is taken over all points τ on the Siegel moduli space such that the associated principally polarized abelian variety has CM by $\mathcal{O}_K$. Igusa class polynomials have rational coefficients [26, Satz 5.8] (as opposed to integral coefficients as in the case of Hilbert class polynomials).
The denominators of Igusa class polynomials are related to arithmetic intersection numbers on the Siegel moduli space of principally polarized abelian surfaces. It is a classical fact that the zero locus of χ_{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 [10, Cor 5.1.2], that if a prime $\mathfrak{p}$ divides the denominator of $(f/\chi_{10}^k)(\tau)$, for τ 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 $\mathfrak{p}$. Computing the order of zeros of χ_{10} is equivalent to

computing the arithmetic intersection number, $\mathrm{div}(\chi_{10}).\mathcal{CM}(K)$, of the divisor of χ_{10} with the cycle of CM points associated to K.
The practical impact of Theorem 2.0.1 is that any of the algorithms [26, 28, 30, 7, 9, 27, 23, 8, 3, 20] to compute minimal polynomials of invariants of genus 2 curves with CM by K can be improved by multiplying by our formula to obtain polynomials with integral coefficients. In all cases, our formula gives an integer multiple of the denominators: even if the restriction that we placed on K is not satisfied, ($\mathcal{O}_K = \mathcal{O}_F[\eta]$), our formula still gives a bound on the denominator because η still has to embed in the endomorphism ring of the product, even if η does not generate all of $\mathcal{O}_K$. Our formula does not take into account any cancellation between primes in the denominator and numerators of Igusa invariants, but in that case our formula still gives a multiple of the denominator.

9. Examples

9.1. Example 1. — $K = \mathbb{Q}(\sqrt{-119 + 28\sqrt{17}})$, $\ell = 7$
In this example we will apply the theorems of this paper to predict the power to which the prime $\ell = 7$ appears in the denominator of the constant terms of the Igusa class polynomials for K. Note that these class polynomials were computed in [11, Section 3.6.3] and so from that calculation we know that $(\mathrm{CM}(K).G_1)_7 = 2$.The class number of K is 2 and the field discriminant is $7^2 \cdot 17^3$, so 7 is a ramified prime in K.
This particular example was chosen to illustrate the fact that there is some subtlety in the formula in the case that N and the conductor of d_u share common factors other than ℓ. At the same time, this example also illustrates the need to compute the expression defined in Theorem 6.1.1 for the number of solutions to the Embedding Problem defined by a pair of endomorphisms x, u.
Writing $\mathcal{O}_K = \mathcal{O}_F[\eta]$, we have $\mathrm{Tr}_{K/F}(\eta) = \alpha_0 + \alpha_1 \frac{D+\sqrt{D}}{2}$, and $\mathrm{N}_{K/F}(\eta) = \beta_0 + \beta_1 \frac{D+\sqrt{D}}{2}$, where $\alpha_0 = 1$, $\alpha_1 = 0$, $\beta_0 = 149$, $\beta_1 = -14$, $D = 17$. The only possible δ values are 4, and 2. For each δ, the only possible value for n where the prime $\ell = 7$ occurs is $n = 0$.
We first consider $\delta = 4$ and $n = 0$; then $d_x(n) = -91$ and $d_u(n) = -56 \cdot 4$.
When $f = 1$, i.e. when $\mathbb{Z}[u]$ is optimally embedded, we want to count ideals of norm $N = 28$. There is 1 ideal of norm 28 of the correct genus, but this ideal does not satisfy the congruence condition. Therefore there are no (x, u) with $\delta = 4$, $n = 0$, and $\mathbb{Z}[u]$ optimally embedded.
When $f = 2$, i.e. when the maximal order containing u is optimally embedded, we want to count ideals of norm 7. There is 1 ideal of norm 7 of the correct genus and it automatically satisfies the congruence condition. So there is one (x, u) with $\delta = 4$, $n = 0$, and the maximal order containing u optimally embedded.
However, there is no left ideal corresponding to an isogeny b. We have $p = 2$, $v(\delta) = 2$. The number of ideals is the number of solutions modulo 2 to $t^2 - t + 9$. This is empty, so there are no left ideals with the desired properties, and thus no solutions to the Embedding Problem (x, y, b, z) with $\delta = 4$, $n = 0$, and $\mathbb{Z}[u]$ not optimally embedded.
Now consider $\delta = 2$: then $d_x(n) = -175$, $d_u(n) = -56$. Since $d_u(n)$ is fundamental, we need only consider when $f = 1$, i.e. when u is optimally embedded. In this case, we want to count ideals of norm 7 of the correct genus; there is exactly 1 of these, so we get one (x, u) with $\delta = 2$, $n = 0$, and u optimally embedded. Now we need to calculate $\#(x, y, b, z)$. We have

$p = 2$, $c = 0$, $r = 1$, and we want to count the number of solutions modulo 1 to $t^2 + t + 2$, which is, of course, 1.
This solution has multiplicity 2, so according to our main theorem, the intersection number at the prime 7 has multiplicity $= 0 + 0 + 2$, which agrees with the prediction coming from the calculation of the Igusa class polynomials.

9.2. Example 2. — $K = \mathbb{Q}(\sqrt{-13 + 3\sqrt{13}})$, $\ell = 23$
This example focuses on a CM field K which does not satisfy the assumptions of the Bruinier-Yang formula, i.e. when D and $\widetilde{D}$ are not primes congruent to 1 mod 4; in this example, $\widetilde{D} = 2^6 13$. For this field, the Bruinier-Yang formula (as stated) underestimates the value of $(\mathrm{CM}(K)\mathbb{G}_1)_{23}$ [16]. Indeed, by van Wamelen the value of $(\mathrm{CM}(K)\mathbb{G}_1)_{23}$ is 4, whereas the value predicted by the Bruinier-Yang formula is 2.
Below we will see that two of the four solutions to the Embedding Problem arise from embeddings into maximal orders in the quaternion algebra in which non-maximal quadratic orders are optimally embedded. This example demonstrates why it was necessary for us to extend (in [21]) the work of Gross-Zagier and Dorman, which described only maximal quaternionic orders with an optimal embedding of a maximal quadratic order.
For this K, the only possible value for δ is 3, and the possible values for n are $n = 52, -52$.
Consider $\delta = 3$, $n = -52$: then $d_x(n) = -8 \cdot 4$, $d_u(n) = -24 \cdot 4$
When $f = 1$, i.e. when $\mathbb{Z}[u]$ is optimally embedded, we want to count ideals of norm 4. There is one ideal of the correct genus multiplicity, and it satisfies the congruence condition, so we get one (x, u). Since $\mathbb{Z}[u]$ is optimally embedded this implies that $c = 0$ and there is one solution to the Embedding Problem (x, y, b, z).
When $f = 2$, i.e. when the maximal order containing u is optimally embedded, we want to count ideals of norm 1. There is one ideal of the correct genus multiplicity and it automatically satisfies the congruence condition, so there is one (x, u). Since f is prime to δ, this implies $c = 0$ and there is one (x, y, b, z).
The case of $\delta = 3$, $n = 52$, with $d_x(n) = -48$, $d_u(n) = -48$, works exactly the same way. Thus there are four solutions to the Embedding Problem, two of which arise from optimal embeddings of non-maximal quadratic orders.

References

[1] Bruinier, J. H, Yang, T., *CM-values of Hilbert modular functions.* Invent. Math., **163**, no. 2, (2006), 229–288.

[2] Cassels, J.W.S, Fröhlich, A., *Algebraic number theory.* Proceedings of an instructional conference organized by the London Mathematical Society (a NATO Advanced Study Institute) with the support of the Inter national Mathematical Union., Academic Press, London, (1967), xviii+366.

[3] Costello, C., Deines-Schartz, A., Lauter, K., Yang, T., *Constructing abelian surfaces for cryptography via Rosenhain invariants.* LMS J. Comput. Math., **17** (Special issue A), (2014), 157–180.

[4] Cox, D. A., *Primes of the form $x^2 + ny^2$*, A Wiley-Interscience Publication, Fermat, class field theory and complex multiplication, John Wiley & Sons Inc., New York, (1989), xiv+351.

[5] Dorman, D. R., *Global orders in definite quaternion algebras as endomorphism rings for reduced CM elliptic curves*, *Conférence Théorie des nombres*, Quebec, PQ, (1987), de Gruyter, Berlin, (1989), 108–116.

[6] Dorman, D. R., *Special values of the elliptic modular function and factorization formulae*, J. Reine Angew. Math., **383**, (1988), 207–220.

[7] Eisenträger, Kirsten, Lauter, K., *A CRT algorithm for constructing genus 2 curves over finite fields*, Proceedings of Arithmetic, Geometry, and Coding Theory, (AGCT-10), Marseille, **Numéro 21**, Société Mathématique de France, (2005), 161–176.

[8] Enge, A., Thomé, E., *Computing class polynomials for abelian surfaces*, Experimental Mathematics, **23**, 129–145, Taylor and Francis, (2014).

[9] Gaudry, P., Houtmann, T., Kohel, D., Ritzenthaler, C., Weng, A., *The 2-adic CM method for genus 2 curves with application to cryptography*, *conference Advances in cryptology—ASIACRYPT 2006*, Lecture Notes in Comput. Sci., **4284**, Springer, Berlin, (2006), 114–129.

[10] Goren, E. Z., Lauter, K. E., *Class invariants for quartic CM fields*, Ann. Inst. Fourier (Grenoble), **57**, (2007), no. 2, 457–480.

[11] Goren, E. Z., Lauter, K. E., *Genus 2 Curves with Complex Multiplication*, International Mathematics Research Notices, (2011), 75 pp..

[12] Goren, E. Z., Lauter, K. E., *A Gross-Zagier formula for quaternion algebras over totally real fields*, Algebra and Number Theory, **Vol. 7**, (2013), no. 6, 1405–1450.

[13] Gross, B. H., *On canonical and quasicanonical liftings*, Invent. Math., **84**, (1986), no. 2, 321–326.

[14] Gross, B. H., Keating, K., *On the intersection of modular correspondences*, Invent. Math., **112**, (1993), 225–245.

[15] Gross, B. H., Zagier, D. B., *On singular moduli*, J. Reine Angew. Math., **355**, (1985), 191–220.

[16] Grundman, H., Johnson-Leung, J., Lauter, K., Salerno, A., Viray, B., Wittenborn, E., *Igusa Class Polynomials, Embeddings of Quartic CM Fields, and Arithmetic Intersection Theory*, WIN–Women in Numbers: Research Directions in Number Theory, Fields Institute Communications, **60**, (2011), 35–60.

[17] Igusa, J., *On Siegel modular forms genus two. II*, Amer. J. Math., **86**, (1964), 392–412.

[18] Igusa, J., *Modular forms and projective invariants*, Amer. J. Math., **89**, (1967), 817–855.

[19] Lang, S., *Elliptic functions*, Graduate Texts in Mathematics, **112**, 2, with an appendix by J. Tate, Springer-Verlag, New York, (1987), xii+326.

[20] Lauter, K., Naehrig, M., Yang, T., *Hilbert theta series and invariants of genus 2 curves*, to appear in Journal of Number Theory.

[21] Lauter, K., Viray, B., *On singular moduli for arbitrary discriminants*, International Mathematics Research Notices, (2014).

[22] Lauter, K., Viray, B., *An arithmetic intersection formula for denominators of Igusa class polynomials*, American Journal of Mathematics, (2014).

[23] Lauter, K., Yang, T., *Computing genus 2 curves from invariants on the Hilbert moduli space*, Journal of Number Theory, Elliptic Curve Cryptography, **131**, issue 5, (2011).

[24] Neukirch, J., *Algebraic number theory*, Grundlehren der Mathematischen Wissenschaften (Fundamental Principles of Mathematical Sciences), **322**, Springer-Verlag, Berlin, (1999), xviii+571.

[25] Serre, J. -P., Tate, J., *Good reduction of abelian varieties*, Ann. of Math. (2), **88**, (1968), 492–517.

[26] Spallek, A. -M., *Kurven vom Geschlecht 2 und ihre Anwendung in Public-Key-Kryptosystemen*, (1994), Universität Gesamthochschule Essen, Ph. D. Thesis.

[27] Streng, M., *Computing Igusa Class Polynomials*, Mathematics of Computation, **83**, (2014), 275–309.

[28] van Wamelen, P., *Examples of genus two CM curves defined over the rationals*, Math. Comp., **68**, no. 225, (1999), 307–320.

[29] Vignéras, M. -F., *Arithmétique des algèbres de quaternions*, Lecture Notes in Mathematics, **800**, Springer, Berlin, (1980), vii+169.

[30] Weng, A., *Constructing hyperelliptic curves of genus 2 suitable for cryptography*, Math. Comp., **72**, (2003), no. 241, 435–458 (electronic).

[31] Yang, T., *Some Interesting Arithmetic Intersection Formulae in Number Theory*, ICCM, **I**, (2007), 534–545.

[32] Yang, T., *Chowla-Selberg Formula and Colmez's Conjecture*, Can. J. Math., **62**, (2010), 456–472.

[33] Yang, T., *An arithmetic intersection formula on Hilbert modular surfaces*, Amer. J. Math., **132**, (2010), 1275–1309.

[34] Yang, T., *Arithmetic intersection on a Hilbert modular surface and the Faltings height*, Asian Journal of Mathematics, **17**, no. 2, 2013, 335–382.

1 décembre 2014

Kristin Lauter, Microsoft Research, 1 Microsoft Way, Redmond, WA 98062, USA • *E-mail :* klauter@microsoft.com
Url : http://research.microsoft.com/en-us/people/klauter/default.aspx

Bianca Viray, Department of Mathematics, Box 1917, Brown University, Providence, RI 02912, USA
E-mail : bviray@math.brown.edu • *Url :* http://math.brown.edu/~bviray