AN ARITHMETIC INTERSECTION FORMULA FOR DENOMINATORS OF IGUSA CLASS POLYNOMIALS

KRISTIN LAUTER AND BIANCA VIRAY

Abstract. In this paper we prove an explicit formula for the arithmetic intersection number $(\mathrm{CM}(K).\mathrm{G}_1)_\ell$ on the Siegel moduli space of abelian surfaces, generalizing the work of Bruinier-Yang and Yang. 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.

Bruinier and Yang conjectured a formula for intersection numbers on an arithmetic Hilbert modular surface, and as a consequence obtained a conjectural formula for the intersection number $(\mathrm{CM}(K).\mathrm{G}_1)_\ell$ under strong assumptions on the ramification of the primitive quartic CM field K. Yang later proved this conjecture assuming that $\mathcal{O}_K$ is freely generated by one element over the ring of integers of the real quadratic subfield. In this paper, we prove a formula for $(\mathrm{CM}(K).\mathrm{G}_1)_\ell$ for more general primitive quartic CM fields, and we use a different method of proof than Yang. We prove a tight bound on this intersection number which holds for *all* primitive quartic CM fields. As a consequence, we obtain a formula for a multiple of the denominators of the Igusa class polynomials for an arbitrary primitive quartic CM field. Our proof entails studying the Embedding Problem posed by Goren and Lauter and counting solutions using our previous article that generalized work of Gross-Zagier and Dorman to arbitrary discriminants.

1. Introduction

For a prime number ℓ, the ℓ-part of the arithmetic intersection number $(\mathrm{CM}(K).\mathrm{G}_1)$ counts, with multiplicity, the number of isomorphism classes of abelian surfaces with CM by a primitive quartic CM field K that reduce modulo ℓ to a product of two elliptic curves with the product polarization. These intersection numbers have been studied in detail by Bruinier-Yang [BY06], Yang [Yan10, Yan], and Goren-Lauter [GL07, GL11]. In this paper, we give an exact formula for this ℓ-part, denoted $(\mathrm{CM}(K).\mathrm{G}_1)_\ell$, under mild assumptions on K, and a tight bound on $(\mathrm{CM}(K).\mathrm{G}_1)_\ell$ for all primitive quartic CM fields K.

The computation of $(\mathrm{CM}(K).\mathrm{G}_1)_\ell$ has applications to the computation of the Igusa class polynomials of K. Igusa class polynomials are polynomials over $\mathbb{Q}$ which are the genus 2 analogue of Hilbert class polynomials; namely, the roots of the Igusa class polynomials of K determine genus 2 curves whose Jacobians have complex multiplication by K. However, in contrast to the genus 1 case, the coefficients of Igusa class polynomials are *not* integral and the presence of denominators makes the computation of these polynomials more difficult. Indeed, all known algorithms to compute Igusa class polynomials require as input some bound on the denominators of the coefficients of the Igusa class polynomials. In addition, the sharpness of the bound directly affects the efficiency of the algorithms. The arithmetic intersection number $\mathrm{CM}(K).\mathrm{G}_1$ gives a method of studying these denominators. In fact,

The second author was partially supported by Microsoft Research, a Ford dissertation year fellowship, NSF grant DMS-1002933, and ICERM.

up to cancellation from the numerators, the ℓ-valuation of the denominators of Igusa class polynomials is exactly a (known) multiple of $(\mathrm{CM}(K).\mathrm{G}_1)_\ell$.

Often, explicit formulas for the arithmetic intersection of CM-cycles with other cycles, such as the Humbert surface, are proved under severe restrictions on the ramification in the CM field K (e.g. [GZ85]). Indeed, Yang proved an explicit formula for $(\mathrm{CM}(K).\mathrm{G}_1)_\ell$ under the assumption that the discriminant of K is of the form $D^2\widetilde{D}$ where D and $\widetilde{D}$ are primes congruent to 1 (mod 4) [Yan10, Yan], and that $\mathcal{O}_K$ is freely generated over the ring of integers of the real quadratic subfield by one element of a certain form.

This explicit formula was originally conjectured, with the assumption on the ramification but without the assumption on $\mathcal{O}_K$, in earlier work of Bruinier and Yang [BY06]. In recent work, the present authors with Grundman, Johnson-Leung, Salerno, and Wittenborn [GJLL$^+$11] showed that the conjecture of Bruinier and Yang does not hold (as stated) if the assumptions on the ramification are relaxed. This gives evidence that, in the general case, the formula *must* be more complicated.

The main result of this paper is an explicitly computable formula for the intersection number $(\mathrm{CM}(K).\mathrm{G}_1)_\ell$, under the same assumption on $\mathcal{O}_K$, for all ℓ outside a small finite set, and a tight upper bound for $(\mathrm{CM}(K).\mathrm{G}_1)_\ell$ in general (§2.1). The dramatically weaker assumptions lead to a formula that is more complicated than that of Bruinier and Yang; however, in many cases it simplifies to a formula that is strikingly similar. We give an example of this in §2.3. As a result of our formula and upper bound, we obtain a formula for a multiple of the denominators of the Igusa class polynomials for every primitive quartic CM field K. We explain this further in §2.2.

Remark. The arithmetic intersection number $\mathrm{CM}(K).\mathrm{G}_1$ was also studied by Howard and Yang [HY12]. They prove, under very mild assumptions, that the values $(\mathrm{CM}(K).\mathrm{G}_1)_\ell$ agree with Fourier coefficients of certain Eisenstein series; however, their work does not give an explicit formula for $(\mathrm{CM}(K).\mathrm{G}_1)_\ell$.

1.1. **Overview of the tools.**

The first part of our proof takes its inspiration from work of Goren and the first author [GL07, GL11] which gave a bound on the denominators appearing in the Igusa class polynomials, first bounding the primes that can appear [GL07], and then bounding the powers [GL11]. Their proof studied necessary conditions for the existence of a solution to the *embedding problem*: the problem of determining whether there is an embedding $\mathcal{O}_K \hookrightarrow \mathrm{End}_{\overline{\mathbb{F}}_\ell}(E_1 \times E_2)$ such that complex conjugation agrees with the Rosati involution associated to the product polarization.

In this paper, we determine conditions that are *equivalent* to the existence of a solution to the embedding problem and use these equivalent conditions to count the number of solutions to the embedding problem. (Yang's proof [Yan10, Yan] also began with a treatment of the embedding problem; however, our formulation of it is different and our methods diverge from Yang's after this step.) First, we show that a solution to the embedding problem gives rise to a supersingular elliptic curve E and endomorphisms $x, u \in \mathrm{End}(E)$ with fixed degree and trace; this is explained in §3.

Next, we count these pairs of endomorphisms using results from our earlier paper [LV] that generalizes work of Gross and Zagier [GZ85]. These results show that the number of pairs (x, u) is equal to a weighted sum of the number of integral ideals in a quadratic imaginary order with a certain norm. This is explained further in §5.

To go from pairs of endomorphisms (x, u) to a solution of the embedding problem, we study isogenies y, b of a fixed degree from an auxiliary elliptic curve E' to E such that $yb^\vee = u$ and such that x, y, and b satisfy an additional relationship depending on K. Using Deuring's correspondence, we translate this to a problem of counting certain ideals in $\mathrm{M}_2(\mathbb{Z}_p)$. We solve this counting problem in §6.

Acknowledgements

The first author thanks Tonghai Yang for explanations of his work [Yan10, Yan]. The second author thanks Ben Howard, Bjorn Poonen, and Joseph H. Silverman for helpful conversations.

2. A formula for $\mathrm{CM}(K) \cdot \mathrm{G}_1$

Notation. We write F for a real quadratic field, and D for the discriminant of the ring of integers $\mathcal{O}_F$. Let K denote a totally imaginary extension of F that does not contain an imaginary quadratic field; K is a *primitive quartic CM field.* We say that an abelian surface A has *CM by* K if there is an embedding of the ring of integers $\mathcal{O}_K$ into the endomorphism ring $\mathrm{End}(A)$. Let $\mathrm{CM}(K)$ denote the moduli stack whose S-points are

$$\left\{ \begin{array}{ll} (A, \iota, \lambda): & A/S \text{ is an abelian surface with principal polarization } \lambda, \\ & \iota\colon \mathcal{O}_K \hookrightarrow \mathrm{End}_S(A), \text{ s.t. } \iota(\overline{\gamma}) = \iota(\gamma)^\vee \end{array} \right\} / \sim$$

where $\phi \mapsto \phi^\vee$ denotes the Rosati involution and $(A, \iota, \lambda) \sim (A', \iota', \lambda')$ if there is an isomorphism of principally polarized abelian surfaces between (A, λ) and (A', λ') that conjugates ι to ι'. There is a finite to one map from $\mathrm{CM}(K)$ to M, the Siegel moduli space of principally polarized abelian surfaces, obtained by sending (A, ι, λ) to (A, λ).

Let η denote a fixed element of $\mathcal{O}_K$ that generates K/F. Often, we will assume that $\mathcal{O}_K$ is freely generated over $\mathcal{O}_F$ and that η is a generator, i.e.,

$$\mathcal{O}_K = \mathcal{O}_F[\eta] \tag{†}$$

We write $\widetilde{D} := \mathrm{N}_{F/\mathbb{Q}}\left(\mathrm{D}_{K/F}(\eta)\right)$ where $\mathrm{D}_{K/F}(\eta)$ denotes the relative discriminant of $\mathcal{O}_F[\eta]$ and we let $\alpha_0, \alpha_1, \beta_0, \beta_1 \in \mathbb{Z}$ be such that $\mathrm{Tr}_{K/F}(\eta) = \alpha_0 + \alpha_1\omega$ and $\mathrm{N}_{K/F}(\eta) = \beta_0 + \beta_1\omega$, where $\omega = \frac{1}{2}(D + \sqrt{D})$. We define

$$c_K := \alpha_0^2 + \alpha_0\alpha_1 D + \frac{1}{4}\alpha_1^2(D^2 - D) - 4\beta_0 - 2\beta_1 D.$$

For any positive integer δ such that $D - 4\delta$ is a square, we define $t_u(\delta) := \alpha_1\delta$ and define $t_x(\delta), t_w(\delta) \in \mathbb{Z}$ to satisfy

$$t_x(\delta) + t_w(\delta) = \alpha_0 + D\alpha_1, \quad t_w(\delta) - t_x(\delta) = \alpha_1\sqrt{D - 4\delta}, \quad \text{where } \sqrt{D - 4\delta} > 0.$$

Then for any integer n such that $2D \mid (n + c_K\delta)$, we define

$$n_u(n) := -\delta \cdot \frac{n + c_K\delta}{2D}, \quad t_{xu^\vee}(n) := \beta_1\delta + \sqrt{D - 4\delta}\frac{n + c_K\delta}{2D},$$

and let $n_x(n), n_w(n) \in \mathbb{Z}$ be such that

$$n_x(n) + n_w(n) = \beta_0 + D\beta_1 - 2n_u(n)/\delta, \quad n_w(n) - n_x(n) = \beta_1\sqrt{D - 4\delta}.$$

We also define $d_*(n) := t_*(n)^2 - 4n_*(n)$ for $* \in \{x, u, w\}$. For any positive integer f_u, set

$$t(n, f_u) = \frac{1}{2f_u^2}(d_x(n)d_u(n) - f_u(t_x t_u - 2t_{xu^\vee}(n))).$$

Since the integer n implicitly depends on a choice of δ, so does anything that depends on n. For simplicity, we omit this dependence on δ in the notation.

The origin of these definitions will become clear in §3; for now, it is enough to note that these values are easily computed once a choice of η is fixed.

Throughout we work with a fixed prime ℓ; we write $\mathbb{B}_{\ell,\infty}$ for the rational quaternion algebra ramified only at ℓ and ∞. For any $\gamma \in \mathbb{B}_{\ell,\infty}$, we let $\gamma^\vee$ denote the image of γ under the natural involution and define $\mathrm{Tr}(\gamma) := \gamma + \gamma^\vee, \mathrm{N}(\gamma) := \gamma\gamma^\vee$.

2.1. **The main result.**

Theorem 2.1. *Assume †. If $\ell \nmid \delta$ for any positive integer δ such that $D - 4\delta$ is a square, then*

$$\frac{(\mathrm{CM}(K).G_1)_\ell}{\log \ell} = \sum_{\substack{\delta \in \mathbb{Z}_{>0} \\ D - 4\delta = \square}} C_\delta \sum_{\substack{n \in \mathbb{Z} \\ \frac{\delta^2 \widetilde{D} - n^2}{4D} \in \ell\mathbb{Z}_{>0} \\ 2D \mid (n + c_K \delta)}} \mu_\ell(n) \sum_{f_u} \mathfrak{I}(n, f_u) \cdot \mathscr{J}\left(d_u(n) f_u^{-2}, d_x(n), t(n, f_u)\right).$$

Otherwise,

$$\frac{(\mathrm{CM}(K).G_1)_\ell}{\log \ell} \leq 2 \sum_{\substack{\delta \in \mathbb{Z}_{>0} \\ D - 4\delta = \square}} C_\delta \sum_{\substack{n \in \mathbb{Z} \\ \frac{\delta^2 \widetilde{D} - n^2}{4D} \in \ell\mathbb{Z}_{>0} \\ 2D \mid (n + c_K \delta)}} \mu_\ell(n) \sum_{f_u} \mathfrak{I}(n, f_u) \cdot \mathscr{J}\left(d_u(n) f_u^{-2}, d_x(n), t(n, f_u)\right).$$

Here $C_\delta = 2$ if $4\delta = D$ and otherwise $C_\delta = 1$, and $\mu_\ell(n) = v_\ell\left(\frac{\delta^2 \widetilde{D} - n^2}{4D}\right)$ if ℓ divides both $d_u(n)$ and $d_x(n)$ and $\mu_\ell(n) = \frac{1}{2}(v_\ell(\frac{\delta^2 \widetilde{D} - n^2}{4D}) + 1)$ otherwise. The sum $\sum_{f_u}$ ranges over positive integers f_u such that $d_u(n)/f_u^2$ is the discriminant of a quadratic imaginary order that is maximal at ℓ. The quantity $\mathscr{J}(d_1, d_2, t)$ is a sum, over isomorphism classes of supersingular elliptic curves modulo ℓ, of a number of pairs of embeddings, precisely $\mathscr{J}(d_1, d_2, t)$ equals

$$\sum_{E/\overline{\mathbb{F}}_\ell} \# \left\{ \begin{array}{ll} (i_1, i_2), i_j \colon \mathbb{Z}\left[\frac{d_j + \sqrt{d_j}}{2}\right] \hookrightarrow \mathrm{End}(E) : & \mathrm{Tr}(i_1(d_1 + \sqrt{d_1}) i_2(d_2 - \sqrt{d_2})) = 4t, \\ & i_1(\mathbb{Q}(\sqrt{d_1})) \cap \mathrm{End}(E) = \mathbb{Z}\left[\frac{d_1 + \sqrt{d_1}}{2}\right] \end{array} \right\} / \, \mathrm{End}(E)^\times.$$

Lastly,

$$\mathfrak{I}(n, f_u) := \prod_{p \mid \delta, p \neq \ell} \left(\sum_{\substack{j=0 \\ j \equiv v_p(\delta) \bmod 2}}^{v_p(\delta)} \mathfrak{I}^{(p)}_{j - r_p}(t_w(n), n_w(n)) \right),$$

where $r_p := \max\left(v_p(\delta) - \min(v_p(f_u), v_p(\frac{d_u(n) - t_u f_u}{2f_u})), 0\right)$ and

$$\mathfrak{I}^{(p)}_C(a_1, a_0) = \begin{cases} \#\{\widetilde{t} \bmod p^C : \widetilde{t}^2 - a_1 \widetilde{t} + a_0 \equiv 0 \pmod{p^C}\} & \text{if } C \geq 0, \\ 0 & \text{if } C < 0. \end{cases}$$

Remark 2.2. *The quantity $\mathscr{J}\,(d_1, d_2, t)$ can be computed, for any given K, via an algorithm presented in* [GJLL$^+$11]*. Additionally, Theorem 2.4 below will give a formula for $\mathscr{J}\,(d_1, d_2, t)$ in most cases, and an upper bound for $\mathscr{J}\,(d_1, d_2, t)$ in the remaining cases, and Conjecture 2.6 and Remark 2.7 give an expression for $\mathscr{J}\,(d_1, d_2, t)$ as a product of local factors which holds in most cases.*

If $\mathcal{O}_K$ is not freely generated over $\mathcal{O}_F$, then the same methods give an upper bound for the arithmetic intersection number.

Theorem 2.3. *For every $\eta \in \mathcal{O}_K$ such that $[\mathcal{O}_K : \mathcal{O}_F[\eta]]$ is relatively prime to ℓ and all primes $p \leq D/4$, we have an upper bound:*

$$\frac{(\mathrm{CM}(K).G_1)_\ell}{\log \ell} \leq 2 \sum_{\substack{\delta \in \mathbb{Z}_{>0} \\ D-4\delta=\square}} C_\delta \sum_{\substack{n \in \mathbb{Z} \\ \frac{\delta^2 \widetilde{D}-n^2}{4D} \in \ell\mathbb{Z}_{>0} \\ 2D \mid (n+c_K\delta)}} \mu_\ell(n) \sum_{f_u} \mathfrak{I}(n, f_u) \cdot \mathscr{J}\left(d_u(n) f_u^{-2}, d_x(n), t(n, f_u)\right),$$

with the notation as in Theorem 2.1.

The quantity $\mathscr{J}\,(d_1, d_2, t)$ is related to the ℓ valuation of $J(d_1, d_2) = \prod_{[\tau_1],[\tau_2]}(j(\tau_1) - j(\tau_2))$. It was considered first in 1985 by Gross and Zagier in the case that d_1 and d_2 are discriminants of imaginary quadratic fields and that d_1 and d_2 are relatively prime [GZ85]. The present authors recently generalized much of [GZ85] to arbitrary discriminants [LV]. As $d_1 = d_u(n) f_u^{-2}$ and $d_2 = d_x(n)$ are not necessarily relatively prime nor necessarily discriminants of *maximal* orders, this generalization is needed to compute $\mathscr{J}\,(d_1, d_2, t)$ and thus to give a formula for $(\mathrm{CM}(K).G_1)_\ell$. Using results from [LV], we obtain the following theorem.

Theorem 2.4. *Fix $n, f_u \in \mathbb{Z}$ as above, set $d_x := d_x(n), d_u := d_u(n), t := t(n, f_u)$, and write $\mathcal{O}_u$ for the quadratic imaginary order of discriminant d_u/f_u^2. If the Hilbert symbol*

$$(d_u, D(n^2 - \delta^2 \widetilde{D}))_p = (d_u, (d_u f_u^{-2} d_x - 2t)^2 - d_u f_u{}^{-2} d_x)_p$$

is equal to -1 for some prime $p \neq \ell$, then $\mathscr{J}\,(d_u f_u^{-2}, d_x, t) = 0$. If $\frac{\delta^2 \widetilde{D}-n^2}{4Df_u^2}$ is coprime to the conductor of $\mathcal{O}_u$, then $\mathscr{J}\,(d_u f_u^{-2}, d_x, t)$ equals

$$2^{\#\{p \,:\, v_p(t) \geq v_p(d_u f_u^{-2}) > 0, p \nmid 2\ell\}} \cdot \tilde{\rho}^{(2)}_{d_u f_u^{-2}}(t, d_x) \cdot \# \left\{ \mathfrak{b} \subseteq \mathcal{O}_u : \mathrm{N}(\mathfrak{b}) = \frac{\delta^2 \widetilde{D} - n^2}{4D\ell f_u^2}, \mathfrak{b} \text{ invertible} \right\}, \quad (2.1)$$

where

$$\widetilde{\rho}^{(2)}_d(s_0, s_1) := \left\{ \begin{array}{ll} 2 & \text{if } d \equiv 12 \bmod 16, s_0 \equiv s_1 \bmod 2 \\ & \text{or if } 8 \mid d, v(s_0) \geq v(d) - 2 \\ 1 & \text{otherwise} \end{array} \right\} \cdot \left\{ \begin{array}{ll} 2 & \text{if } 32 \mid d, 4 \mid (s_0 - 2s_1) \\ 1 & \text{otherwise} \end{array} \right\}.$$

Furthermore, in all cases, $\mathscr{J}\,(d_u f_u^{-2}, d_x, t)$ is bounded above by (2.1) *and there is an algorithm to compute $\mathscr{J}\,(d_u f_u^{-2}, d_x, t)$.*

Remark 2.5. *If $\frac{\delta^2 \widetilde{D}-n^2}{4Df_u^2}$ is coprime to the conductor of $\mathcal{O}_u$, then the quantity*

$$2^{\#\{p \,:\, v_p(t) \geq v_p(d_u f_u^{-2}) > 0, p \nmid 2\ell\}} \cdot \tilde{\rho}^{(2)}_{d_u f_u^{-2}}(t, d_x)$$

simplifies to

$$2^{\#\{p \,:\, p \mid \gcd(N f_u^{-2}, d_u f_u^{-2}), p \nmid \ell\}}$$

where $N = \frac{\delta^2 \widetilde{D} - n^2}{4D}$.

In the case that $\frac{\delta^2 \widetilde{D} - n^2}{4D}$ is coprime to the conductor, we can also express $\mathscr{J}\,(d_u f_u^{-2}, d_x, t)$ as a product of local factors. This expression leads us to the following conjecture.

Conjecture 2.6. *Let d_1 and d_2 be discriminants of quadratic imaginary orders and fix an integer t. Assume that conductor of d_1, the conductor of d_2, and $m := \frac{1}{4}(d_1 d_2 - (d_1 d_2 - 2t)^2)$ have no simultaneous common factor. Then*

$$\mathscr{J}\,(d_1, d_2, t) = \prod_{p|m, p\neq \ell} \begin{cases} 1 + v_p(m) & \left(\frac{d_{(p)}}{p}\right) = 1, p \nmid f_1, \\ 2 & \left(\frac{d_{(p)}}{p}\right) = 1, p|f_1, \text{ or} \\ & p|d_{(p)}, (d_{(p)}, -m)_p = 1, p \nmid f_1 \\ 1 & \left(\frac{d_{(p)}}{p}\right) = -1, p \nmid f_1, v_p(m) \text{ even or} \\ & p|d_{(p)}, (d_{(p)}, -m)_p = 1, p|f_1, v_p(m) = 2 \\ 0 & \text{otherwise,} \end{cases}$$

where $d_{(p)} \in \{d_1, d_2\}$ is such that the quadratic imaginary order of discriminant $d_{(p)}$ is maximal at p and f_1 denotes the conductor of d_1.

Remark 2.7. *This conjecture holds when f_1 and m are coprime; in that case it follows from Theorem 2.4.*

Together, Theorems 2.1 and 2.4 give a sharp bound on $(\mathrm{CM}(K).G_1)_\ell$ for all primes ℓ, and a sharp bound on the primes ℓ such that $(\mathrm{CM}(K).G_1)_\ell \neq 0$. The following Corollary gives a characterization of these primes.

Corollary 2.8. *Assume † and that $(\mathrm{CM}(K).G_1)_\ell \neq 0$. Then there exists a $\delta \in \mathbb{Z}_{>0}$ and $n \in \mathbb{Z}$ such that $D - 4\delta$ is a square, $n \equiv -c_K \delta \pmod{2D}$,*

$$N := \frac{\delta^2 \widetilde{D} - n^2}{4D} \in \ell\mathbb{Z}_{>0}, \quad \text{and} \quad (d_u(n), -N)_p = \begin{cases} 1 & \text{if } p \neq \ell, \\ -1 & p = \ell. \end{cases}$$

Remark 2.9. *One obtains the same corollary even when $\mathcal{O}_K$ is not generated over $\mathcal{O}_F$ by one element, by replacing † with the assumption that $\mathcal{O}_F[\eta]$ is maximal at ℓ and all prime $p \leq D/4$. Note that different choices of $\eta \in \mathcal{O}_K$ result in different values of $\widetilde{D} = \mathrm{N}_{F/\mathbb{Q}}(\mathrm{D}_{K/F}(\eta))$ and each choice results in a valid upper bound.*

Proof. By Theorem 2.1, $(\mathrm{CM}(K).\mathrm{G}_1)_\ell$ is always bounded above by a sum over $\delta \in \mathbb{Z}_{>0}$ such that $D - 4\delta$ is a square and a sum over $n \in \mathbb{Z}$ such that $2D|(n + c_K\delta)$ and such that $N := \frac{\delta^2 \widetilde{D} - n^2}{4D}$ is a positive integer divisible by ℓ. Thus, it remains to show that if $(\mathrm{CM}(K).G_1)_\ell \neq 0$, then

$$(d_u(n), -N)_p = \begin{cases} 1 & \text{if } p \neq \ell, \\ -1 & p = \ell, \end{cases}$$

for some δ, n as above.

We first prove that if n satisfies the above assumptions, then $d_u(n)$ is negative. Since K is a totally imaginary extension of F, the relative discriminant of η is negative under both real embeddings of $F \hookrightarrow \mathbb{R}$. Using the definition of α_i, β_i and c_K, one can check that

$$\mathrm{D}_{K/F}(\eta) = c_K + \alpha_1^2 \frac{D}{2} + \sqrt{D}\left(\alpha_0\alpha_1 + \alpha_1^2\frac{D}{2} - 2\beta_1\right).$$

Recall that $\mathrm{N}_{F/\mathbb{Q}}(\mathrm{D}_{K/F}(\eta)) = \widetilde{D}$, thus $c_K + \alpha_1^2\frac{D}{2} < -\sqrt{\widetilde{D}}$. Now consider

$$d_u(n) = (\alpha_1\delta)^2 + \frac{2\delta(n + c_K\delta)}{D} = \frac{2\delta^2}{D}\left(\alpha_1^2\frac{D}{2} + \frac{n}{\delta} + c_K\right).$$

Since $\delta^2\widetilde{D} - n^2 > 0$, $\frac{n}{\delta}$ is bounded above by $\sqrt{\widetilde{D}}$. Thus $d_u(n) < \frac{2\delta^2}{D}\left(\alpha_1^2\frac{D}{2} + \sqrt{\widetilde{D}} + c_K\right)$. We have already shown that $\alpha_1^2\frac{D}{2} + \sqrt{\widetilde{D}} + c_K < 0$ and $2\delta^2/D$ is clearly positive, so $d_u(n)$ is strictly negative.

Since N is assumed to be positive, $(d_u(n), -N)_\infty = -1$, and so, by the product formula, there exists some prime p such that $(d_u(n), -N)_p = -1$. If $p \neq \ell$, then by Theorem 2.4, $\mathscr{J}(d_u f_u^{-2}, d_x, t) = 0$ for all $f_u \in \mathbb{Z}$. Another application of Theorem 2.1 shows that this implies that $(\mathrm{CM}(K), \mathrm{G}_1)_\ell = 0$. □

2.2. **An application: Denominators of Igusa class polynomials.** One of the important applications of the results in this paper is the computation of Igusa class polynomials. Igusa invariants and Igusa class polynomials are the genus 2 analogues of the j-invariant and the Hilbert class polynomial in genus 1. More precisely, Igusa invariants i_1, i_2, i_3 generate the function field of the coarse moduli space of smooth genus 2 curves, and the Igusa class polynomials $H_{j,K}$, for $j = 1, 2, 3$, are polynomials whose roots are Igusa invariants of genus 2 curves $C/\mathbb{C}$ with an embedding $\iota\colon \mathcal{O}_K \hookrightarrow \mathrm{End}(\mathrm{Jac}(C))$. If a genus 2 curve C has CM by K, then C is defined over $\overline{\mathbb{Q}}$ and all of the Galois conjugates of C also have CM by K. Thus, $H_{j,K} \in \mathbb{Q}[z]$ for all j.

However, in contrast to the genus 1 case, the coefficients of $H_{j,K}$ are *not* integral. Therefore, in order to recover the coefficients from a complex or p-adic approximation, one needs more information on the denominators. The denominators of the coefficients of $H_{j,K}$ divide a (known) multiple of the arithmetic intersection number $\mathrm{CM}(K).\mathrm{G}_1$ (using multiplicative notation) [GL07, GL11, Yan10]. For a precise statement of this divisibility, see [Yan10, §9].

Since Theorems 2.1 and 2.3 give a multiple of and, in many cases, an exact formula for $(\mathrm{CM}(K).\mathrm{G}_1)_\ell$, we obtain a formula for a multiple of the denominators of $H_{j,K}$ for *all* primitive quartic CM fields. Corollary 2.8 also gives a restrictive characterization and bound on the primes that can appear in the denominators.

2.3. **Relationship to the Bruinier-Yang conjecture.** Theorem 2.1 appears strikingly similar to the conjecture of Bruinier and Yang [BY06] which was later proved by Yang [Yan10, Yan]. Here we give a simpler version of our formula, under additional assumptions, which makes the similarity even more apparent.

Theorem 2.10. *Assume †, that $\ell \nmid \delta$ for any positive integer such that $D - 4\delta$ is a square, and that $d_u(n)$ is a fundamental discriminant for any $n \in \mathbb{Z}$ such that $N = \frac{\delta^2\widetilde{D} - n^2}{4D} \in \ell\mathbb{Z}_{>0}$*

and $2D|(n+c_K\delta)$. *Then*

$$\frac{(\mathrm{CM}(K).G_1)_\ell}{\log\ell} = \sum_{\substack{\delta\in\mathbb{Z}_{>0}\\ D-4\delta=\square}} C_\delta \sum_{\substack{n\in\mathbb{Z}\\ \frac{\delta^2\widetilde{D}-n^2}{4D}\in\ell\mathbb{Z}_{>0}\\ 2D|(n+c_K\delta)}} \mu_\ell(n)\tilde{\rho}_{d_u(n)}(N)\tilde{\mathfrak{A}}_{d_u(n)}(N\ell^{-1}),$$

where $C_\delta = \frac{1}{2}$ *if* $D = 4\delta$ *and* $C_\delta = 1$ *otherwise,*

$$\mu_\ell(n) = \begin{cases} v_\ell(N) & \text{if } \ell|\gcd(d_x(n), d_u(n)),\\ \frac{v_\ell(N)+1}{2} & \text{otherwise,}\end{cases} \qquad \tilde{\rho}_d(M) = \begin{cases} 0 & \text{if } (d,-M)_p = -1\\ & \text{for some } p|d, p\neq\ell\\ 2^{\#\{p|\gcd(d,M):p\neq\ell\}} & \text{otherwise,}\end{cases}$$

and $\tilde{\mathfrak{A}}_d(M) := \#\{\mathfrak{b}\subseteq\mathbb{Z}[\frac{d+\sqrt{d}}{2}] : \mathrm{N}(\mathfrak{b}) = M\}$.

The Bruinier-Yang formula sums over the same integers δ and, under the assumption that $D, \widetilde{D} \equiv 1 \bmod 4$ and squarefree, the same integers n (see [ABL$^+$]). Then for a fixed δ and n, the Bruinier-Yang formula is a product of a valuation term and the number of ideals of a fixed norm – the difference is that in Bruinier-Yang the ideals lie in the maximal order of the reflex field of K, rather than in a quadratic imaginary order. In recent work, the present authors and Anderson, Balakrishnan, and Park [ABL$^+$] have shown that the formula from Theorem 2.10 agrees with the Bruinier-Yang formula, under the assumptions required for both formulas, without using Theorem 2.10 or Yang's results [Yan10, Yan].

3. Proof of Theorem 2.1

Since K does not contain an imaginary quadratic field, $\mathrm{CM}(K)$ and G_1 intersect properly [Yan, §3] and so

$$\frac{(\mathrm{CM}(K).G_1)_\ell}{\log\ell} = \sum_{P\in(\mathrm{CM}(K)\cap G_1)(\overline{\mathbb{F}}_\ell)} \frac{1}{\#\operatorname{Aut}(P)}\cdot\text{length }\widetilde{\mathcal{O}}_{G_1\cap\mathrm{CM}(K),P} \tag{3.1}$$

where $\widetilde{\mathcal{O}}_{G_1\cap\mathrm{CM}(K),P}$ is the local ring of $G_1\cap\mathrm{CM}(K)$ at P.

The cycle G_1 parametrizes products of elliptic curves with the product polarization; the Rosati involution induced by this polarization is given by

$$g = \begin{pmatrix} g_{1,1} & g_{1,2}\\ g_{2,1} & g_{2,2}\end{pmatrix} \in \operatorname{End}(E_1\times E_2) \mapsto g^\vee = \begin{pmatrix} g_{1,1}^\vee & g_{2,1}^\vee\\ g_{1,2}^\vee & g_{2,2}^\vee\end{pmatrix} \text{ [GL07, Section 3],}$$

where $g_{i,j}\in\operatorname{Hom}(E_j, E_i)$ and $g_{i,j}^\vee$ denotes the dual isogeny of $g_{i,j}$. Given this definition, one can see that a pair of elliptic curves E_1, E_2, together with an embedding $\iota\colon\mathcal{O}_K\hookrightarrow\operatorname{End}(E_1\times E_2)$ that satisfies $\iota(\overline{\alpha}) = \iota(\alpha)^\vee$, determines a point $P\in(\mathrm{CM}(K)\cap G_1)(\overline{\mathbb{F}}_\ell)$. Conversely, a point $P\in(\mathrm{CM}(K)\cap G_1)(\overline{\mathbb{F}}_\ell)$ determines an *isomorphism class* (E_1, E_2, ι); we say two tuples $(E_1, E_2, \iota\colon\mathcal{O}_K\hookrightarrow\operatorname{End}(E_1\times E_2))$ and $(E_1', E_2', \iota'\colon\mathcal{O}_K\hookrightarrow\operatorname{End}(E_1'\times E_2'))$ are isomorphic if there exists an isomorphism $\psi\colon E_1\times E_2\xrightarrow{\sim}E_1'\times E_2'$ such that

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

When $E_i = E_i'$, then the tuples are isomorphic if and only if there exists a $\psi\in\operatorname{Aut}(E_1\times E_2)$ such that $\psi\circ\iota(\alpha) = \iota'(\alpha)\circ\psi$ for all $\alpha\in\mathcal{O}_K$ and $\psi\psi^\vee = 1$.

Given two elliptic curves E_1, E_2, let $\mathbb{W}[[t_1,t_2]]$ be the deformation space of E_1, E_2, and let $\mathbb{E}_1, \mathbb{E}_2$ be the universal curves over this space. We let $I_{E_1,E_2,\iota} \subset \mathbb{W}[[t_1,t_2]]$ denote the minimal ideal such that there exists an $\widetilde{\iota}\colon \mathcal{O}_K \hookrightarrow \operatorname{End}_{\mathbb{W}[[t_1,t_2]]/I_{E_1,E_2,\iota}}(\mathbb{E}_1, \mathbb{E}_2)$ 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, (3.1) can be rewritten as

$$\frac{(\mathrm{CM}(K).G_1)_\ell}{\log \ell} = \sum_{(E_1,E_2,\iota)/\sim} \frac{1}{\#\operatorname{Aut}(E_1,E_2,\iota)} \cdot \text{length } \frac{\mathbb{W}[[t_1,t_2]]}{I_{E_1,E_2,\iota}}, \tag{3.2}$$

where $\operatorname{Aut}(E_1,E_2,\iota) := \{\sigma \in \operatorname{Aut}(E_1 \times E_2) : \sigma\iota(\alpha)\sigma^\vee = \iota(\alpha)\ \forall \alpha \in \mathcal{O}_K \text{ and } \sigma\sigma^\vee = 1\}$. The condition $\sigma\sigma^\vee = 1$ ensures that σ preserves the product polarization.

Since $\mathcal{O}_K = \mathcal{O}_F[\eta]$, giving an embedding $\iota\colon \mathcal{O}_K \hookrightarrow \operatorname{End}(E_1 \times E_2)$ is equivalent to specifying the image of $\omega = \frac{1}{2}(D + \sqrt{D})$ and η, i.e., specifying two elements Λ_1, Λ_2 in $\operatorname{End}(E_1 \times E_2)$ such that

$$\Lambda_1\Lambda_2 = \Lambda_2\Lambda_1, \quad \Lambda_2 + \Lambda_2^\vee = \alpha_0 + \alpha_1\Lambda_1, \quad \Lambda_2\Lambda_2^\vee = \beta_0 + \beta_1\Lambda_1, \text{ and } \quad \Lambda_1^2 - D\Lambda_1 + \frac{1}{4}(D^2 - D) = 0.$$

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 [GL07, 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 $\operatorname{End}(E_1 \times E_2)$ as 2×2 matrices $(g_{i,j})$ where $g_{i,j} \in \operatorname{End}(E_j, E_i)$ 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 is an integer and x, b, y, z satisfy

$$\begin{aligned} \delta := \mathrm{N}(b) &= \tfrac{D-(D-2a)^2}{4}, & \operatorname{Tr}(x) &= \alpha_0 + a\alpha_1, \\ \operatorname{Tr}(yb^\vee) = \operatorname{Tr}(y^\vee b) &= \mathrm{N}(b)\alpha_1, & \operatorname{Tr}(z) &= \alpha_0 + (D-a)\alpha_1, \\ \mathrm{N}(z) + \mathrm{N}(y) &= \beta_0 + (D-a)\beta_1, & \beta_1 b &= \alpha_1 xb - xy + yz^\vee, \\ \mathrm{N}(x) + \mathrm{N}(y) &= \beta_0 + a\beta_1, & bz &= xb + (D-2a)y. \end{aligned} \tag{3.3}$$

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 $2a \le D$. 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. Define $I := I_{x,y,b,z} \subseteq \mathbb{W}[[t_1,t_2]]$ to be the minimal ideal such that there exists

$$\widetilde{x} \in \operatorname{End}_{\mathbb{W}[[t_1,t_2]]/I}(\mathbb{E}_1), \quad \widetilde{y}, \widetilde{b} \in \operatorname{Hom}_{\mathbb{W}[[t_1,t_2]]/I}(\mathbb{E}_2, \mathbb{E}_1), \quad \text{and } \widetilde{z} \in \operatorname{End}_{\mathbb{W}[[t_1,t_2]]/I}(\mathbb{E}_2)$$

that reduce to x, y, b, and z, respectively, modulo the maximal ideal of $\mathbb{W}[[t_1,t_2]]$. Then it is clear from the definition of (x, y, b, z) that

$$\text{length } \frac{\mathbb{W}[[t_1,t_2]]}{I_{E_1,E_2,\iota}} = \text{length } \frac{\mathbb{W}[[t_1,t_2]]}{I_{x,y,b,z}}.$$

Motivated by the definition of isomorphisms of triples (E_1, E_2, ι) that was given above, we say that two such 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. Thus, $\#\,\mathrm{Aut}(x, y, b, z) = \#\,\mathrm{Aut}(E_1, E_2, \iota)$.

If $4\delta = D$, then this no longer holds. If $E_1 \neq E_2$, then $\#\,\mathrm{Aut}(x, y, b, z) = \#\,\mathrm{Aut}(E_1, E_2, \iota)$ for all ι and corresponding x, y, b, z; however, (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 there are twice as many automorphisms of (E_1, E_2, ι) as there are of (x, y, b, z), where ι is the corresponding embedding. In all cases, we see that for a fixed δ

$$\sum_{E_1, E_2, \iota} \frac{1}{\#\,\mathrm{Aut}(E_1, E_2, \iota)} \cdot \mathrm{length}\ \frac{\mathbb{W}[[t_1, t_2]]}{I_{E_1, E_2, \iota}} = C_\delta \sum_{\substack{E_1, E_2 \\ x, y, b, z}} \frac{1}{\#\,\mathrm{Aut}(x, y, b, z)} \cdot \mathrm{length}\ \frac{\mathbb{W}[[t_1, t_2]]}{I_{x, y, b, z}},$$

where $C_\delta = \frac{1}{2}$ if $4\delta = D$ and 1 otherwise.

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

$$\begin{aligned} \mathrm{Tr}(u) &= \alpha_1 \delta, & \mathrm{Tr}(x) &= \alpha_0 + a\alpha_1, \\ (D - 2a)\,\mathrm{N}(u) + \delta\,\mathrm{Tr}(xu^\vee) &= \beta_1 \delta^2, & \delta\,\mathrm{N}(x) + \mathrm{N}(u) &= \delta\,(\beta_0 + a\beta_1)\,, \end{aligned} \tag{3.4}$$

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 (3.3) on (x, y, b, z). Let $I_{x,u} \subseteq \mathbb{W}[[t_1]]$ be the minimal ideal such that there exists

$$\tilde{x}, \tilde{u} \in \mathrm{End}_{\mathbb{W}[[t_1]]/I_{x,u}}(\mathbb{E}_1)$$

that reduce to x, u respectively modulo the maximal ideal of $\mathbb{W}[[t_1]]$.

The remainder of the proof breaks into four steps.

1. Compute $\sum_{(E,x,u)} \mathrm{length}\ \frac{\mathbb{W}[[t_1]]}{I_{x,u}}$, where the sum ranges over isomorphism classes of (E, x, u) satisfying (3.4)(§3.1),
2. For a fixed (E, x, u) determine the number of isomorphism classes of (E', y, b, z) such that $u = yb^\vee$ and (x, y, b, z), satisfy (3.3) (§3.2),
3. Calculate $\#\,\mathrm{Aut}(x, y, b, z)$ (§3.3).
4. Determine how the length of $\frac{\mathbb{W}[[t_1, t_2]]}{I_{x,y,b,z}}$ relates to the length of $\frac{\mathbb{W}[[t_1]]}{I_{x,u}}$. (§3.4).

As it is not necessarily obvious how the arguments in §§3.1–3.4 come together, we summarize the argument in §3.5.

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

In this section we will compute

$$\sum_{\substack{(E,x,u) \text{ satisfying} \\ (3.4)}} \mathrm{length}\ \frac{\mathbb{W}[[t_1]]}{I_{x,u}},$$

where the sum ranges over one representative from each isomorphism class; we say that (E, x, u) is isomorphic to (E', x', u') if there exists an isomorphism $\psi\colon E \to E'$ such that $\psi \circ x = x' \circ \psi$ and $\psi \circ u = u' \circ \psi$.

First we show that the elements (E, x, u) are naturally partitioned by an integer n and that E is always supersingular.

Proposition 3.1. *Let E be an elliptic curve over $\overline{\mathbb{F}}_\ell$ and assume that there exists endomorphisms x and u of E that satisfy (3.4). Then E is supersingular and there exists an integer n such that*

$$\frac{\delta^2\widetilde{D} - n^2}{4D} \in \ell\mathbb{Z}_{>0}, \text{ and } n + c_K\delta \equiv 0 \pmod{2D}, \tag{3.5}$$

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

Proof. Let $\widetilde{R} := \mathbb{Z} \oplus \mathbb{Z}x \oplus \mathbb{Z}u \oplus \mathbb{Z}xu^\vee$ denote the sub-order of $\operatorname{End}(E)$ generated by x and u and for any element $v \in \operatorname{End}(E)$, write $\mathrm{D}(v) := \operatorname{Tr}(v)^2 - 4\deg(v)$ for the discriminant of the element. A straightforward calculation shows that the discriminant of $\widetilde{R}$ is $\left(\frac{\mathrm{D}(x)\,\mathrm{D}(u) - (\operatorname{Tr}(x)\operatorname{Tr}(u) - 2\operatorname{Tr}(xu^\vee))^2}{4}\right)^2$ and that

$$\mathrm{D}(x)\,\mathrm{D}(u) - (\operatorname{Tr}(x)\operatorname{Tr}(u) - 2\operatorname{Tr}(xu^\vee))^2 = -\,\mathrm{D}(2xu^\vee - \operatorname{Tr}(u)x + \operatorname{Tr}(x)u).$$

Since the discriminant of any endomorphism of E is non-positive, we conclude that

$$\frac{\mathrm{D}(x)\,\mathrm{D}(u) - (\operatorname{Tr}(x)\operatorname{Tr}(u) - 2\operatorname{Tr}(xu^\vee))^2}{4}$$

is a non-negative integer. Now let $n := \frac{-2D\,\mathrm{N}(u)}{\delta} - \delta c_K$. An easy, although tedious, computation shows that

$$\frac{\delta^2\widetilde{D} - n^2}{4D} = \frac{\mathrm{D}(x)\,\mathrm{D}(u) - (\operatorname{Tr}(x)\operatorname{Tr}(u) - 2\operatorname{Tr}(xu^\vee))^2}{4}. \tag{3.6}$$

Since K does not contain an imaginary quadratic field, $\widetilde{D}$ is not a square, and so this quantity must be strictly positive. This implies that $\widetilde{R}$ is rank 4 and so we conclude that E is supersingular and $\widetilde{R}$ is a suborder in $\mathbb{B}_{\ell,\infty}$, the quaternion algebra ramified only at ℓ and infinity. Since ℓ divides the discriminant of any order in $\mathbb{B}_{\ell,\infty}$, we have $\delta^2\widetilde{D} - n^2 \in 4D\ell\mathbb{Z}_{>0}$. This completes the proof of the first assertion. The second assertion follows since

$$\frac{n + c_K\delta}{2D} = \frac{-\,\mathrm{N}(u)}{\delta} = \mathrm{N}(x) - \beta_0 - a\beta_1 \in \mathbb{Z}.$$

□

Remark 3.2. *In* [GL07, p.465]*, Goren and the first author proved that E must be supersingular if K does not contain an imaginary quadratic field. Proposition 3.1 gives another proof of this result.*

Proposition 3.1 shows that the tuples (E, x, u) satisfying (3.4) can be partitioned by integers n satisfying (3.5). By the proof of Proposition 3.1, fixing such an n implies that $\mathrm{N}(u) = n_u(n), \mathrm{N}(x) = n_x(n)$, and $\operatorname{Tr}(xu^\vee) = t_{xu^\vee}(n)$ where

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

The trace of x and u are already determined by δ, so we define $d_u(n) := (\alpha_1\delta)^2 - 4n_u(n)$ and $d_x(n) := (\alpha_0 + a\alpha_1)^2 - 4n_x(n)$. For the rest of the section, we assume that n is a fixed integer satisfying (3.5). We define

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

where $[(E,x,u)]$ denotes the isomorphism class of (E,x,u). We claim that the length of $\mathbb{W}[[t]]/I_{x,u}$ is constant for all $(E,x,u) \in \mathcal{E}$.

Theorem 3.3. *Let $(E,x,u) \in \mathcal{E}$. Then*

$$\text{length } \mathbb{W}[[t]]/I_{x,u} = \begin{cases} v_\ell(\frac{\delta^2\widetilde{D}-n^2}{4D}) & \text{if } \ell | \gcd(d_u(n), d_x(n)), \\ \frac{1}{2}\left(v_\ell(\frac{\delta^2\widetilde{D}-n^2}{4D}) + 1\right) & \text{otherwise.} \end{cases}$$

Proof. First we show that $\mathcal{E} \neq \varnothing$ only if at least one of $d_u(n), d_x(n)$ is the discriminant of a quadratic imaginary order that is maximal at ℓ.

Lemma 3.4. *Let E be a supersingular elliptic curve over $\overline{\mathbb{F}}_\ell$ and let $x, u \in \operatorname{End}(E)$ be endomorphisms satisfying* (3.4)*. Then the indices*

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

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

Proof. Define $w := x + (D-2a)\frac{u}{\delta}$. The conditions (3.4) on x, u imply that

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} a & \delta \\ 1 & D-a \end{pmatrix}, \quad \begin{pmatrix} x & u \\ u/\delta & w \end{pmatrix}, \quad \text{and} \quad \begin{pmatrix} ax+u & \delta x + (D-a)u \\ x + (D-a)u/\delta & (D-a)w + u \end{pmatrix}$$

generate a rank 4 $\mathbb{Z}$-submodule $\widetilde{S} \subseteq \operatorname{M}_2(\mathbb{B}_{\ell,\infty})$ that is isomorphic to $\mathcal{O}_K$ (the isomorphism sends the above matrices to $1, \frac{1}{2}(D+\sqrt{D}), \eta$, and $\frac{1}{2}(D+\sqrt{D})\eta$, respectively). Let p be a prime and let S be any order in $\operatorname{M}_2(\mathbb{B}_{\ell,\infty} \otimes_\mathbb{Q} \mathbb{Q}_p)$ that contains $\widetilde{S}$. Since $\mathcal{O}_K$ is the unique maximal order of K, an integral combination of the matrices above can only be in pS if every coefficient is divisible by p. We will show that if p divides both $[\mathbb{Q}(x) \cap \operatorname{End}(E) : \mathbb{Z}[x]]$ and $[\mathbb{Q}(u) \cap \operatorname{End}(E) : \mathbb{Z}[u]]$, then some p-primitive integral combination of the above matrices is in $p\operatorname{M}_2(\operatorname{End}(E))$, thus arriving at a contradiction.

If p divides $[\mathbb{Q}(x) \cap \operatorname{End}(E) : \mathbb{Z}[x]]$ and $[\mathbb{Q}(u) \cap \operatorname{End}(E) : \mathbb{Z}[u]]$, then

$$\frac{2px - p\operatorname{Tr}(x) + \operatorname{D}(x)}{2p}, \quad \frac{2pu - p\operatorname{Tr}(u) + \operatorname{D}(u)}{2p},$$

are both in $p\operatorname{End}(E)$. Consider the p-primitive combination

$$\frac{\operatorname{D}(u) - p\operatorname{Tr}(u)}{2p} + \left[a - D + \begin{pmatrix} a & \delta \\ 1 & D-a \end{pmatrix}\right] \cdot \left[\frac{\operatorname{D}(x) - p\operatorname{Tr}(x)}{2p} + \begin{pmatrix} x & u \\ u/\delta & w \end{pmatrix}\right].$$

After expanding and rearranging terms, we can express this p-primitive combination as

$$\frac{2pu - p\operatorname{Tr}(u) + \operatorname{D}(u)}{2p} + \frac{2px - p\operatorname{Tr}(x) + \operatorname{D}(x)}{2p}\begin{pmatrix} 2a-D & \delta \\ 1 & 0 \end{pmatrix},$$

which is clearly in $p\operatorname{M}_2(\operatorname{End}(E) \otimes \mathbb{Z}_p)$. This completes the proof of the first statement. By [Vig80, Chap. II, Lemma 1.5] $\operatorname{End}(E) \otimes \mathbb{Z}_\ell$ consists of all integral elements in $\operatorname{End}(E) \otimes \mathbb{Q}_\ell$

so both $\mathbb{Q}(u)\cap\operatorname{End}(E)$ and $\mathbb{Q}(x)\cap\operatorname{End}(E)$ are orders that are maximal at ℓ. Since at most one of $[\mathbb{Q}(x)\cap\operatorname{End}(E):\mathbb{Z}[x]]$ and $[\mathbb{Q}(u)\cap\operatorname{End}(E):\mathbb{Z}[u]]$ are divisible by ℓ, at least one of $\mathbb{Z}[x]$ and $\mathbb{Z}[u]$ is maximal at ℓ, as desired. □

Now we return to the proof of Theorem 3.3. Let $d_1\in\{d_x,d_u\}$ be such that d_1 is the discriminant of a quadratic imaginary order that is maximal at ℓ and such that d_1 has minimal ℓ-valuation; this is possible by the preceding lemma. Let $\omega_1\in\{\frac{1}{2}(d_u-t_u)+u,\frac{1}{2}(d_x-t_x)+x\}$ be such that ω_1 has discriminant d_1. We define d_2, and ω_2 to be such that

$$\{d_1,d_2\}=\{d_u,d_x\},\quad \text{and } \{2\omega_1,2\omega_2\}=\{d_u-t_u+2u,d_x-t_x+2x\}.$$

From these definitions, it is clear that $I_{x,u}=I_{\omega_1,\omega_2}$.

Work of Gross [Gro86] shows that $\mathbb{W}[[t]]/I_{\omega_1}$ is isomorphic to $\mathbb{W}_{d_1}$, the ring of integers in $\mathbb{Q}_\ell(\sqrt{d_1})^{\mathrm{unr}}$. An explicit description of $\operatorname{End}_{\mathbb{W}_{d_1}/\mathfrak{m}^k}(\mathbb{E}\bmod I_{\omega_1})$ (where $\mathfrak{m}$ is the unique maximal order of $\mathbb{W}_{d_1}$) is given in [LV, §6], for all k. Using this description and [LV, Proof of Thm. 3.1], we see that $\omega_2\in\operatorname{End}_{\mathbb{W}_{d_1}/\mathfrak{m}^k}(\mathbb{E}\bmod I_{\omega_1})$ if and only if ℓ^r divides

$$\frac{d_1d_2-(d_1d_2-2\operatorname{Tr}(\omega_1\omega_2^\vee))^2}{4}=\frac{d_xd_u-(t_xt_u-2t_{xu^\vee}(n))^2}{4},\tag{3.7}$$

where $r=k$ if $\ell|d_1$ and $r=2k-1$ otherwise. By the proof of Proposition 3.1, the quantity in (3.7) is equal to $(\delta^2\widetilde{D}-n^2)/(4D)$. Since the length of $\mathbb{W}[[t]]/I_{\omega_1,\omega_2}$ is equal to the maximum k such that $\omega_2\in\operatorname{End}_{\mathbb{W}_{d_1}/\mathfrak{m}^k}(\mathbb{E}\bmod I_{\omega_1})$ this completes the proof. □

Corollary 3.5. *The sum* $\sum_{\substack{(E,x,u)\text{ satisfying}\\(3.4)}}\text{length}\,\frac{\mathbb{W}[[t_1]]}{I_{x,u}}$ *equals*

$$\sum_{\substack{n\in\mathbb{Z}\\ \delta^2\widetilde{D}-n^2\in 4D\ell\mathbb{Z}_{>0}\\ 2D|(n+c_K\delta)}}\#\mathcal{E}(n)\cdot\begin{cases}v_\ell(\frac{\delta^2\widetilde{D}-n^2}{4D}) & \text{if }\ell|\gcd(d_u(n),d_x(n)),\\ \frac{1}{2}\left(v_\ell(\frac{\delta^2\widetilde{D}-n^2}{4D})+1\right) & \text{otherwise.}\end{cases}$$

The remainder of the section will be devoted to the proof of the following proposition.

Proposition 3.6. *Let $n\in\mathbb{Z}$ be such that $\delta^2\widetilde{D}-n^2\in 4D\ell\mathbb{Z}_{>0}$ and $2D|(n+c_K\delta)$. Then*

$$\#\mathcal{E}(n)=\sum_{f_u\in\mathbb{Z}_{>0}}\mathscr{J}(d_u(n)f_u^{-2},d_x(n),t(n,f_u)).$$

Proof. Recall that $\mathscr{J}(d_1,d_2,t)$ equals

$$\sum_{E/\overline{\mathbb{F}}_\ell}\#\left\{\begin{matrix}i_j\colon\mathbb{Z}\left[\frac{d_j+\sqrt{d_j}}{2}\right]\hookrightarrow\operatorname{End}(E): & \operatorname{Tr}(i_1(d_1+\sqrt{d_1})i_2(d_2-\sqrt{d_2}))=4t,\\ & i_1(\mathbb{Q}(\sqrt{d_1}))\cap\operatorname{End}(E)=\mathbb{Z}\left[\frac{d_1+\sqrt{d_1}}{2}\right]\end{matrix}\right\}/\operatorname{End}(E)^\times$$

where the sum ranges over isomorphism classes of elliptic curves. Let $(E,x,u)\in\mathcal{E}(n)$ and set $f_u:=[\mathbb{Q}(u)\cap\operatorname{End}(E):\mathbb{Z}[u]]$. We let $d_1:=d_u(n)f_u^{-2}$ and $d_2:=d_x(n)$. Define two embeddings

$$i_1\colon\mathbb{Z}\left[\frac{d_1+\sqrt{d_1}}{2}\right]\to\operatorname{End}(E),\quad\frac{d_1+\sqrt{d_1}}{2}\mapsto\frac{1}{2f_u^2}\left(2f_uu-f_u\alpha_1\delta+d_u(n)\right),$$

$$i_2\colon\mathbb{Z}\left[\frac{d_2+\sqrt{d_2}}{2}\right]\to\operatorname{End}(E),\quad\frac{d_2+\sqrt{d_2}}{2}\mapsto\frac{1}{2}\left(2x-(\alpha_0+a\alpha_1)+d_x(n)\right).$$

From the definition of f_u and d_j, one can easily check that these maps are well-defined and that $i_1(\mathbb{Q}(\sqrt{d_1}))\cap \mathrm{End}(E)=\mathbb{Z}\left[\frac{d_1+\sqrt{d_1}}{2}\right]$. One also has

$$\begin{aligned}\mathrm{Tr}(i_1(d_1+\sqrt{d_1})i_2(d_2-\sqrt{d_2})) &= \frac{1}{f_u^2}\,\mathrm{Tr}((2f_uu-f_u\alpha_1\delta+d_u(n))\,(2x^\vee-(\alpha_0+a\alpha_1)+d_x(n)))\\ &= \frac{4}{f_u}t_{xu^\vee}(n)-\frac{2}{f_u}t_xt_u+\frac{2d_u(n)d_x(n)}{f_u^2}=4t(n,f_u),\end{aligned}$$

as desired. It is clear that if (E,x,u) and (E,x',u') are isomorphic, then the corresponding embeddings described above differ by conjugation by an element of $\mathrm{End}(E)^\times$. This completes the proof. □

3.2. **Determining the pre-image of** (E,x,u)**.** In this section we prove the following theorem.

Theorem 3.7. *Let E be a supersingular elliptic curve and assume there exists $x,u\in\mathrm{End}(E)$ satisfying* (3.4). *Let $f_u\in\mathbb{Z}_{>0}$ be such that $\mathbb{Q}(u)\cap\mathrm{End}(E)$ is an order of discriminant $d:=\frac{\mathrm{D}(u)}{f_u^2}$. Then*

$$\#\left\{(E',y,b,z): u=yb^\vee,(x,y,b,z)\text{ satisfy }\ (3.3)\right\}=\prod_{p\mid\delta,p\neq\ell}\left(\sum_{\substack{j=0\\ j\equiv v_p(\delta)\bmod 2}}^{v_p(\delta)}\mathfrak{I}^{(p)}_{j-r_p}(\mathrm{Tr}(w),\mathrm{N}(w))\right),$$

where $w:=x+(D-2a)u/\delta$, $r_p:=\max\left(v_p(\delta)-\min(v_p(f_u),v_p(\frac{\mathrm{D}(u)-\mathrm{Tr}(u)f_u}{2f_u})),0\right)$ and

$$\mathfrak{I}^{(p)}_C(a_1,a_0)=\begin{cases}\#\{\widetilde{t}\bmod p^C:\widetilde{t}^2-a_1\widetilde{t}+a_0\equiv 0\pmod{p^C}\} & \text{if } C\geq 0,\\ 0 & \text{if } C<0.\end{cases}$$

Proof. Fix an (E,x,u) satisfying (3.4). Assume that there exists an elliptic curve E', $b,y\in\mathrm{Hom}(E',E)$, and $z\in\mathrm{End}(E')$ such that $u=yb^\vee$, $bz=xb+(D-2a)y$. Then there is a left integral ideal $I:=\mathrm{Hom}(E',E)\circ b^\vee$ of $R:=\mathrm{End}(E)$ which has the following properties:

(1) $\mathrm{N}(I)=\delta$,
(2) $\delta,u\in I$, and
(3) $w:=x+(D-2a)\frac{u}{\delta}\in\mathrm{RO}(I):=\{A\in R\otimes\mathbb{Q}:IA\subseteq I\}$.

In fact, we claim that this map is a bijection (when (E,y,b,z) are considered up to equivalence), so

$$\#\left\{[(E',y,b,z)]:u=yb^\vee,(x,y,b,z)\text{ satisfying }\ (3.3)\right\}=\#\left\{I\subseteq R:\text{ satisfying }(1),(2),(3)\right\}.$$

The proof of this claim relies on Deuring's correspondence between supersingular elliptic curves and ideal is $\mathbb{B}_{\ell,\infty}$; we describe this now. Fix a supersingular elliptic curve $E/\overline{\mathbb{F}}_\ell$, and fix an isomorphism $\psi:\mathrm{End}(E)\xrightarrow{\sim}R\subseteq\mathbb{B}_{\ell,\infty}$, where R is a maximal order. Note that ψ allows us to view elements of $\mathrm{End}(E)\otimes\mathbb{Q}$ as elements of $\mathbb{B}_{\ell,\infty}$. Given an element $\phi\in\mathrm{Hom}(E,E')$, we obtain an embedding $\mathrm{Hom}(E',E)\to\mathrm{End}(E)$ by mapping $f\mapsto f\circ\phi$. Thus we can view $\mathrm{Hom}(E',E)$ as a left ideal of $\mathrm{End}(E)$ or, by using the isomorphism ψ, as a left ideal I of R. In fact, Deuring showed that the map

$$\{(E',\phi:E\to E')\}\to\{\text{left ideals } I \text{ of } R\},\quad (E',\phi)\mapsto\psi(\mathrm{Hom}(E',E)\phi)$$

is surjective. In addition, if $\psi(\operatorname{Hom}(E', E)\phi') = \psi(\operatorname{Hom}(E'', E)\phi')$, then $\phi'' = \varphi' \circ \phi'$, for some $\varphi' \in \operatorname{Isom}(E', E'')$. For a more complete description of this correspondence see Deuring's original article [Deu41] or [Wat69, §§3,4].

The morphism ψ also allows us to view $\operatorname{End}(E')$ as a subring of $\mathbb{B}_{\ell,\infty}$; fix an isogeny $\phi\colon E \to E'$, and consider the map $\psi'\colon \operatorname{End}(E') \to \mathbb{B}_{\ell,\infty}$ that sends an endomorphism f to $\frac{1}{\deg(\phi)}\psi(\phi^\vee \circ f \circ \phi)$. Let $R' = \psi'(\operatorname{End}(E'))$. It is clear that R' is contained in the right order of the ideal $I = \psi(\operatorname{Hom}(E', E)\phi)$, and since R' is a maximal order we must have equality.

Now we return to the proof of the claim. Let $I \subseteq R$ be an ideal satisfying conditions (1), (2), and (3). Then, by the discussion above, there exists an elliptic curve E' and an isogeny $\phi\colon E \to E'$. Let $b := \phi^\vee$. Since I has norm δ, the degree of b is also δ. Since $u \in I$, there exists a $y \in \operatorname{Hom}(E', E)$ such that $yb^\vee = u$; moreover, y is unique. Since $x + (D-2a)u/\delta \in \operatorname{RO}(I)$, there exists a $z \in \operatorname{End}(E')$ such that $bzb^\vee/\delta = x + (D-2a)u/\delta$, or rather that $bz = xb + (D-2a)y$; one can check that this relation uniquely determines z. Thus, given an I that satisfies conditions (1), (2), and (3), we obtain (E', y, b, z) such that $u = yb^\vee$ and (x, y, b, z) satisfy (3.3).

Let E_1', E_2' be elliptic curves and $\phi_i\colon E \to E_i'$ isogenies such that $\operatorname{Hom}(E_i', E)\phi_i = I$. Define $b_i := \phi_i^\vee$. Since $\operatorname{Hom}(E_1', E)\phi_1 = \operatorname{Hom}(E_2', E)\phi_2$, there exists some $\phi_{1,2} \in \operatorname{Isom}(E_1', E_2')$ such that $b_1 = b_2 \circ \phi_{1,2}$. As described above, there exists $y_i \in \operatorname{Hom}(E_i', E)$ and $z_i \operatorname{End}(E_i')$ that are unique such that

$$u = y_i b_i^\vee, \quad b_i z_i = x b_i + (D-2a)y_i.$$

Since $\tilde{y}_1 := y_2 \circ \phi_{1,2}$ and $\tilde{z}_1 := \phi_{1,2}^\vee z_2 \phi_{1,2}$ also satisfy these equations, we have $y_1 = \tilde{y}_1$ and $z_1 = \tilde{z}_1$. Thus (x, y_1, b_1, z_1) is isomorphic to (x, y_2, b_2, z_2). This completes the proof of the claim.

Now we have reduced the problem to a question about ideals in $\mathbb{B}_{\ell,\infty}$.

Theorem 3.8. *Fix R a maximal order in $\mathbb{B}_{\ell,\infty}$. Assume that $x, u \in R$ and $\gamma, \delta \in \mathbb{Z}$ are such that*

$$\operatorname{Tr}(u), \quad \operatorname{N}(u), \quad \text{and} \quad \operatorname{Tr}(xu^\vee) + \gamma\operatorname{N}(u)/\delta \quad \text{are 0 modulo } \delta. \tag{3.8}$$

Define $w := x + \gamma u/\delta$, $c_p \in \mathbb{Z}$ to be such that $up^{-c_p} \in R_p \setminus pR_p$, and $r_p := \max(v_p(\delta) - c_p, 0)$. Assume that for all $p|\delta, p \neq \ell$, either $c_p = 0$ or $\mathbb{Q}_p(p^{r_p}w) \cap (\operatorname{End}(E) \otimes \mathbb{Z}_p) = \mathbb{Z}_p[p^{r_p}w]$. Then $\#\{I \subseteq R : \delta, u \in I, \operatorname{N}(I) = \delta, \text{ and } w := x + \gamma u/\delta \in \operatorname{RO}(I)\}$ equals

$$\prod_{p|\delta, p\neq\ell}\left(\sum_{\substack{j=0 \\ j \equiv v_p(\delta) \pmod 2}}^{v_p(\delta)} \mathfrak{I}_{j-r_p}^{(p)}(\operatorname{Tr}(w), \operatorname{N}(w))\right),$$

where

$$\mathfrak{I}_C^{(p)}(a_1, a_0) = \begin{cases} \#\{\widetilde{t} \bmod p^C : \widetilde{t}^2 - a_1\widetilde{t} + a_0 \equiv 0 \pmod{p^C}\} & \text{if } C \geq 0, \\ 0 & \text{if } C < 0. \end{cases}$$

Since the proof of this theorem is completely independent of the rest of the paper, we defer it until §6. If we show that $x, u, \delta, \gamma = D - 2a$ satisfy the assumptions of Theorem 3.8, and that $c_p = \min(v_p(f_u), v_p(\frac{\operatorname{D}(u) - f_u\operatorname{Tr}(u)}{2f_u}))$, then we can apply Theorem 3.8 to complete the proof of Theorem 3.7

It is clear from (3.4) that the assumptions listed in (3.8) are satisfied; we now prove the claim regarding $p^{r_p}w$.

Lemma 3.9. *Let p be a prime such that $p|\delta$ and $c_p \neq 0$. Then*

$$\mathbb{Q}_p(p^{r_p}w) \cap (\mathrm{End}(E) \otimes \mathbb{Z}_p) = \mathbb{Z}_p[p^{r_p}w].$$

Proof. From the definition of c_p, it is clear that $\tilde{w} := p^{r_p}w \in (\mathrm{End}(E) \otimes \mathbb{Z}_p)$. If $\mathrm{D}(\tilde{w})$ has trivial conductor, then the result is immediate. Assume that $\mathrm{D}(\tilde{w})$ has non-trivial conductor. Then $\mathbb{Q}_p(\tilde{w}) \cap (\mathrm{End}(E) \otimes \mathbb{Z}_p) \neq \mathbb{Z}_p[\tilde{w}]$ if and only if $\frac{\tilde{w}}{p} + \frac{\mathrm{D}(\tilde{w}) - p\,\mathrm{Tr}(w)}{2p^2} \in \mathrm{End}(E) \otimes \mathbb{Z}_p$.

First assume that $r_p > 0$. Since w is integral $p^2|\,\mathrm{D}(\tilde{w})$ and $p|\,\mathrm{Tr}(\tilde{w})$. Thus

$$\frac{\tilde{w}}{p} + \frac{\mathrm{D}(\tilde{w}) - p\,\mathrm{Tr}(w)}{2p^2} \in \mathrm{End}(E) \otimes \mathbb{Z}_p$$

if and only if $\frac{\tilde{w}}{p} \in \mathrm{End}(E) \otimes \mathbb{Z}_p$, which in turn is equivalent to $\frac{1}{p}(D-2a)\frac{u}{p^{c_p}}\frac{p^{v(\delta)}}{\delta} \in \mathrm{End}(E) \otimes \mathbb{Z}_p$. By definition of c_p, this occurs if and only if $p|D-2a$. Assume that p is odd. Since D is the discriminant of a real quadratic field $v_p(D) \leq 1$, so either $p \nmid D-2a$ or $v_p(\delta) = 1$. However, if $r_p > 0$ and $c_p \neq 0$, then $v_p(\delta) \geq 2$. Therefore $p \nmid D-2a$ and hence $\mathbb{Q}_p(p^{r_p}w) \cap (\mathrm{End}(E) \otimes \mathbb{Z}_p) = \mathbb{Z}_p[p^{r_p}w]$. If $p = 2$, then a similar calculation gives the same result.

Now assume that $r_p = 0$. This case will be similar to the proof of Lemma 3.4. Consider the element

$$\left[-a + \begin{pmatrix} a & \delta \\ 1 & D-a \end{pmatrix}\right] \cdot \left[\frac{\mathrm{D}(w) - p\,\mathrm{Tr}(w)}{2p} + \begin{pmatrix} x & u \\ u/\delta & w \end{pmatrix}\right] = \begin{pmatrix} u & \delta w' \\ w' & u + (D-2a)w' \end{pmatrix}$$

in $\mathrm{M}_2(\mathrm{End}(E))$, where $w' = w + \frac{\mathrm{D}(w) - p\,\mathrm{Tr}(w)}{2p}$. If $\mathbb{Q}_p(\tilde{w}) \cap (\mathrm{End}(E) \otimes \mathbb{Z}_p) \neq \mathbb{Z}_p[\tilde{w}]$, then this element is in $p\,\mathrm{M}_2(\mathrm{End}(E))$. However,

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} a & \delta \\ 1 & D-a \end{pmatrix}, \quad \begin{pmatrix} x & u \\ u/\delta & w \end{pmatrix}, \quad \text{and} \quad \begin{pmatrix} ax + u & \delta x + (D-a)u \\ x + (D-a)u/\delta & (D-a)w + u \end{pmatrix}$$

generate a rank 4 algebra that is isomorphic to $\mathcal{O}_K$ so a p-primitive integral combination of these elements can never be in $p\,\mathrm{M}_2(\mathrm{End}(E))$. Thus $\mathbb{Q}_p(\tilde{w}) \cap (\mathrm{End}(E) \otimes \mathbb{Z}_p) = \mathbb{Z}_p[\tilde{w}]$. □

Now we turn to the computation of c_p. By the definition of f_u,

$$\mathbb{Q}_p(u) \cap (\mathrm{End}(E) \otimes \mathbb{Z}_p) = \mathbb{Z}_p\left[\frac{u}{f_u} + \frac{\mathrm{D}(u) - f_u\,\mathrm{Tr}(u)}{2f_u^2}\right].$$

Since

$$\frac{u}{p^s} = \frac{f_u}{p^s}\left(\frac{u}{f_u} + \frac{\mathrm{D}(u) - f_u\,\mathrm{Tr}(u)}{2f_u^2}\right) - \frac{\mathrm{D}(u) - f_u\,\mathrm{Tr}(u)}{2f_u p^s},$$

it is clear that $\frac{u}{p^s} \in \mathrm{End}(E) \otimes \mathbb{Z}_p$ if and only if $s \leq v_p(f_u)$ and $s \leq v_p(\frac{\mathrm{D}(u) - f_u\,\mathrm{Tr}(u)}{2f_u p^s})$. Since c_p is the maximal s such that $u/p^s \in \mathrm{End}(E) \otimes \mathbb{Z}_p$, this completes the proof of Theorem 3.7. □

3.3. Computing $\#\,\mathrm{Aut}(x, y, b, z)$.

Lemma 3.10. *Fix elliptic curves E_1, E_2 and assume there exist isogenies $x \in \mathrm{End}(E_1), z \in \mathrm{End}(E_2)$, and $y, b \in \mathrm{Hom}(E_2, E_1)$ satisfying* (3.3). *Then $\#\,\mathrm{Aut}(x, y, b, z) = 2$.*

Proof. Recall that

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

It is clear that there is a homomorphism $\mathrm{Aut}(x,y,b,z) \to \mathrm{Aut}(x, yb^\vee)$, $\quad (\phi_1,\phi_2) \mapsto \phi_1$. Similarly we obtain a homomorphism

$$\mathrm{Aut}(x,y,b,z) \to \mathrm{Aut}(z, b^\vee y) := \{\phi \in \mathrm{Aut}(E) : \phi z = z\phi, \phi b^\vee y = b^\vee y \phi\},$$

that sends $(\phi_1,\phi_2) \mapsto \phi_2$. Therefore, we have an embedding

$$\mathrm{Aut}(x,y,b,z) \hookrightarrow \mathrm{Aut}(x, u := yb^\vee) \times \mathrm{Aut}(z, u^* := b^\vee y).$$

The proof of Proposition 3.1 shows that x, u generate a sub-order of $\mathrm{End}(E_1)$ of finite index and that $\mathrm{End}(E_1)$ is rank 4. The same argument can be applied to $z, u^* = b^\vee y \in \mathrm{End}(E_2)$ to show that these elements generate a sub-order of $\mathrm{End}(E_2)$ of finite index and that $\mathrm{End}(E_2)$ is rank 4. Thus, $\mathrm{Aut}(x,u) \subseteq Z(\mathrm{End}(E_1))^\times$ and $\mathrm{Aut}(z,u^*) \subseteq Z(\mathrm{End}(E_2)^\times)$ where $Z(A)$ denotes the center of A. Since the center of $\mathrm{End}(E_i)$ is just $\mathbb{Z}$, we see that $\mathrm{Aut}(x,u) = \mathrm{Aut}(z,u^*) = \{\pm 1\}$. Using the embedding above, it is easy to check that $\mathrm{Aut}(x,y,b,z) = \{\pm(1,1)\}$. □

3.4. **Relating multiplicities.** Fix elliptic curves E_1, E_2, and isogenies $x \in \mathrm{End}(E)$, $y, b \in \mathrm{Hom}(E_2, E_1)$, and $z \in \mathrm{End}(E_2)$ satisfying (3.3). Let $I_z \subseteq \mathbb{W}[[t_1,t_2]]$ be the minimal ideal such that there exists an isogeny $\widetilde{z} \in \mathrm{End}_{\mathbb{W}[[t_1,t_2]]/I_{x,y,b,z}}(\mathbb{E}_2)$ that reduces to z modulo the maximal ideal of $\mathbb{W}[[t_1,t_2]]$ and define I_{u^*} similarly where $u^* := b^\vee y$. Since z, u^* are endomorphisms of E_1, we can view I_z, I_{u^*} as ideals of $\mathbb{W}[[t_2]]$; similarly we may view $I_{x,u}$ as an ideal of $\mathbb{W}[[t_1]]$.

Proposition 3.11. *The length of* $\frac{\mathbb{W}[[t_1,t_2]]}{I_{x,y,b,z}}$ *is bounded above by* $2\left(\text{length } \frac{\mathbb{W}[[t_1]]}{I_{x,u}}\right)$. *If* $\ell \nmid \delta$, *then*

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

Proof. By the same argument used in Lemma 3.4 applied to z, u^* instead of x, u, either $\mathbb{Z}[z]$ or $\mathbb{Z}[u^*]$ is an order that is maximal at ℓ. If $\mathbb{Z}[z]$ is maximal at ℓ, then define $J := I_z$; otherwise define $J := I_{u^*}$. By definition of $I_{x,y,b,z}, I_{x,u}$, and J, we have the containments $I_{x,u}, J \subseteq I_{x,y,b,z}$. Therefore, we have a surjection

$$\frac{\mathbb{W}[[t_1,t_2]]}{I_{x,u}+J} \twoheadrightarrow \frac{\mathbb{W}[[t_1,t_2]]}{I_{x,y,b,z}}.$$

This gives

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

By [Gro86], J is generated by a linear or quadratic monic polynomial in t_2. Thus

$$\text{length } \frac{\mathbb{W}[[t_1,t_2]]}{I_{x,u}+J} \leq 2\left(\text{length } \frac{\mathbb{W}[[t_1]]}{I_{x,u}}\right).$$

This completes the first half of the proof.

Now we assume that $\ell \nmid \delta$. Since $\deg(b) = \delta$ is prime to ℓ, b gives an isomorphism between the formal groups of E_1 and E_2. Then the argument is exactly the same as in [GK93, Proof of Lemma 5.5]. □

3.5. **Summary.** Now we resume our proof of Theorem 2.1. Recall that we had shown that

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

The argument in §3.3 and Proposition 3.11 show that

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

and if $\ell \nmid \delta$, then

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

Using the results from §§3.1–3.4 we will rearrange the terms as follows

$$\begin{aligned}
&\frac{1}{2}\sum_{\substack{\delta\in\mathbb{Z}_{>0}\\ D-4\delta=\square}} C_\delta \sum_{E_1}\sum_{E_2} \sum_{\substack{x,y,b,z\\ \text{up to iso.}\\ \text{as above}}} \text{length}\ \frac{\mathbb{W}[[t_1]]}{I_{x,yb^\vee}}\\
&= \frac{1}{2}\sum_{\substack{\delta\in\mathbb{Z}_{>0}\\ D-4\delta=\square}} C_\delta \sum_{\substack{[(E_1,x,u)]\\ \text{as above}}} \text{length}\ \frac{\mathbb{W}[[t_1]]}{I_{x,u}}\cdot \#\left\{(E_2,y,b,z) \text{ as above} : u = yb^\vee\right\}\\
&= \frac{1}{2}\sum_{\substack{\delta\in\mathbb{Z}_{>0}\\ D-4\delta=\square}} C_\delta \sum_{\substack{n\in\mathbb{Z}\text{ s.t.}\\ \frac{\delta^2\widetilde{D}-n^2}{4D}\in\ell\mathbb{Z}_{>0}\\ 2D\mid(n+c_K\delta)}} \mu_\ell(n) \sum_{[(E_1,x,u)]\in\mathcal{E}(n)} \#\left\{(E_2,y,b,z) \text{ as above} : u = yb^\vee\right\}\\
&= \frac{1}{2}\sum_{\substack{\delta\in\mathbb{Z}_{>0}\\ D-4\delta=\square}} C_\delta \sum_{\substack{n\in\mathbb{Z}\text{ s.t.}\\ \frac{\delta^2\widetilde{D}-n^2}{4D}\in\ell\mathbb{Z}_{>0}\\ 2D\mid(n+c_K\delta)}} \mu_\ell(n) \sum_{f_u\in\mathbb{Z}_{>0}} \sum_{\substack{[(E_1,x,u)]\in\mathcal{E}(n)\\ [\mathbb{Q}(u)\cap\mathrm{End}(E_1):\mathbb{Z}[u]]=f_u}} \#\left\{(E_2,y,b,z) \text{ as above} : u = yb^\vee\right\}\\
&= \frac{1}{2}\sum_{\substack{\delta\in\mathbb{Z}_{>0}\\ D-4\delta=\square}} C_\delta \sum_{\substack{n\in\mathbb{Z}\text{ s.t.}\\ \frac{\delta^2\widetilde{D}-n^2}{4D}\in\ell\mathbb{Z}_{>0}\\ 2D\mid(n+c_K\delta)}} \mu_\ell(n) \sum_{f_u\in\mathbb{Z}_{>0}} \mathfrak{I}(n,f_u) \sum_{\substack{[(E_1,x,u)]\in\mathcal{E}(n)\\ [\mathbb{Q}(u)\cap\mathrm{End}(E_1):\mathbb{Z}[u]]=f_u}} 1\\
&= \frac{1}{2}\sum_{\substack{\delta\in\mathbb{Z}_{>0}\\ D-4\delta=\square}} C_\delta \sum_{\substack{n\in\mathbb{Z}\text{ s.t.}\\ \frac{\delta^2\widetilde{D}-n^2}{4D}\in\ell\mathbb{Z}_{>0}\\ 2D\mid(n+c_K\delta)}} \mu_\ell(n) \sum_{f_u\in\mathbb{Z}_{>0}} \mathfrak{I}(n,f_u)\mathscr{J}(d_u(n)f_u^{-2}, d_x(n), t(n,f_u)).
\end{aligned}$$

This completes the proof of Theorem 2.1. □

4. Proof of Theorem 2.3

If η is any element of $\mathcal{O}_K \setminus \mathcal{O}_F$, then given any embedding $\iota\colon \mathcal{O}_K \hookrightarrow \mathrm{End}(E_1\times E_2)$ we can restrict the domain to obtain an embedding $\iota|_{\mathcal{O}_F[\eta]}\colon \mathcal{O}_F[\eta] \hookrightarrow \mathrm{End}(E_1\times E_2)$. From the definition of $I_{E_1,E_2,\iota} \subseteq \mathbb{W}[[t_1,t_2]]$, it is clear that

$$\text{length}\ \frac{\mathbb{W}[[t_1,t_2]]}{I_{E_1,E_2,\iota}} \leq \text{length}\ \frac{\mathbb{W}[[t_1,t_2]]}{I_{E_1,E_2,\iota|_{\mathcal{O}_F[\eta]}}}.$$

Since the center of $\operatorname{End}(E_1 \times E_2) \otimes \mathbb{Q}$ is exactly $\mathbb{Q}$, it is also clear that

$$\operatorname{Aut}(E_1, E_2, \iota) = \operatorname{Aut}(E_1, E_2, \iota|_{\mathcal{O}_F[\eta]}).$$

If $\iota \colon \mathcal{O}_F[\eta] \hookrightarrow \operatorname{End}(E_1 \times E_2)$ is any embedding (ι may or may not arise as the restriction of an embedding $\mathcal{O}_K \hookrightarrow \operatorname{End}(E_1 \times E_2)$), then

$$\frac{1}{\#\operatorname{Aut}(E_1,E_2,\iota)} \cdot \text{length}\ \frac{\mathbb{W}[[t_1,t_2]]}{I_{E_1,E_2,\iota}}$$

is positive. Therefore

$$(\mathrm{CM}(K).\mathrm{G}_1)_\ell = \sum_{\substack{E_1,E_2 \\ \iota\colon \mathcal{O}_K \hookrightarrow \operatorname{End}(E_1\times E_2)}} \frac{1}{\#\operatorname{Aut}(E_1,E_2,\iota)} \cdot \text{length}\ \frac{\mathbb{W}[[t_1,t_2]]}{I_{E_1,E_2,\iota}} \tag{4.1}$$

is bounded above by

$$\sum_{\substack{E_1,E_2 \\ \iota\colon \mathcal{O}_F[\eta] \hookrightarrow \operatorname{End}(E_1\times E_2)}} \frac{1}{\#\operatorname{Aut}(E_1,E_2,\iota)} \cdot \text{length}\ \frac{\mathbb{W}[[t_1,t_2]]}{I_{E_1,E_2,\iota}}. \tag{4.2}$$

We compute (4.2) in the same way that we computed (4.1). As long as η generates an order that is maximal at ℓ and all primes $p|\delta$ where δ is any positive integer such that $D-4\delta$ is a square, the entire proof goes through verbatim with the exception of Lemma 3.4.

When η does not generate the full maximal order $\mathcal{O}_K$, the arguments in the proof of Lemma 3.4 prove the following slightly weaker lemma:

Lemma 4.1. *Let E be a supersingular elliptic curve over $\overline{\mathbb{F}}_\ell$ and let $x, u \in \operatorname{End}(E)$ be endomorphisms satisfying* (3.4)*. Then greatest common divisor of the indices*

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

is supported only at primes dividing $[\mathcal{O}_K : \mathcal{O}_F[\eta]]$. In particular, if $[\mathcal{O}_K : \mathcal{O}_F[\eta]]$ is coprime to ℓ, then at least one of $\mathbb{Z}[x]$, $\mathbb{Z}[u]$ is a quadratic imaginary order maximal at ℓ.

As the rest of the proof only requires that at least one of $\mathbb{Z}[x]$ and $\mathbb{Z}[u]$ is maximal at ℓ and that any $p|\delta \leq D/4$ does not divide both $[\mathbb{Q}(x) \cap \operatorname{End}(E) : \mathbb{Z}[x]]$ and $[\mathbb{Q}(u) \cap \operatorname{End}(E) : \mathbb{Z}[u]]$, this lemma, together with our assumption on η, suffices to complete the proof of Theorem 2.3. □

5. Embeddings of imaginary quadratic orders into endomorphism rings of supersingular elliptic curves

In this section, we prove Theorem 2.4 which we restate here for the reader's convenience.

Theorem. *Fix $n, f_u \in \mathbb{Z}$ as above, set $d_x := d_x(n), d_u := d_u(n), t := t(n, f_u)$, and write $\mathcal{O}_u$ for the quadratic imaginary order of discriminant d_u/f_u^2. If the Hilbert symbol*

$$(d_u, D(n^2 - \delta^2 \widetilde{D}))_p = (d_u, (d_u f_u^{-2} d_x - 2t)^2 - d_u f_u{}^{-2} d_x)_p$$

is equal to -1 *for some prime* $p \neq \ell$*, then* $\mathscr{J}(d_u f_u^{-2}, d_x, t) = 0$*. Otherwise* $\mathscr{J}(d_u f_u^{-2}, d_x, t)$ *is bounded above by*

$$2^{\#\{p\,:\,v_p(t)\geq v_p(d_u f_u^{-2})>0, p\nmid 2\ell\}} \cdot \tilde{\rho}^{(2)}_{d_u f_u^{-2}}(t, d_2) \cdot \# \left\{ \mathfrak{b} \subseteq \mathcal{O}_u : \mathrm{N}(\mathfrak{b}) = \frac{\delta^2 \widetilde{D} - n^2}{4D\ell f_u^2}, \mathfrak{b} \text{ invertible} \right\},$$

where

$$\widetilde{\rho}_d^{(2)}(s_0, s_1) := \left\{ \begin{array}{ll} 2 & \text{if } d \equiv 12 \bmod 16, s_0 \equiv s_1 \bmod 2 \\ & \text{or if } 8 \mid d, v(s_0) \geq v(d) - 2 \\ 1 & \text{otherwise} \end{array} \right\} \cdot \left\{ \begin{array}{ll} 2 & \text{if } 32 \mid d, 4 \mid (s_0 - 2s_1) \\ 1 & \text{otherwise} \end{array} \right\}.$$

Furthermore, we have equality in the case that $\frac{\delta^2 \widetilde{D} - n^2}{4Df_u^2}$ *is coprime to the conductor of* $\mathcal{O}_u$ *and, in all cases, there is an algorithm to compute* $\mathscr{J}(d_u f_u^{-2}, d_x, t)$*.*

5.1. **Background.** The proof of Theorem 2.4 relies heavily on results proved in [LV]. We state the relevant results here and summarize the main ideas of the proofs. The interested reader is referred to [LV] for the details.

Let d_1 and d_2 be discriminants of quadratic imaginary orders and assume that the quadratic imaginary order of discriminant d_1 is maximal at ℓ. Write f_i for the conductor of the order of discriminant d_i. For every $\mathrm{SL}_2(\mathbb{Z})$-class of elements in the upper half plane with discriminant d_1, we fix a representative τ_1. Let $E(\tau_1)/\overline{\mathbb{Q}}_\ell$ be the elliptic curve with j-invariant $j(\tau_1)$. We may assume that $E(\tau_1)$ has good reduction and write $\overline{E(\tau_1)}$ for the reduced elliptic curve over $\overline{\mathbb{F}}_\ell$. We fix an isomorphism $i_{\tau_1} : \mathbb{Z}[\frac{1}{2}(d_1 + \sqrt{d_1})] \xrightarrow{\sim} \mathrm{End}(E(\tau_1))$ and let $\omega_1 \in \mathrm{End}(E(\tau_1))$ denote the image of $\frac{1}{2}(d_1 + \sqrt{d_1})$ in $\mathrm{End}(E(\tau_1))$ under this isomorphism.

Consider the following set

$$\coprod_{[\tau_1]} \left\{ \begin{array}{ll} \phi \in \mathrm{End}(\overline{E(\tau_1)}) : & \mathrm{Tr}(\phi) = d_2, \mathrm{N}(\phi) = \frac{1}{4}(d_2^2 - d_2), \\ & \mathrm{Tr}(\omega_1 \cdot \phi^\vee) = t, \mathbb{Q}(\phi) \cap \mathrm{End}(\overline{E(\tau_1)}) = \mathbb{Z}[\phi] \end{array} \right\} \tag{5.1}$$

By [LV, Thm. 3.1 and proof of Thm. 3.1], we have:

Theorem 5.1. *Assume that* $d_1 d_2 \neq (d_1 d_2 - 2t)^2$*. If the Hilbert symbol*

$$(d_2, (d_1 d_2 - 2t)^2 - d_1 d_2)_p$$

is equal to -1 *for some prime* $p \neq \ell$*, then* (5.1) *is empty. Otherwise the cardinality of* (5.1) *is bounded above by*

$$2^{\#\{p\,:\,v_p(t)\geq v_p(d_1)>0, p\nmid 2\ell\}} \cdot \tilde{\rho}_{d_1}(t, d_2) \cdot \mathfrak{A}\left(\frac{1}{4}(d_1 d_2 - (d_1 d_2 - 2t)^2) \right),$$

where

$$\widetilde{\rho}_d^{(2)}(s_0, s_1) := \left\{ \begin{array}{ll} 2 & \text{if } d \equiv 12 \bmod 16, s_0 \equiv s_1 \bmod 2 \\ & \text{or if } 8 \mid d, v(s_0) \geq v(d) - 2 \\ 1 & \text{otherwise} \end{array} \right\} \cdot \left\{ \begin{array}{ll} 2 & \text{if } 32 \mid d, 4 \mid (s_0 - 2s_1) \\ 1 & \text{otherwise} \end{array} \right\}.$$

and

$$\mathfrak{A}(N) = \# \left\{ \begin{array}{ll} & \mathrm{N}(\mathfrak{b}) = N, \mathfrak{b} \text{ invertible}, \\ \mathfrak{b} \subseteq \mathcal{O}_{d_1} : & p \nmid \mathfrak{b} \text{ for all } p | \gcd(N, f_2), p \nmid \ell d_1 \\ & \mathfrak{p}^3 \nmid \mathfrak{b} \text{ for all } \mathfrak{p} | p | \gcd(N, f_2, d_1), p \neq \ell \end{array} \right\}.$$

Furthermore, this upper bound is an equality in the case that $\frac{d_1d_2-(d_1d_2-2t)^2}{4}$ *is coprime to the conductor of* $\mathcal{O}_{d_1}$ *and, in all cases, there is an algorithm to compute the cardinality of* (5.1).

Idea of proof: A calculation shows that the discriminant of the suborder $R := \mathbb{Z}[\omega_1] \oplus \mathbb{Z}[\omega_1]\phi$ is $(\frac{1}{4}(d_1d_2 - (d_1d_2-2t)^2))^2$. Since, by assumption, this quantity is nonzero, the suborder R has rank 4 and so must be contained in $\mathbb{B}_{\ell,\infty}$. Using arguments like those in Proposition 3.1, one shows that $d_1d_2 > (d_1d_2-2t)^2$ and thus we obtain the Hilbert symbol statement.

To prove the upper bound, we need to develop more machinery. In [LV, §6], we give explicit presentations of $\mathrm{End}(\overline{E(\tau_1)})$ as suborders of $\mathrm{M}_2(\mathbb{Q}(\sqrt{d_1}))$. Using this presentation, one shows that elements ϕ of fixed norm and trace give rise to invertible ideals in $\mathcal{O}_{d_1}$ that have a fixed ideal class in $\frac{\operatorname{Pic}\mathcal{O}_{d_1}}{2\operatorname{Pic}\mathcal{O}_{d_1}}$. Moreover, multiple elements can give rise to the same ideal only if t is sufficiently divisible by primes dividing d_1.

If $\frac{1}{4}(d_1d_2 - (d_1d_2-2t)^2)$ is coprime to the conductor of $\mathcal{O}_{d_1}$, then the converse holds, i.e., given an ideal in a fixed ideal class, one can construct one (or multiple, depending on t) endomorphisms ϕ with the desired properties. The interested reader can find the details in [LV, §§5,6].

5.2. **Proof of Theorem 2.4.** Let d_1 and d_2 be discriminants of quadratic imaginary orders and assume that the quadratic imaginary order of discriminant d_1 is maximal at ℓ. Recall that $\mathscr{J}(d_1,d_2,t)$ equals

$$\sum_{E/\overline{\mathbb{F}}_\ell} \# \left\{ \begin{array}{ll} i_j\colon \mathbb{Z}\left[\frac{d_j+\sqrt{d_j}}{2}\right] \hookrightarrow \mathrm{End}(E): & \mathrm{Tr}(i_1(d_1+\sqrt{d_1})i_2(d_2-\sqrt{d_2})) = 4t, \\ & i_1(\mathbb{Q}(\sqrt{d_1})) \cap \mathrm{End}(E) = i_1(\mathbb{Z}\left[\frac{d_1+\sqrt{d_1}}{2}\right]) \end{array} \right\} / \mathrm{End}(E)^\times.$$

We will relate $\mathscr{J}(d_1,d_2,t)$ to the number of endomorphisms of reductions of elliptic curves with complex multiplication; precisely, we will show that $\mathscr{J}(d_1,d_2,t)$ equals

$$\frac{4}{w_1 e}\sum_{[\tau_1]} \# \left\{ \phi \in \mathrm{End}(\overline{E(\tau_1)}) : \mathrm{Tr}(\phi) = d_2, \mathrm{N}(\phi) = \frac{1}{4}(d_2^2 - d_2), \mathrm{Tr}(i_{\tau_1}(d_1+\sqrt{d_1})\cdot\phi^\vee) = 2t \right\}.$$

Let $E/\overline{\mathbb{F}}_\ell$ be an elliptic curve and let $i_1\colon \mathbb{Z}\left[\frac{d_1+\sqrt{d_1}}{2}\right] \hookrightarrow \mathrm{End}(E)$ be an embedding such that $i_1(\mathbb{Q}(\sqrt{d_1})) \cap \mathrm{End}(E) = i_1(\mathbb{Z}\left[\frac{d_1+\sqrt{d_1}}{2}\right])$. By Deuring's lifting theorem[Lan87, Chap. 13, Thm. 14], there exists a τ_1 in the upper half-plane of discriminant d_1 such that $\overline{E(\tau_1)}$ is isomorphic to E. Furthermore, after possibly replacing E with an isomorphic curve, and conjugating i_1, i_2 by an automorphism ψ of E, we may assume that the embedding $i_{\tau_1}\colon \mathbb{Z}\left[\frac{d_1+\sqrt{d_1}}{2}\right] \xrightarrow{\sim} \mathrm{End}(E(\tau_1)) \hookrightarrow \mathrm{End}(\overline{E(\tau_1)})$ either agrees with i_1 or differs from i_1 by precomposition with the nontrivial Galois automorphism. By [Gro86], the class of τ_1 modulo $\mathrm{SL}_2(\mathbb{Z})$ is unique if $\ell \nmid d_1$ and otherwise there are exactly two choices for the class of τ_1. Moreover, the choice of $\psi/\{\pm 1\}$ is unique up to multiplication by units in $(\operatorname{Im} i_1)/\{\pm 1\}$.

Conversely, every τ_1 gives rise to an elliptic curve $\overline{E(\tau_1)}/\overline{\mathbb{F}}_\ell$ and an embedding

$$i_{\tau_1}\colon \mathbb{Z}\left[\frac{d_1+\sqrt{d_1}}{2}\right] \xrightarrow{\sim} \mathrm{End}(E(\tau_1)) \hookrightarrow \mathrm{End}(\overline{E(\tau_1)}).$$

By [LV, Prop. 2.2], we have $i_{\tau_1}(\mathbb{Q}(\sqrt{d_1})) \cap \mathrm{End}(E) = i_{\tau_1}(\mathbb{Z}\left[\frac{d_1+\sqrt{d_1}}{2}\right])$. Thus,

$$\sum_{E/\overline{\mathbb{F}}_\ell} \# \frac{\{i_1 \colon \mathbb{Z}\left[\frac{d_1+\sqrt{d_1}}{2}\right] \hookrightarrow \mathrm{End}(E)\}}{\mathrm{End}(E)^\times} = \frac{2}{e} \cdot \#\{[\tau_1] : \mathrm{disc}(\tau_1) = d_1\},$$

where e denotes the ramification index of ℓ in $\mathbb{Q}(\sqrt{d_1})$.

Now fix an element τ_1 and fix an embedding $i_2 \colon \mathbb{Z}\left[\frac{d_2+\sqrt{d_2}}{2}\right] \hookrightarrow \mathrm{End}(\overline{E(\tau_1)})$ such that $\mathrm{Tr}(i_{\tau_1}(d_1+\sqrt{d_1}) i_2(d_2-\sqrt{d_2})) = 4t$. Then i_2 uniquely determines an element $\phi \in \mathrm{End}(\overline{E(\tau_1)}))$ such that

$$\mathrm{Tr}(\phi) = d_2, \quad \mathrm{N}(\phi) = \frac{1}{4}(d_2^2 - d_2), \quad \mathrm{Tr}(i_{\tau_1}(d_1 + \sqrt{d_1})\phi^\vee) = 2t,$$

namely $\phi := i_2\left(\frac{d_2+\sqrt{d_2}}{2}\right)$. Conversely, a choice of ϕ uniquely determines an embedding $i_2 \colon \mathbb{Z}\left[\frac{d_2+\sqrt{d_2}}{2}\right] \hookrightarrow (\mathrm{End}(\overline{\tau_1}))$. Therefore, $\mathscr{J}(d_1, d_2, t)$ equals

$$\frac{1}{e} \cdot \frac{2}{w_1} \cdot 2 \sum_{[\tau_1]} \# \left\{ \phi \in \mathrm{End}(\overline{E(\tau_1)}) : \mathrm{Tr}(\phi) = d_2, \mathrm{N}(\phi) = \frac{1}{4}(d_2^2 - d_2), \mathrm{Tr}(i_{\tau_1}(d_1 + \sqrt{d_1}) \cdot \phi^\vee) = 2t \right\}.$$

In [LV, Thm. 3.1], the present authors explain how to compute

$$\sum_{[\tau_1]} \# \left\{ \begin{array}{ll} \phi \in \mathrm{End}(\overline{E(\tau_1)}) : & \mathrm{Tr}(\phi) = d_2, \mathrm{N}(\phi) = \frac{1}{4}(d_2^2 - d_2), \\ & \mathrm{Tr}(i_{\tau_1}(d_1 + \sqrt{d_1}) \cdot \phi^\vee) = 2t, \mathbb{Q}(\phi) \cap \mathrm{End}(E(\tau_1)) = \mathbb{Z}[\phi] \end{array} \right\}.$$

It is straightforward to see how to modify the proof of [LV, Thm. 3.1] in order to omit the last condition, that is, the condition that $\mathbb{Q}(\phi) \cap \mathrm{End}(E(\tau_1)) = \mathbb{Z}[\phi]$. Roughly speaking, one should omit every step that involves the conductor of the order of discriminant d_2, as only the condition that $\mathbb{Q}(\phi) \cap \mathrm{End}(E(\tau_1)) = \mathbb{Z}[\phi]$ depends on this conductor. After making these changes to the proof, one proves that the quantity

$$\sum_{[\tau_1]} \# \left\{ \phi \in \mathrm{End}(\overline{E(\tau_1)}) : \mathrm{Tr}(\phi) = d_2, \mathrm{N}(\phi) = \frac{1}{4}(d_2^2 - d_2), \mathrm{Tr}(i_{\tau_1}(d_1 + \sqrt{d_1}) \cdot \phi^\vee) = 2t \right\}$$

is 0 if there exists a prime $p \neq \ell$ such that the Hilbert symbol

$$(d_u, D(n^2 - \delta^2 \widetilde{D}))_p = (d_u, (d_u f_u^{-2} d_x - 2t)^2 - d_u {f_u}^{-2} d_x)_p = -1,$$

and otherwise, that it is bounded above by

$$2^{\#\{p \,:\, v_p(t) \geq v_p(d_u f_u^{-2}) > 0, p \nmid 2\ell\}} \cdot \tilde{\rho}^{(2)}_{d_u f_u^{-2}}(t, d_2) \cdot \# \left\{ \mathfrak{b} \subseteq \mathcal{O}_u : \mathrm{N}(\mathfrak{b}) = \frac{\delta^2 \widetilde{D} - n^2}{4D\ell f_u^2}, \mathfrak{b} \text{ invertible} \right\}.$$

One also shows that the upper bound is an equality in the case that $\frac{\delta^2 \widetilde{D} - n^2}{4D f_u^2}$ is relatively prime to the conductor of the order of discriminant $d_u f_u^{-2}$. This should not be surprising, as it is basically the statement of Theorem 5.1 with the conditions involving f_2, the conductor of the order of discriminant d_2, omitted. □

Remark 5.2. *There is an alternative way of proving Theorem 2.4 that does not require making the necessary modifications to the proof of* [LV, Thm. 3.1]. *First one notes that*

$$\left\{ \begin{array}{rl} \phi \in \operatorname{End}(\overline{E(\tau_1)}): & \operatorname{Tr}(\phi) = d_2, \mathrm{N}(\phi) = \frac{1}{4}(d_2^2 - d_2), \\ & \operatorname{Tr}(\omega_1 \cdot \phi^\vee) = t, \end{array} \right\}$$

equals

$$\coprod_{f \mid f_2} \left\{ \begin{array}{rl} & \operatorname{Tr}(\tilde{\phi}) = d_2 f^{-2}, \mathrm{N}(\tilde{\phi}) = \frac{1}{4}(d_2^2 f^{-4} - d_2 f^{-2}), \\ \tilde{\phi} \in \operatorname{End}(\overline{E(\tau_1)}): & \operatorname{Tr}(\omega_1 \cdot \tilde{\phi}^\vee) = \frac{1}{2f^2}(2ft + d_1 f - d_2 f + d_2), \\ & \mathbb{Q}(\tilde{\phi}) \cap \operatorname{End}(\overline{E(\tau_1)}) = \mathbb{Z}[\tilde{\phi}] \end{array} \right\},$$

where f ranges over all positive divisors of f_2, the conductor of the order of discriminant d_2; the map $\tilde{\phi} \mapsto \frac{1}{2}(2f\tilde{\phi} - d_2 f^{-1} + d_2)$ gives a bijective map from the latter set to the former. Then, one uses repeated applications of Theorem 5.1 to compute the cardinality of the latter set. A series of algebraic manipulations will complete the proof.

6. Ideals in $\mathbb{B}_{\ell,\infty}$

In this section we prove Theorem 3.8, which we restate here for the reader's convenience. Recall that for any integral ideal I in $\mathbb{B}_{\ell,\infty}$, $\mathrm{RO}(I) = \{y \in \mathbb{B}_{\ell,\infty} : Iy \subseteq I\}$ is the right order of I.

Theorem. *Fix R a maximal order in $\mathbb{B}_{\ell,\infty}$. Assume that $x, u \in R$ and $\gamma, \delta \in \mathbb{Z}$ are such that*

$$\operatorname{Tr}(u), \quad \mathrm{N}(u), \quad \text{and} \quad \operatorname{Tr}(xu^\vee) + \gamma\,\mathrm{N}(u)/\delta \quad \text{are 0 modulo } \delta.$$

Define $w := x + \gamma u/\delta$, $c_p \in \mathbb{Z}$ to be such that $up^{-c_p} \in R_p \setminus pR_p$, and $r_p := \max(v_p(\delta) - c_p, 0)$. Assume that for all $p|\delta, p \neq \ell$, either $c_p = 0$ or $\mathbb{Q}_p(p^{r_p}w) \cap R \otimes \mathbb{Z}_p = \mathbb{Z}_p[p^r w]$.

Then $\#\{I \subseteq R : \delta, u \in I, \mathrm{N}(I) = \delta, \text{ and } w \in \mathrm{RO}(I)\}$ equals

$$\prod_{p|\delta, p\neq\ell} \left(\sum_{\substack{j=0 \\ j \equiv v_p(\delta) \pmod 2}}^{v_p(\delta)} \mathfrak{I}^{(p)}_{j-r_p}(\operatorname{Tr}(w), \mathrm{N}(w)) \right),$$

where

$$\mathfrak{I}^{(p)}_C(a_1, a_0) = \begin{cases} \#\{\tilde{t} \bmod p^C : \tilde{t}^2 - a_1\tilde{t} + a_0 \equiv 0 \pmod{p^C}\} & \text{if } C \geq 0, \\ 0 & \text{if } C < 0. \end{cases}$$

This section is independent of the rest of the paper, so we disregard any notation fixed elsewhere.

For any prime p, let $R_p := R \otimes_{\mathbb{Z}} \mathbb{Z}_p$. If $p \neq \ell$, then after fixing an isomorphism of $\mathbb{B}_{\ell,\infty} \otimes \mathbb{Q}_p$ with $\mathrm{M}_2(\mathbb{Q}_p)$ we can view R_p as a maximal order in $\mathrm{M}_2(\mathbb{Q}_p)$. Moreover, after conjugating by an appropriate element, we may assume that $R_p = \mathrm{M}_2(\mathbb{Z}_p)$. If I_p is an ideal in $\mathrm{M}_2(\mathbb{Z}_p)$, then $\mathrm{RO}(I_p) := \{A \in \mathrm{M}_2(\mathbb{Q}_p) : I_p A \subseteq I_p\}$. By [Vig80, Chap. 2, Thm. 2.3], there are $1 + p + \cdots + p^N$ ideals of norm p^N in $\mathrm{M}_2(\mathbb{Z}_p)$, and they are all of the form

$$R_p \begin{pmatrix} p^n & t \\ 0 & p^m \end{pmatrix}, \tag{6.1}$$

where n, m are positive integers such that $n+m = N$, and $t \in \mathbb{Z}_p$. The triple $(n, m, t \bmod p^m)$ uniquely determines the ideal. By abuse of notation, we will use the triple (n, m, t) to refer to both the element $\begin{pmatrix} p^n & t \\ 0 & p^m \end{pmatrix}$ and the ideal it generates.

We say an element $y \in \mathrm{M}_2(\mathbb{Q}_p)$ is *optimally embedded* if $\mathbb{Q}_p(y) \cap R_p = \mathbb{Z}_p[y]$ and that y is *primitive* if $w \in R_p \setminus pR_p$. An ideal I is *primitive* if it is generated by a primitive element, i.e. if $I = (n, m, t)$ where at least one of n, m, or $v(t)$ are zero. We divide primitive ideals into three cases: Case 1) $n = 0$, Case 2) $m = 0$, and Case 3) $n, m > 0$, and $v(t) = 0$. Note that these cases are mutually exclusive unless we are considering the unit ideal.

In §6.1 we give a formula that computes, for a fixed integral element $y \in \mathrm{M}_2(\mathbb{Q}_p)$ and integer N, the number of ideals I_p of norm p^N with $y \in \mathrm{RO}(I_p)$. In §6.2, we give a criterion to determine whether one ideal is contained in another. In §6.3, we explain how the results in the two previous sections come together to prove Theorem 3.8.

6.1. Right orders of ideals in $\mathrm{M}_2(\mathbb{Z}_p)$.

Lemma 6.1. *Let $y \in \mathrm{M}_2(\mathbb{Q}_p)$ be an integral element. Assume that there exists an $r \in \mathbb{Z}_{\geq 0}$ such that $p^r y$ is optimally embedded. Then there exists an $A \in \mathrm{GL}_2(\mathbb{Z}_p)$ such that*

$$AyA^{-1} = \begin{pmatrix} 0 & -\mathrm{N}(y)p^r \\ p^{-r} & \mathrm{Tr}(y) \end{pmatrix}$$

Proof. Write $y = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. First assume that p divide the conductor of $\mathrm{D}(p^r y) := \mathrm{Tr}(p^r y)^2 - 4\,\mathrm{N}(p^r y)$. Then we may consider the element

$$y' := p^r y + \frac{p^{2r}\,\mathrm{D}(y) - p^{r+1}\,\mathrm{Tr}(y)}{2p};$$

since $p^r y$ is optimally embedded, y' is primitive. By writing y' as a matrix, we see that the primitivity of y' implies that one of $a - d$, b or c has valuation exactly $-r$. If p does not divide the conductor of $\mathrm{D}(p^r y)$, then necessarily $r = 0$. In this case, using the relation $\mathrm{D}(y) = (a-d)^2 - 4bc$, we can also show that one of $a - d$, b, or c has valuation exactly $-r$.

If $v(b) = -r$, then let $A = \begin{pmatrix} -dp^r & bp^r \\ 1 & 0 \end{pmatrix}$. If $v(c) = -r$, then let $A = \begin{pmatrix} cp^r & -ap^r \\ 0 & 1 \end{pmatrix}$. If $v(b), v(c) > -r$, and $v(a-d) = -r$, then let $A = \begin{pmatrix} (c-d)p^r & (b-a)p^r \\ 1 & 1 \end{pmatrix}$. One can easily check that these matrices fulfill the assertions in the lemma. □

Proposition 6.2. *Let y be an integral element of $\mathrm{M}_2(\mathbb{Q}_p)$. Assume that there exists an $r \in \mathbb{Z}_{\geq 0}$ such that $p^r y$ is optimally embedded. Then the number of primitive ideals I_p of norm p^N such that $y \in \mathrm{RO}(I_p)$ is $\mathfrak{I}^{(p)}_{N-r}(\mathrm{Tr}(y), \mathrm{N}(y))$, where:*

$$\mathfrak{I}^{(p)}_{N-r}(a_1, a_0) = \begin{cases} \#\{\widetilde{t} \bmod p^{N-r} : \widetilde{t}^2 - a_1\widetilde{t} + a_0 \equiv 0 \pmod{p^{N-r}}\} & \text{if } N \geq r, \\ 0 & \text{if } N < r. \end{cases}$$

In particular, there is a unique primitive ideal J_p of norm p^r such that $y \in \mathrm{RO}(J_p)$. Furthermore, if I_p is any other ideal such that $y \in \mathrm{RO}(I_p)$ then $I_p \subseteq J_p$.

Proof. By Lemma 6.1, there exists $A \in \mathrm{GL}_2(\mathbb{Z}_p)$ such that $\tilde{y} := AyA^{-1} = \begin{pmatrix} 0 & -\mathrm{N}(y)p^r \\ p^{-r} & \mathrm{Tr}(y) \end{pmatrix}$. Recall that an element y is in the right order of R_pT if and only if $TyT^{-1} \in R_p$. Therefore, y is in the right order of R_pT if and only if $\tilde{y}$ is in the right order of R_pTA^{-1}.Thus it suffices to count the number of ideals I_p such that $\tilde{y} \in \mathrm{RO}(I_p)$.

Let I_p correspond to the triple (n, m, t). Then $\tilde{y} \in \mathrm{RO}(I_p)$ if and only if

$$m - n - r \geq 0, \quad v(t) - n - r \geq 0, \quad t^2 p^{-r-N} - t\,\mathrm{Tr}(w)p^{-m} + \mathrm{N}(w)p^{n-m+r} \in \mathbb{Z}_p. \tag{6.2}$$

The first two conditions imply that $m \geq n$ and $v(t) \geq n$. Since one of $m, n, v(t)$ must be 0, this implies that $n = 0$ and $m = N$. Now the first condition shows that there are no solutions if $N < r$; so from now on we assume that $r \leq N$. The second condition implies that $t = p^r\widetilde{t}$; substituting this into the third condition we obtain

$$\widetilde{t}^2 p^{r-N} - \mathrm{Tr}(w)\widetilde{t}p^{r-N} + \mathrm{N}(w)p^{r-N} \in \mathbb{Z}_p. \tag{6.3}$$

This completes the proof of the formula for $\mathfrak{I}_{M-r}(\mathrm{Tr}(w), \mathrm{N}(w))$.

The argument above shows that any ideal I_p such that $y \in \mathrm{RO}(I_p)$ is equal to

$$R_p \begin{pmatrix} 1 & \widetilde{t}p^r \\ 0 & p^N \end{pmatrix} A,$$

where $\widetilde{t}$ satisfies (6.3) and $N \geq r$; in particular, if $N = r$, there is a unique ideal $J_p := R_p \begin{pmatrix} 1 & 0 \\ 0 & p^r \end{pmatrix} A$ such that $y \in \mathrm{RO}(J_p)$. Since

$$\begin{pmatrix} 1 & \widetilde{t}p^r \\ 0 & p^N \end{pmatrix} A \cdot \left[\begin{pmatrix} 1 & 0 \\ 0 & p^r \end{pmatrix} A \right]^{-1} = \begin{pmatrix} 1 & \widetilde{t} \\ 0 & p^{N-r} \end{pmatrix} \in R_p,$$

$I_p \subseteq J_p$, as desired. □

6.2. **Lattice of ideals in** $\mathrm{M}_2(\mathbb{Z}_p)$**.**

Lemma 6.3. *Let z be a primitive integral element of $\mathrm{M}_2(\mathbb{Z}_p)$. Then there is a unique ideal of norm p^N containing z for all $N \leq v_p(\mathrm{N}(z))$. We write $I_{z,N}$ for this unique ideal.*

Proof. Let (n, m, t) be a generator for the ideal R_pz, i.e. $(n, m, t) = \epsilon z$, for some $\epsilon \in R_p^\times$. Then (n, m, t) is contained in an ideal I if and only if z is contained in I. Assume that (n, m, t) is contained in (n', m', t'), where $m' + n' = N$. Thus, the product

$$\begin{pmatrix} p^n & t \\ 0 & p^m \end{pmatrix} \begin{pmatrix} p^{-n'} & -t'p^{-N} \\ 0 & p^{-m'} \end{pmatrix} = \begin{pmatrix} p^{n-n'} & tp^{-m'} - t'p^{n-N} \\ 0 & p^{m-m'} \end{pmatrix}$$

must be in R_p. Therefore, $n \geq n', m \geq m', t \equiv t'p^{n-n'} \pmod{p^{m'}}$. A case-by-case analysis shows that there is a unique primitive tuple (n', m', t') with $n' + m' = N$ that satisfies these conditions; they are listed here for the readers' convenience.

$$n = 0 \Rightarrow n' = 0, m' = N, t' \equiv t \pmod{p^N}, \tag{6.4}$$

$$m = 0 \Rightarrow n' = N, m' = 0, \tag{6.5}$$

$$v(t) = 0 \Rightarrow n' = \min(n, N), m' = N - n', t' \equiv t \pmod{p^{m'}}. \tag{6.6}$$

We remark that there is no condition on t' in (6.5) since t' is only defined modulo $p^{m'} = 1$. □

Lemma 6.4. *Let j, k, r, s be non-negative integers and let y, z be primitive elements of norm at least p^r, p^s respectively. Then $p^j I_{y,r} \subseteq p^k I_{z,s}$ if and only if $r, s \geq s - j + k$ and $I_{y,s-j+k} = I_{z,s-j+k}$. (If $s - j + k < 0$ then this last condition is vacuous.)*

Proof. We prove the backwards direction first. Let y_N, z_N denote generators for $I_{y,N}$, $I_{z,N}$ respectively for any (valid) integer N. Since $s \geq s - j + k$ and $I_{y,s-j+k} = I_{z,s-j+k}$, we may write z_s as $z' y_{s-j+k}$ for some $z' \in R_p$ of norm p^{j-k}. We rewrite $p^j y_r (p^k z_s)^{-1}$ as follows

$$p^{j-k} y_r (z' y_{s-j+k})^{-1} = y_r y_{s-j+k}^{-1} \cdot p^{j-k} z'^{-1}.$$

By definition of y_N and since $r \geq s - j + k$, $y_r y_{s-j+k}^{-1} \in R_p$. Additionally, since z' has norm p^{j-k}, $p^{j-k} z'^{-1} \in R_p$. Thus $p^j I_{y,r} \subseteq p^k I_{z,s}$.

Now we consider the forward direction; assume that $p^j I_{y,r} \subseteq p^k I_{z,s}$. Then $p^{j-k} I_{y,r} \subseteq I_{z,s} \subseteq R_p$. Since $I_{y,r}$ is primitive, this implies that $j \geq k$, or equivalently that $s \geq s + k - j$. Without loss of generality we reduce to the case that $k = 0$.

If $s \leq j$, then all remaining conditions are vacuous, so we assume that $s > j$. Let (n_r, m_r, t_r) be a generator of $I_{y,r}$ and (n_s, m_s, t_s) be a generator of $I_{z,s}$. By assumption, we have

$$p^j \begin{pmatrix} p^{n_r} & t_r \\ 0 & p^{m_r} \end{pmatrix} \begin{pmatrix} p^{-n_s} & -t_s p^{-s} \\ 0 & p^{-m_s} \end{pmatrix} = \begin{pmatrix} p^{j+n_r-n_s} & t_r p^{j-m_s} - t_s p^{j+n_r-s} \\ 0 & p^{j+m_r-m_s} \end{pmatrix} \in R_p,$$

or, equivalently

$$j + n_r \geq n_s, \quad j + m_r \geq m_s, \quad t_r p^{n_s} \equiv t_s p^{n_r} \pmod{p^{s-j}}.$$

If $n_s = 0$, then $j + r \geq j + m_r \geq m_s = s$. Similarly if $m_s = 0$, then $j + r \geq j + n_r \geq n_s = s$. If $n_s, m_s > 0$, then $v(t_s) = 0$. Since $t_r t_s^{-1} p^{j+m_r-m_s} - p^{j+r-s} \in \mathbb{Z}_p$, this again implies that $j + r \geq s$. It remains to show that $I_{z,s-j} = I_{y,s-j}$.

First we treat the case when $n_r = 0$. Then $m_s > 0$ and $t_s \equiv t_r p^{n_s}$. Since at least one of $v(t_s)$, n_s must be zero, this shows that $n_s = 0$ and $t_r \equiv t_s \ (\mathrm{mod}\ p)^{s-j}$. Using (6.4)–(6.6), we see that $I_{y,s-j} \leftrightarrow (0, s-j, t_r \bmod p^{s-j})$ and $I_{z,s-j} \leftrightarrow (0, s-j, t_s \bmod p^{s-j})$ so we have equality.

Now consider the case when $m_r = 0$. Then by (6.4)–(6.6) $I_{y,s-j} \leftrightarrow (s-j, 0, 0)$. Since $j \geq m_s$, $n_s \geq s - j > 0$. By another application of (6.4)–(6.6), we see that regardless of whether $m_s = 0$ or $m_s > 0$ and $v(t_s) = 0$ we have $I_{z,s-j} \leftrightarrow (s-j, 0, 0)$.

Finally we consider the case where $n_r, m_r > 0$ and $v(t_r) = 0$. If $n_r < s - j$, then $I_{y,s-j} \leftrightarrow (n_r, s - j - n_r, t_r \bmod p^{s-j-n_r})$. In this case, the conditions above show that $m_s, n_s > 0$. This in turn implies that t_s is a p-adic unit, and since $t_s p^{n_r} \equiv t_r p^{n_s} \ (\mathrm{mod}\ p)^{s-j}$ we have $n_s = n_r < s_j$. Then, by (6.4)–(6.6), $I_{z,s-j} \leftrightarrow (n_r, s - j - n_r, t_s \bmod p^{s-j-n_r})$, which is equal to $I_{y,s-j}$. The sole remaining case is when $n_r \geq s - j$ which implies that $I_{y,s-j} = (s-j, 0, 0)$. Since $t_s t_r^{-1} p^{n_r} \equiv p^{n_s} \pmod{p^{s-j}}$, $n_s \geq s - j$. As in the previous paragraph, this means that regardless of whether $m_s = 0$ or $m_s > 0$ and $v(t_s) = 0$ we have $I_{z,s-j} \leftrightarrow (s-j, 0, 0)$. □

6.3. **Proof of Theorem 3.8.** Recall that R is a fixed maximal order in $\mathbb{B}_{\ell,\infty}$ and $x, u \in R$ and $\gamma, \delta \in \mathbb{Z}$ are such that

$$\mathrm{Tr}(u), \quad \mathrm{N}(u), \quad \text{and} \quad \mathrm{Tr}(xu^\vee) + \gamma\,\mathrm{N}(u)/\delta \quad \text{are 0 modulo } \delta.$$

We are interested in computing the number of left integral ideals I of R that satisfy

$$\delta, u \in I, \quad \mathrm{N}(I) = \delta, \quad \text{and } w := x + \gamma u/\delta \in \mathrm{RO}(I), \tag{6.7}$$

where $\mathrm{RO}(I) = \{y \in \mathbb{B}_{\ell,\infty} : Iy \subseteq I\}$ is the right order of I. Note that, due to the assumptions above, w is integral, i.e. $\mathrm{N}(w)$ and $\mathrm{Tr}(w)$ are in $\mathbb{Z}$.

For any prime p, let $R_p := R \otimes_{\mathbb{Z}} \mathbb{Z}_p$. By [Vig80, Chap. 3, Prop. 5.1], the map

$$\{\text{left ideals of } R\} \to \prod_p{}' \{\text{left ideals of } R_p\}, \quad I \mapsto (I_p)$$

is a bijection ($I_p := I \otimes_{\mathbb{Z}} \mathbb{Z}_p$). Thus

$$\#\{I \subseteq R : I \text{ satisfies } (6.7)\} = \prod_p \#\{I_p \subseteq R_p : I_p \text{ satisfies } (6.7)\}$$

If $p \nmid \delta$, then the first condition of (6.7) implies that $\mathrm{N}(I_p) = \langle 1 \rangle$ and so $I_p = R_p$. If $p = \ell$, then R_ℓ is the unique maximal order in $\mathbb{B}_{\ell,\infty} \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$ and ideals in R_ℓ are completely classified by the ℓ-valuation of their norms, and for any ideal $I_\ell \subseteq R_\ell$ we have that $R(I_\ell) = R_\ell$. Since w is integral and $\delta \mid \mathrm{N}(u)$ it is clear that the ideal of norm $\ell^{v(\delta)}$ satisfies conditions (6.7). Thus for all p outside the finite set $\{p : p|\delta, p \neq \ell\}$, we have

$$\#\{I_p \subseteq R_p := R \otimes_{\mathbb{Z}} \mathbb{Z}_p : \text{ satisfying } (6.7)\} = 1.$$

Henceforth we assume that $p|\delta$ and $p \neq \ell$. Recall that $c_p \in \mathbb{Z}$ is such that $up^{-c_p} \in R_p \setminus pR_p$ and $r_p = \max(v_p(\delta) - c_p, 0)$.

Lemma 6.5. *We have $w \in \mathrm{RO}(R_p u + R_p \delta)$ and the norm of $R_p u + R_p \delta$ divides $\delta^2 p^{-r_p}$.*

Proof. In order to prove that $w \in \mathrm{RO}(R_p u + R_p \delta)$, we will show that δw and uw are both contained in $R_p u + R_p \delta$. The first containment is straightforward. For the second containment, we need the fact that $\mathrm{Tr}(ab) = \mathrm{Tr}(ba)$ for any $a, b \in R_p$ and (3.4). Consider the following expansion

$$\begin{aligned} uw &= \mathrm{Tr}(u)w - u^\vee w = \mathrm{Tr}(u)w - u^\vee x - \gamma u^\vee u/\delta \\ &= \mathrm{Tr}(u)w + x^\vee u - (\mathrm{Tr}(u^\vee x) + \gamma\, \mathrm{N}(u)/\delta). \end{aligned}$$

Since, by assumption, $\mathrm{Tr}(u)$ and $\mathrm{Tr}(xu^\vee + \gamma\, \mathrm{N}(u)/\delta$ are divisible by δ, $uw \in R_p u + R_p \delta$.

Now we compute the norm of $R_p u + R_p \delta$. If $r_p = 0$, then $u \in R_p \delta$ and $\mathrm{N}(R_p u + R_p \delta) = \mathrm{N}(R_p \delta) = \delta^2$. Now assume that $r_p > 0$. We claim that $v_p(\mathrm{N}(u)) \geq 2c_p + r = c_p + v_p(\delta)$. If $c_p = 0$, then this follows from our assumptions on x, u, δ, and γ.

Assume that $c_p > 0$ and that $v_p(\mathrm{N}(u)) < c_p + v_p(\delta)$. Using the criterion in Lemma 6.4 we can show that $\delta \in R_p u$ so $R_p u + R_p \delta = R_p u$. Since $\mathrm{RO}(R_p u) = \mathrm{RO}(R_p u p^{-c_p})$, by the first part of the proof w is in the right order of an ideal of norm $\mathrm{N}(u) - 2c_p < r_p$. However, Proposition 6.2 shows that this is impossible since by assumption $p^{r_p} w$ is optimally embedded in $\mathrm{M}_2(\mathbb{Z}_p)$. This proves the claim.

To review, we have shown that if $r_p > 0$ then $v_p(\mathrm{N}(u)) \geq c_p + v_p(\delta)$. If $\mathrm{N}(u) = c_p + v_p(\delta)$ then clearly $\mathrm{N}(R_p u + R_p \delta) | \delta p^{c_p}$. Assume that $\mathrm{N}(u) > c_p + v_p(\delta)$ and write u as $\begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{pmatrix}$. By the definition of c_p, there exists i, j such that $v_p(a_{i,j}) = c_p$. Define $A \in \mathrm{M}_2(\mathbb{Z}_p)$ to be such that row i and column j consist only of zeros and the remaining entry has a 1. Then

$$\mathrm{N}(u + \delta A) = \mathrm{N}(u) + \delta\, \mathrm{Tr}(Au^\vee) = \mathrm{N}(u) + \delta a_{i,j}.$$

Since $u + \delta A \in R_p u + R_p \delta$, this shows that $\mathrm{N}(R_p u + R_p \delta) | \delta p^{c_p}$, which completes the proof. □

Now we are in a position to prove that there are

$$\sum_{\substack{j=0 \\ j\equiv v_p(\delta) \pmod 2}}^{v_p(\delta)} \mathfrak{I}^{(p)}_{j-r_p}(\mathrm{Tr}(w), \mathrm{N}(w))$$

many ideals $I_p \subset R_p$ that satisfy (6.7).

If $c_p = 0$, then the sum is 1, so we must prove that there is a unique ideal that satisfies (6.7). In this case u is a primitive element of R_p so Lemmas 6.3 and 6.4 imply that there is a unique ideal of norm δ that contains u, $I_{u,v(\delta)}$. We clearly have $R_pu + R_p\delta \subseteq I_{u,v(\delta)}$. Lemma 6.5 gives the opposite containment, so we have equality. Another application of Lemma 6.5 shows that $w \in \mathrm{RO}(I_{u,v(\delta)})$.

Henceforth we assume that $c_p > 0$. Using Lemma 6.4 and Lemma 6.5, one can show that $R_pu + R_p\delta = p^c I_{u',r}$, where $u' := up^{-c_p}$. Therefore, $w \in \mathrm{RO}(p^c I_{u',r}) = \mathrm{RO}(I_{u',r})$. By assumption w, r_p satisfy the hypotheses of Proposition 6.2, so $I_{u',r}$ is the unique ideal of norm p^r such that $w \in \mathrm{RO}(I_{u',r})$, and moreover, for any ideal I such that $w \in \mathrm{RO}(I)$ we have $I \subseteq I_{u',r}$. By Lemma 6.4, we also know that for any ideal I of norm $p^{v(\delta)}$ such that $I \subseteq I_{u',r}$ we have $u, \delta \in I$. Thus it suffices to count the number of ideals I of norm $p^{v(\delta)}$ such that $w \in \mathrm{RO}(I)$. This is equal to the number of primitive ideals of norm p^j where j is at most $v(\delta)$ and $j \equiv v(\delta) \pmod 2$. Applying Proposition 6.2 completes the proof.

Since we have already shown that

$$\#\{I \subseteq R : I \text{ satisfies } (6.7)\} = \prod_{p|\delta, p\neq\ell} \#\{I_p \subseteq R_p : I_p \text{ satisfies } (6.7)\},$$

this proves Theorem 3.8. □

References

[ABL+] Jacqueline Anderson, Jennifer S. Balakrishnan, Kristin Lauter, Jennifer Park, and Bianca Viray, *Comparing arithmetic intersection theory formulas*. Preprint, 2012.

[BY06] Jan Hendrik Bruinier and Tonghai Yang, *CM-values of Hilbert modular functions*, Invent. Math. **163** (2006), no. 2, 229–288. MR2207018 (2008b:11053)

[Deu41] Max Deuring, *Die Typen der Multiplikatorenringe elliptischer Funktionenkörper*, Abh. Math. Sem. Hansischen Univ. **14** (1941), 197–272 (German). MR0005125 (3,104f)

[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). MR2310947 (2008i:11075)

[GL11] ______, *Genus 2 Curves with Complex Multiplication*, International Mathematics Research Notices, posted on 2011, 75 pp., DOI 10.1093/imrn/rnr052, (to appear in print).

[Gro86] Benedict H. Gross, *On canonical and quasicanonical liftings*, Invent. Math. **84** (1986), no. 2, 321–326, DOI 10.1007/BF01388810. MR833193 (87g:14051)

[GZ85] Benedict H. Gross and Don B. Zagier, *On singular moduli*, J. Reine Angew. Math. **355** (1985), 191–220. MR772491 (86j:11041)

[GK93] Benedict H. Gross and Kevin Keating, *On the intersection of modular correspondences*, Invent. Math. **112** (1993), 225–245.

[GJLL+11] Helen Grundman, Jennifer Johnson-Leung, Kristin Lauter, Adriana Salerno, Bianca Viray, and Erika Wittenborn, *Igusa class polynomials, embeddings of quartic CM fields, and arithmetic intersection theory*, Fields Institute Communications, vol. 60, American Mathematical Society, 2011. WIN - Women in Numbers, Research Directions in Number Theory.

[HY12] Benjamin Howard and Tonghai Yang, *Intersections of Hirzebruch-Zagier divisors and CM cycles*, Lecture Notes in Mathematics, vol. 2041, Springer, Heidelberg, 2012. MR2951750

[Lan87] Serge Lang, *Elliptic functions*, 2nd ed., Graduate Texts in Mathematics, vol. 112, Springer-Verlag, New York, 1987. With an appendix by J. Tate. MR890960 (88c:11028)

[Lau] Kristin Lauter, *Primes in the denominators of Igusa Class Polynomials.* Preprint, `arXiv:0301.240`.

[LV] Kristin Lauter and Bianca Viray, *On singular moduli for arbitrary discriminants.* Preprint, `arXiv:1206.6942`.

[Vig80] Marie-France Vignéras, *Arithmétique des algèbres de quaternions*, Lecture Notes in Mathematics, vol. 800, Springer, Berlin, 1980 (French). MR580949 (82i:12016)

[Wat69] William C. Waterhouse, *Abelian varieties over finite fields*, Ann. Sci. École Norm. Sup. (4) **2** (1969), 521–560. MR0265369 (42 #279)

[Yan10] Tonghai Yang, *An arithmetic intersection formula on Hilbert modular surfaces*, Amer. J. Math. **132** (2010), 1275–1309.

[Yan] ——, *Arithmetic intersection on a Hilbert modular surface and the Faltings height.* 2007, Preprint.

Microsoft Research, 1 Microsoft Way, Redmond, WA 98062, USA
E-mail address: `klauter@microsoft.com`
URL: `http://research.microsoft.com/en-us/people/klauter/default.aspx`

Department of Mathematics, Box 1917, Brown University, Providence, RI 02912, USA
E-mail address: `bviray@math.brown.edu`
URL: `http://math.brown.edu/~bviray`