COMPARING ARITHMETIC INTERSECTION FORMULAS FOR DENOMINATORS OF IGUSA CLASS POLYNOMIALS

JACQUELINE ANDERSON, JENNIFER S. BALAKRISHNAN, KRISTIN LAUTER, JENNIFER PARK, AND BIANCA VIRAY

Abstract. Bruinier and Yang conjectured a formula for intersection numbers on an arithmetic Hilbert modular surface, and as a consequence obtained a conjectural formula for $\mathrm{CM}(K).\mathrm{G}_1$ under strong assumptions on the ramification in K. Yang later proved this conjecture under slightly stronger assumptions on the ramification. In recent work, Lauter and Viray proved a different formula for $\mathrm{CM}(K).\mathrm{G}_1$ for primitive quartic CM fields with a mild assumption, using a method of proof independent from that of Yang. In this paper we show that these two formulas agree, for a class of primitive quartic CM fields which is slightly larger than the intersection of the fields considered by Yang and Lauter and Viray. Furthermore, the proof that these formulas agree does *not* rely on the results of Yang or Lauter and Viray. As a consequence of our proof, we conclude that the Bruinier-Yang formula holds for a slightly largely class of quartic CM fields K than what was proved by Yang, since it agrees with the Lauter-Viray formula, which is proved in those cases. The factorization of these intersection numbers has applications to cryptography: precise formulas for them 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.

1. Introduction

In this paper we study the relationship between two formulas proved for arithmetic intersection numbers on the Siegel moduli space of principally polarized abelian surfaces. Specifically, these are formulas for the arithmetic intersection of the CM points of K, denoted by $\mathrm{CM}(K)$, with the Humbert surface G_1, which parametrizes abelian surfaces isomorphic to a product of elliptic curves with the product polarization; the ℓ-part of this arithmetic intersection number is denoted $(\mathrm{CM}(K).\mathrm{G}_1)_\ell$.

The study of these particular intersection numbers was largely motivated by applications to cryptography. In order to generate genus 2 curves over a finite field whose Jacobians have prime order, the *CM method* proceeds by computing the minimal polynomials of the invariants of the genus 2 curves with CM by a primitive quartic CM field K. These minimal polynomials are analogous to the Hilbert class polynomials for imaginary quadratic fields K. Indeed, Igusa defined a collection of invariants for genus 2 curves and proved expressions for them in terms of quotients of Siegel modular forms. For genus 2 curves with complex multiplication (CM) by a primitive quartic CM field K, these invariants lie in the Hilbert class field of the reflex field of K, and their minimal polynomials, *Igusa class polynomials*,

2010 *Mathematics Subject Classification.* Primary 1R11; Secondary 11G15, 11R27.

The second author was supported by NSF grant DMS-1103831. The fourth author was partially supported by NSF grant DMS-1069236 and by a NSERC PGSD grant. The last author was partially supported by NSF grant DMS-1002933 and ICERM.

have coefficients which are rational, not necessarily integral as is the case for Hilbert class polynomials related to invariants of elliptic curves.

Ignoring cancellation with numerators, the primes which appear in the denominators of Igusa class polynomials are those which appear in $(\mathrm{CM}(K).G_1)$, the arithmetic intersection on the Siegel moduli space of the divisor of the Siegel modular form χ_{10} with the CM points of K. In [GL07], it was proved that these primes are those ℓ for which there is a solution to an *Embedding Problem*, that is, there exists an embedding of $\mathcal{O}_K$ into $M_2(\mathbb{B}_{\ell,\infty})$ with certain properties. Studying this embedding problem, [GL07] gave a bound on the primes which can appear, and [GL11] gave a bound on the powers to which they can appear.

At the same time, Bruinier and Yang, using methods from Arakelov intersection theory, gave a conjectural exact formula for the factorization of the denominators under certain conditions on the ramification in the primitive quartic CM field K [BY06]. They assume that the discriminant of K is $D^2\widetilde{D}$, where D and $\widetilde{D}$ are both primes congruent to 1 (mod 4). In [Yan10, Yan], Yang proved the conjectured intersection formula assuming the ring of integers of K is generated by one element over the ring of integers of the real quadratic subfield. Yang's proof uses results of Gross-Keating, and then computes local densities by evaluating certain local integrals over the quaternions.

In practice, very few primitive quartic CM fields have ramification of such restricted form. In [GJLL$^+$11], Grundman, Johnson-Leung, Salerno, Wittenborn, and the third and last author studied all 13 quartic cyclic CM fields in van Wamelen's tables of CM genus 2 curves defined over $\mathbb{Q}$, compared denominators with the number of solutions to the Embedding Problem and Bruinier and Yang's formula, and found that the Bruinier-Yang formula does not hold in general as stated when the assumptions on the ramification of K are relaxed. For applications to the computation of genus 2 curves for cryptography, it is important to have a precise formula for the denominators of Igusa class polynomials which holds for general primitive quartic CM fields.

In [LV], the third and last author proved a formula for $(\mathrm{CM}(K).G_1)$ for primitive quartic CM fields K with almost no assumptions on K. A simplified version of this formula holds with an extra mild assumption. The proof of their formula follows from parameterizing solutions to the Embedding Problem by pairs of endomorphisms of a supersingular elliptic curve E, $x, u \in \mathrm{End}(E)$ with a fixed norm and trace. This, in turn, is related to a counting problem studied by Gross and Zagier in their formula for the factorization of differences of singular moduli.

The formula given by Bruinier and Yang is strikingly similar to the simplified version of the formula in [LV]. Indeed, both formulas involve two nested sums where the summand is a product that includes the number of ideals of a given norm. However, the Bruinier-Yang formula counts ideals in a quartic CM field, whereas the Lauter-Viray formula counts ideals in an imaginary quadratic order.

In this paper, we show that the formulas of Bruinier-Yang (BY) and Lauter-Viray (LV) agree, *without* using that the formulas compute the same arithmetic intersection number. As a consequence of our result, we conclude that the BY formula holds for a slightly larger class of quartic CM fields K than what was proved by Yang. See §5 for more details.

1.1. **Idea of proof.** The BY formula sums over elements in $\widetilde{F}$, the real quadratic subfield of $\widetilde{K}$, the reflex field of K, counting the number of ideals of $\widetilde{K}$ with certain norms, with a

certain multiplicity. The LV formula sums over certain integers which turn out to be in one-to-one correspondence with the elements of $\widetilde{F}$ which arise in BY, under the assumptions on the ramification of K (see Proposition 5.3). For each such integer n in the LV formula, two related imaginary quadratic fields are defined, with suborders of discriminants $d_u = d_u(n)$ and $d_x = d_x(n)$ respectively. The LV formula counts ideals in $\mathbb{Z}[(d_u + \sqrt{d_u})/2]$ with norm equal to N, a quantity related to n, with certain multiplicities. The heart of our proof of the equality of these two formulas is Proposition 6.7, which shows how the splitting behavior of certain primes in the quadratic extension $\widetilde{K}/\widetilde{F}$ is related to the splitting behavior of certain primes in the quadratic extensions $\mathbb{Q}(\sqrt{d_u})$ and $\mathbb{Q}(\sqrt{d_x})$. Thus the results of this paper can be viewed as a kind of "reciprocity" between splitting behavior of certain primes in different quadratic extensions. The resulting equality of local factors in the BY and LV formulas also involves the multiplicities which appear in the LV formula arising from genus theory, and indeed our proofs rely heavily on computations of related Hilbert symbols.

1.2. **Outline of paper.** In §§2 and 3, we precisely state the BY formula and the LV formula, respectively. We also prove that these formulas can be expressed as a product of local factors, which will be instrumental in the proof of our main result.

Both formulas rely on a relative integral basis for the ring of integers of K over the ring of integers of the real quadratic subfield F. In §4 we give the possibilities for this integral basis under the assumption that D is prime and $\widetilde{D}$ is squarefree.

We precisely state our main result in §5 and begin the proof by showing that the BY formula and LV formula both sum over the same indices. The crux of the proof is in §6, where we show that the summands in the BY formula and LV formula agree by comparing the local factors.

1.3. **Notation.** Let $F/\mathbb{Q}$ denote a real quadratic field, and let

$$D = \mathrm{Disc}_{F/\mathbb{Q}}(\mathcal{O}_F).$$

Let $A, B \in \frac{1}{2}\mathbb{Z}$ be such that $A + B\sqrt{D} \in \mathcal{O}_F$ and $K = F(\sqrt{A + B\sqrt{D}})$ is a totally imaginary quadratic extension of F. Throughout this paper, K will be assumed to be a *primitive* quartic CM field, which is the case if it is either non-Galois or Galois cyclic [Shi98, Ch. II, §8.4]. Write

$$\widetilde{D} = \mathrm{Norm}_{F/\mathbb{Q}}(\mathrm{Disc}_{K/F}(\mathcal{O}_K))$$

and write $\widetilde{F} = \mathbb{Q}(\sqrt{\widetilde{D}})$. There is a choice of CM-type of K for which the reflex field $\widetilde{K}$ equals $\widetilde{F}(\sqrt{2A + 2\sqrt{A^2 - B^2 D}})$; throughout we work with this fixed type and reflex field. Denote the relative discriminant of $\widetilde{K}/\widetilde{F}$ by

$$\mathfrak{D}_{\widetilde{K}/\widetilde{F}} = \mathrm{Disc}_{\widetilde{K}/\widetilde{F}}(\mathcal{O}_{\widetilde{K}}).$$

Acknowledgements

This project was started during the Women in Numbers 2 workshop at the Banff International Research Station; we thank the workshop organizers, Chantal David, Matilde Lalín, and Michelle Manes, and the staff at BIRS for their support.

2. The Bruinier-Yang formula

In this section, we describe the formula for $(\mathrm{CM}(K).\mathrm{G}_1)_\ell$ that was conjectured by Bruinier and Yang [BY06] and later proved by Yang [Yan]. One of the factors (which we denote by $R_{\widetilde{K}/\widetilde{F}}$) in this intersection formula is multiplicative, so it makes sense to express it in terms of local factors over each prime. The key result of this section is Theorem 2.5, which does exactly this. We start by recalling the necessary definitions to state the formula of Bruinier and Yang.

2.1. **Yang's Theorem.**

Definition 2.1. Let $\mathfrak{a} \subseteq \widetilde{F}$ be an ideal. We define

$$R_{\widetilde{K}/\widetilde{F}}(\mathfrak{a}) := \#\{\mathfrak{n} \subset \mathcal{O}_{\widetilde{K}} \mid \mathrm{Norm}_{\widetilde{K}/\widetilde{F}}(\mathfrak{n}) = \mathfrak{a}\}.$$

The following proves a special case of the conjecture of Bruinier and Yang, which we will refer to throughout as the Bruinier-Yang formula.

Theorem 2.2. [Yan, Thm. 1.2] *Assume that D and $\widetilde{D}$ are congruent to 1 modulo 4 and prime. Further assume that $\mathcal{O}_K = \mathcal{O}_F[(w + \sqrt{A + B\sqrt{D}})/2]$ for some $w \in \mathcal{O}_F$; this implies that $\widetilde{D} = A^2 - B^2 D$. Then for each rational prime ℓ, $(G_1.CM(K))_\ell/(\log \ell)$ equals*

$$\sum_{\delta = \frac{D-x^2}{4} \in \mathbb{Z}_{\geq 0}} \sum_{\substack{n \text{ s.t. } \frac{n+\delta\sqrt{\widetilde{D}}}{2D} \in \mathfrak{D}_{\widetilde{K}/\widetilde{F}}^{-1} \\ |n| < \delta\sqrt{\widetilde{D}}}} B_{\frac{n+\delta\sqrt{\widetilde{D}}}{2D}}(\ell), \tag{2.1}$$

where x is some integer, and

$$B_t(\ell) = \sum_{\mathfrak{l} \mid \ell} \begin{cases} 0 & \text{if } \mathfrak{l} \text{ splits in } \widetilde{K} \\ \frac{1}{2}(v_{\mathfrak{l}}(t) + 1) R_{\widetilde{K}/\widetilde{F}}(t\mathfrak{D}_{\widetilde{K}/\widetilde{F}}\mathfrak{l}^{-1}) f(\mathfrak{l}/\ell) & \text{otherwise,} \end{cases}$$

where the sum ranges over prime ideals $\mathfrak{l}$ of $\mathcal{O}_{\widetilde{F}}$ lying over ℓ and $f(\mathfrak{l}/\ell)$ denotes the inertial degree of $\mathfrak{l}$ over $\mathcal{O}_F$.

Remarks 2.3.

(1) According to [KW89], if $A^2 - B^2 D$ is not a square, then K is primitive, so this assumption is certainly satisfied if $\widetilde{D}$ is prime or squarefree.
(2) In Lemma 4.4 and Corollary 4.5 of [BY06], it is proved that under the assumptions of the above theorem, $\mathrm{Norm}(\mathfrak{D}_{\widetilde{K}/\widetilde{F}}) = D$.
(3) If $D = 5$ so that the only value for δ is 1, then Yang [Yan10] showed that the same statement holds if the assumption that $\widetilde{D}$ is 1 modulo 4 and prime is replaced with the assumption that $\widetilde{D}$ is 1 modulo 4 and squarefree.
(4) Yang's theorem and the Bruinier-Yang conjecture actually deal with intersections of Hirzebruch-Zagier divisors with the CM-cycle on Hilbert modular surfaces. However, as the cycle $CM(K)$ naturally lives on a Hilbert modular surface, and the pullback of G_1 can be expressed as a sum of Hirzebruch-Zagier divisors [vdG88, Prop. 2.8, Chap. IX], the work of Yang implies Theorem 2.2.

2.2. **A local interpretation of the Bruinier-Yang formula.**

Definition 2.4. Let p be a rational prime, and let $\mathfrak{a}$ be an ideal in $\widetilde{F}$. Then we define:

$$\varepsilon_{\widetilde{K}/\widetilde{F}}(p,\mathfrak{a}) := \prod_{\mathfrak{p}|p, v_{\mathfrak{p}}(\mathfrak{a})>0} \begin{cases} \frac{1}{2}(1+(-1)^{v_{\mathfrak{p}}(\mathfrak{a})}) & \text{if } \mathfrak{p} \text{ is inert in } \widetilde{K} \\ v_{\mathfrak{p}}(\mathfrak{a})+1 & \text{if } \mathfrak{p} \text{ is split in } \widetilde{K} \\ 1 & \text{otherwise.} \end{cases}$$

Let $n \in \mathbb{Z}$ be such that $|n| < \delta\sqrt{\widetilde{D}}$ and such that $\mathfrak{N} := (\frac{n+\delta\sqrt{\widetilde{D}}}{2D})$ divides $\mathfrak{D}^{-1}_{\widetilde{K}/\widetilde{F}}$. For simplicity, we let $t = \frac{n+\delta\sqrt{\widetilde{D}}}{2D}$. Assume that $\mathrm{Norm}(\mathfrak{D}_{\widetilde{K}/\widetilde{F}}) = D$. Then we define

$$N := \mathrm{Norm}(\mathfrak{N}\mathfrak{D}_{\widetilde{K}/\widetilde{F}}) = \frac{\delta^2\widetilde{D}-n^2}{4D}.$$

Theorem 2.5. *Let ℓ be a rational prime. If $v_{\mathfrak{l}}(\mathfrak{N}\mathfrak{D}_{\widetilde{K}/\widetilde{F}}) = 0$ for all primes $\mathfrak{l}|\ell$ in $\mathcal{O}_{\widetilde{F}}$, then $B_t(\ell) = 0$. Assume that there exists exactly one prime $\mathfrak{l}|\ell$ in $\mathcal{O}_{\widetilde{F}}$ such that $v_{\mathfrak{l}}(\mathfrak{N}\mathfrak{D}_{\widetilde{K}/\widetilde{F}}) > 0$ and this prime $\mathfrak{l}$ is unramified in $\widetilde{K}$. Then*

$$B_t(\ell) = \begin{cases} \frac{v_{\mathfrak{l}}(\mathfrak{N})+1}{2} f(\mathfrak{l}/l) \prod_{p|N, p\neq\ell} \varepsilon_{\widetilde{K}/\widetilde{F}}(p, \mathfrak{N}\mathfrak{D}_{\widetilde{K}/\widetilde{F}}) & \text{if } \mathfrak{l} \text{ is inert in } \widetilde{K}/\widetilde{F}, \\ & \text{and } v_{\mathfrak{l}}(\mathfrak{N}) \equiv 1 \bmod 2 \\ 0 & \text{otherwise.} \end{cases} \tag{2.2}$$

Proof. If $v_{\mathfrak{l}}(\mathfrak{N}\mathfrak{D}_{\widetilde{K}/\widetilde{F}}) = 0$ for all primes $\mathfrak{l}$ in $\mathcal{O}_{\widetilde{F}}$ lying over ℓ, then $\mathfrak{l}^{-1}\mathfrak{N}\mathfrak{D}_{\widetilde{K}/\widetilde{F}}$ is not integral so it cannot be the norm of an integral ideal in $\mathcal{O}_{\widetilde{K}}$. Thus,

$$R_{\widetilde{K}/\widetilde{F}}(\mathfrak{l}^{-1}\mathfrak{N}\mathfrak{D}_{\widetilde{K}/\widetilde{F}}) = 0$$

for all $\mathfrak{l}|\ell$ and so $B_t(\ell) = 0$.

Henceforth, assume that there exists exactly one prime $\mathfrak{l}|\ell$ in $\mathcal{O}_{\widetilde{F}}$ such that $v_{\mathfrak{l}}(\mathfrak{N}\mathfrak{D}_{\widetilde{K}/\widetilde{F}}) > 0$ and this prime $\mathfrak{l}$ is unramified in $\widetilde{K}$. Then for any $\mathcal{O}_{\widetilde{F}}$-prime $\mathfrak{l}'|\ell$, $\mathfrak{l}' \neq \mathfrak{l}$, the ideal $\mathfrak{l}'^{-1}\mathfrak{N}\mathfrak{D}_{\widetilde{K}/\widetilde{F}}$ is not integral and so $R_{\widetilde{K}/\widetilde{F}}(\mathfrak{l}'^{-1}\mathfrak{N}\mathfrak{D}_{\widetilde{K}/\widetilde{F}}) = 0$. Thus we have the simplified expression

$$B_t(\ell) = \begin{cases} 0 & \text{if } \mathfrak{l} \text{ splits in } \widetilde{K} \\ \frac{1}{2}(v_{\mathfrak{l}}(\mathfrak{N})+1) R_{\widetilde{K}/\widetilde{F}}(\mathfrak{N}\mathfrak{D}_{\widetilde{K}/\widetilde{F}}\mathfrak{l}^{-1}) f(\mathfrak{l}/\ell) & \text{otherwise.} \end{cases}$$

To prove the local formula, first assume that $\mathfrak{l}$ is not inert in $\widetilde{K}/\widetilde{F}$. By assumption, $\mathfrak{l}$ is also unramified, so $\mathfrak{l}$ must be split and $B_{\mathfrak{N}}(\ell) = 0$. If $\mathfrak{l}$ is inert in $\widetilde{K}/\widetilde{F}$ and $v_{\mathfrak{l}}(\mathfrak{N}) = v_{\mathfrak{l}}(\mathfrak{N}\mathfrak{D}_{\widetilde{K}/\widetilde{F}})$ is even, then $v_{\mathfrak{l}}(\mathfrak{l}^{-1}\mathfrak{N}\mathfrak{D}_{\widetilde{K}/\widetilde{F}})$ is odd. But since $\mathfrak{l}$ is inert, the $\mathfrak{l}$-valuation of $\mathrm{Norm}_{\widetilde{K}/\widetilde{F}}(\mathfrak{B})$ is even for any ideal $\mathfrak{B}$ of $\widetilde{K}$. Thus $R(\mathfrak{l}^{-1}\mathfrak{N}\mathfrak{D}_{\widetilde{K}/\widetilde{F}}) = 0 = B_t(\ell)$.

From now on, we may assume that $\mathfrak{l}$ is inert in $\widetilde{K}$ and that $v_{\mathfrak{l}}(\mathfrak{N})$ is odd. Recall that by definition, we have $R_{\widetilde{K}/\widetilde{F}}(\mathfrak{l}^{-1}\mathfrak{N}\mathfrak{D}_{\widetilde{K}/\widetilde{F}}) = \#\{\mathfrak{a} \subset \mathcal{O}_{\widetilde{K}} \mid \mathrm{Norm}_{\widetilde{K}/\widetilde{F}}(\mathfrak{a}) = \mathfrak{N}\mathfrak{D}_{\widetilde{K}/\widetilde{F}}\mathfrak{l}^{-1}\}$.

By the unique factorization of ideals in $\mathcal{O}_{\widetilde{K}}$ and $\mathcal{O}_{\widetilde{F}}$,

$$R_{\widetilde{K}/\widetilde{F}}(\mathfrak{N}\mathfrak{D}_{\widetilde{K}/\widetilde{F}}\mathfrak{l}^{-1}) = \prod_{p} \prod_{\mathfrak{p}|p} R_{\widetilde{K}/\widetilde{F}}(\mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{N}\mathfrak{D}_{\widetilde{K}/\widetilde{F}}\mathfrak{l}^{-1})}).$$

Since the ideal $\mathfrak{ND}_{\widetilde{K}/\widetilde{F}}\mathfrak{l}^{-1}$ is integral, we need only consider rational primes p such that $p|N$. Additionally, the factor at ℓ is equal to 1, so

$$R_{\widetilde{K}/\widetilde{F}}(\mathfrak{ND}_{\widetilde{K}/\widetilde{F}}\mathfrak{l}^{-1}) = \prod_{p|N, p\neq\ell}\prod_{\mathfrak{p}|p} R_{\widetilde{K}/\widetilde{F}}(\mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{ND}_{\widetilde{K}/\widetilde{F}})}).$$

Then it suffices to show that $\prod_{\mathfrak{p}|p} R_{\widetilde{K}/\widetilde{F}}(\mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{ND}_{\widetilde{K}/\widetilde{F}})}) = \varepsilon_{\widetilde{K}/\widetilde{F}}(p, \mathfrak{ND}_{\widetilde{K}/\widetilde{F}})$ for $p \neq \ell$.

Let $\mathfrak{p}|p$ be a prime ideal in $\mathcal{O}_{\widetilde{F}}$. Let $v = v_{\mathfrak{p}}(\mathfrak{ND}_{\widetilde{K}/\widetilde{F}})$. If $\mathfrak{p}$ is inert in $\widetilde{K}$, then there is a unique prime $\mathfrak{P}$ lying over $\mathfrak{p}$ and $\mathrm{Norm}_{\widetilde{K}/\widetilde{F}}(\mathfrak{P}) = \mathfrak{p}^2$. Thus if v is odd, there are no ideals in $\mathcal{O}_{\widetilde{K}}$ whose relative norm has $\mathfrak{p}$-adic valuation v, and if v is even, $R_{\widetilde{K}/\widetilde{F}}(\mathfrak{p}^v) = 1$. Now suppose that $\mathfrak{p}$ splits in $\widetilde{K}$. Then we can write $\mathfrak{p} = \mathfrak{P}_1\mathfrak{P}_2$ and $\mathrm{Norm}_{\widetilde{K}/\widetilde{F}}(\mathfrak{P}_i) = \mathfrak{p}$ so the only ideals in $\mathcal{O}_{\widetilde{K}}$ with relative norm equal to $\mathfrak{p}^v$ are of the form $\mathfrak{P}_1^{n_1}\mathfrak{P}_2^{n_2}$, where $n_1 + n_2 = v$ and $0 \leq n_1, n_2 \leq v$. Thus $R_{\widetilde{K}/\widetilde{F}}(\mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{ND}_{\widetilde{K}/\widetilde{F}})}) = v + 1$. Finally, if $\mathfrak{p}\mathcal{O}_{\widetilde{K}} = \mathfrak{P}^2$ is ramified, then the only ideal in $\mathcal{O}_{\widetilde{K}}$ with relative norm $\mathfrak{p}^v$ is $\mathfrak{P}^v$, so $R_{\widetilde{K}/\widetilde{F}}(\mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{ND}_{\widetilde{K}/\widetilde{F}})}) = 1$. We observe that this matches the expression for $\varepsilon_{\widetilde{K}/\widetilde{F}}(p, \mathfrak{N})$ exactly. □

3. The Lauter-Viray formula

In this section, we describe the formula for $(\mathrm{CM}(K).\mathrm{G}_1)_\ell$ proved by the third and last author [LV]. As in the Bruinier-Yang formula, some of the factors in this intersection formula are multiplicative. The key result of this section is Theorem 3.3 where we show that the formula in [LV] has an expression involving products of local factors.

3.1. **A simplified version of the Lauter-Viray formula.** Throughout, we assume that $\mathcal{O}_K$ is freely generated over $\mathcal{O}_F$ and write η for a generator, i.e., $\mathcal{O}_K = \mathcal{O}_F[\eta]$. We define integers $\alpha_0, \alpha_1, \beta_0, \beta_1$ (depending on η) satisfying

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

Let ℓ be a rational prime and let δ be a positive integer such that $D - 4\delta$ is a square. We define

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

For any integer n such that $2D|(n + c_K)$ and $\frac{\delta^2\widetilde{D}-n^2}{4D}$ is a positive integer, we define

$$\begin{aligned}
t_u &:= \alpha_1\delta,\\
t_x &:= \alpha_0 + \frac{1}{2}(D - \sqrt{D-4\delta})\alpha_1,\\
d_u(n) &:= (\alpha_1\delta)^2 + 4\frac{(n+c_K)\delta}{2D},\\
d_x(n) &:= (\alpha_0 + \frac{1}{2}(D - \sqrt{D-4\delta})\alpha_1)^2 - 4\left(\beta_0 + \frac{1}{2}(D - \sqrt{D-4\delta})\beta_1 + \frac{n+c_K}{2D}\right),\\
t_{xu^\vee}(n) &= \beta_1\delta + \sqrt{D-4\delta}\frac{n+c_K}{2D}.
\end{aligned}$$

The curious reader may refer to [LV, §2] to see how these quantities arise.

Theorem 3.1. [LV, Thm. 2.10] *Assume that for every $\delta \in \mathbb{Z}_{>0}$ and $n \in \mathbb{Z}$ such that $D-4\delta$ is a square, $2D|(n+c_K\delta)$ and $N := \frac{\delta^2\widetilde{D}-n^2}{4D} \in \mathbb{Z}_{>0}$, we have that ℓ does not divide both δ and N and that $d_u(n)$ is a fundamental discriminant. Then $(\mathrm{CM}(K).G_1)_\ell/(\log \ell)$ equals*

$$\sum_{\substack{\delta\in\mathbb{Z}_{>0}\\ D-4\delta=\square}} \sum_{\substack{n\in\mathbb{Z},\\ 2D|n+c_K\delta\\ \delta^2\widetilde{D}-n^2\in 4D\mathbb{Z}_{>0}}} \mu(n)\tilde{\rho}_{d_u(n)}(N)R_{d_u(n)}(N\ell^{-1}), \tag{3.1}$$

where $R_d(A) = \#\{\mathfrak{b} \subseteq \mathcal{O}_d = \mathbb{Z}[\frac{d+\sqrt{d}}{2}] : \mathfrak{b} \text{ invertible }, \mathrm{Norm}(\mathfrak{b}) = A\}$,

$$\mu(n) = \begin{cases} v_\ell(N) & \text{if } \ell|\gcd(d_u(n), d_x(n)), \\ \frac{v_\ell(N)+1}{2} & \text{otherwise,} \end{cases}$$

$$\tilde{\rho}_d(A) = \begin{cases} 0 & \text{if } (d,-A)_p = -1 \\ & \text{for some } p|d, p\neq\ell, \\ 2^{\#\{p:p|\gcd(d,A),p\neq\ell\}} & \text{otherwise,} \end{cases}$$

and $(a,b)_p$ denotes the Hilbert symbol at p.

3.2. **A local interpretation of the Lauter-Viray formula.**

Definition 3.2. Let $\mathcal{O}_d = \mathbb{Z}[\frac{d+\sqrt{d}}{2}]$. Define

$$\varepsilon_d(p,A) = \begin{cases} \frac{1}{2}(1+(-1)^{v_p(A)}) & \text{if } p \text{ is inert in } \mathcal{O}_d \\ v_p(A)+1 & \text{if } p \text{ is split in } \mathcal{O}_d \\ 2 & \text{if } p|d \text{ and } (d,-A)_p = 1 \\ 0 & \text{otherwise.} \end{cases}$$

Theorem 3.3. *For any δ, n, N which arise as in Theorem 3.1, let $d_u = d_u(n)$ and $d_x = d_x(n)$. Let ℓ be a prime that does not ramify in both $\mathcal{O}_{d_u}$ and $\mathcal{O}_{d_x}$. Then*

$$\mu(n)R_{d_u}(\ell^{-1}N)\tilde{\rho}_{d_u}(N) = \begin{cases} \mu(n)\prod_{p|N,p\neq\ell}\varepsilon_{d_u}(p,N) & \text{if } \ell \text{ is inert in } \mathcal{O}_{d_u} \text{ or } \mathcal{O}_{d_x} \\ & \text{and } v_\ell(N) \equiv 1 \bmod 2 \\ 0 & \text{otherwise.} \end{cases} \tag{3.2}$$

Proof. Recall that the Hilbert symbol $(a,b)_p$ remains unchanged when a is multiplied by a norm from $\mathbb{Q}_p(\sqrt{b})$. Thus since $d_xd_u = \mathrm{Norm}_{\mathbb{Q}_p(\sqrt{-N})}(t_xt_u - 2t_{xu^\vee} - 2\sqrt{-N})$ [LV, Eqn. 3.6], we have

$$(d_u,-N)_p = (d_x,-N)_p$$

for all primes p (including ∞).

Assume that ℓ is split in $\mathcal{O}_{d_u}$ or $\mathcal{O}_{d_x}$, or that ℓ is inert in $\mathcal{O}_{d_u}$ or $\mathcal{O}_{d_x}$ and $v_\ell(N)$ is even. Then the right hand side of formula 3.2 is zero. If ℓ is split in $\mathcal{O}_{d_u}$ or $\mathcal{O}_{d_x}$, then the Hilbert symbol $(d_u,-N)_\ell = 1$ because either d_u or d_x is a square modulo ℓ. Recall that if $\mathbb{Q}_\ell(\sqrt{a})$ is a nontrivial unramified extension of $\mathbb{Q}_\ell$, then $(a,b)_\ell = 1$ if and only if $v_\ell(b)$ is even ([Ser70, Thm 1, p. 39]). Thus if ℓ is inert in $\mathcal{O}_{d_u}$ or $\mathcal{O}_{d_x}$ and $v_\ell(N)$ is even then $(d_u,-N)_\ell = 1$. By [LV, Proof of Cor. 2.7] d_u is negative and so $(d_u,-N)_\infty = -1$. Therefore, by the product formula, there exists some prime $p \neq \ell$ such that $(d_u,-N)_p = -1$. If p is ramified in $\mathcal{O}_{d_u}$, then this is exactly the condition to have $\tilde{\rho}_{d_u}(N) = 0$, so the left hand side

of formula 3.2 is also zero. If p is unramified in $\mathcal{O}_{d_u}$, then since $(d_u, -N)_p = -1$, p must be inert in $\mathcal{O}_{d_u}$ and $v_p(N)$ must be odd by the same argument as above. In this case, there is no ideal in $\mathcal{O}_{d_u}$ with norm $\ell^{-1}N$ and so $R_{d_u}(\ell^{-1}N) = 0$.

Since, by assumption, ℓ does not ramify in both $\mathcal{O}_{d_u}$ and $\mathcal{O}_{d_x}$, the remaining case is when ℓ is inert in $\mathcal{O}_{d_u}$ or $\mathcal{O}_{d_x}$ and $v_\ell(N)$ is odd. If ℓ is inert in $\mathcal{O}_{d_x}$, then since ℓ divides $N = \frac{1}{4}(d_x d_u - (d_x d_u - 2t)^2)$, ℓ is either inert or ramified in $\mathcal{O}_{d_u}$. In either case, $R_{d_u}(\ell^{2k}) = 1$ for any non-negative integer k, so

$$R_{d_u}(\ell^{-1}N) = \prod_{p|N} R_{d_u}(p^{v_p(\ell^{-1}N)}) = \prod_{p|N, p\neq\ell} R_{d_u}(p^{v_p(N)}).$$

Then, by the same argument as in the proof of Theorem 2.5,

$$R_{d_u}(\ell^{-1}N) = \prod_{p|N, p\neq\ell} \begin{cases} \frac{1}{2}(1 + (-1)^{v_p(N)}) & \text{if } p \text{ is inert in } \mathcal{O}_{d_u}, \\ v_p(N) + 1 & \text{if } p \text{ is split in } \mathcal{O}_{d_u}, \\ 1 & \text{if } p | d_u. \end{cases}$$

Furthermore, it follows from the definition of $\tilde{\rho}_{d_u}$ that

$$\tilde{\rho}_{d_u}(N) = \prod_{\substack{p|\gcd(N,d_u), \\ p\neq\ell}} \begin{cases} 2 & \text{if } (d_u, -N)_p = 1, \\ 0 & \text{if } (d_u, -N)_p = -1. \end{cases}$$

From these two local expansions, it is clear that

$$\mu(n) R_{d_u}(\ell^{-1}N) \tilde{\rho}_{d_u}(N) = \mu(n) \prod_{p|N, p\neq\ell} \varepsilon_{d_u}(p, N)$$

if ℓ is inert in $\mathcal{O}_{d_u}$ or $\mathcal{O}_{d_x}$ and $v_\ell(N) \equiv 1 \bmod 2$. This completes the proof. □

4. Relative integral bases

In the previous section (and hence throughout the paper), a number of quantities, such as $\alpha_0, \alpha_1, \beta_0, \beta_1$ and the others defined in terms of these, are expressed in a way that depends on the form of the integral basis $\{1, \eta\}$ for $\mathcal{O}_F$. In this section, we use a result of Spearman and Williams to determine the possible forms η can take, thus narrowing down the possibilities for the other quantities given in Section 3. Throughout, we let $A, B \in \frac{1}{2}\mathbb{Z}$ be such that $A + B\sqrt{D}$ is squarefree in $\mathcal{O}_F$ and such that $K = F(\sqrt{A + B\sqrt{D}})$.

Lemma 4.1. *Assume that D and $\widetilde{D}$ are 1 modulo 4 and squarefree and that $\mathcal{O}_K$ is freely generated over $\mathcal{O}_F$. Then a relative integral basis for K over F is $\{1, \eta\}$, where*

$$\eta = \frac{1 + \sqrt{A + B\sqrt{D}}}{2} \quad \text{or} \quad \eta = \frac{2B + \sqrt{D} + 2\sqrt{A + B\sqrt{D}}}{4}.$$

Furthermore, the latter case only occurs if $D \equiv 5 \bmod 8$ and $A, B \in \frac{1}{2}\mathbb{Z} \setminus \mathbb{Z}$.

Proof. In [SW96], Spearman and Williams give a necessary and sufficient condition for the existence of a relative integral basis for a quartic number field over a quadratic subfield. In addition, in the cases where a relative integral basis exists, they give an explicit description of such an integral basis. This lemma will follow almost immediately from their work.

Spearman and Williams use the classification of quartic number fields with a quadratic subfield that was given in an earlier paper of Huard, Spearman, and Williams [HSW95]; there are 51 cases with labels A1-A8, B1-B8, C1-C8, and D1-D27. If $D \equiv 5 \bmod 8$, then the field falls in cases C1 - C8 and if $D \equiv 1 \bmod 8$ then the field falls in cases D1-D27.

By [SW96, Thm 1], if $\widetilde{D}$ is squarefree, then K falls into one of nine cases, only five of which have the property that $D \equiv 1 \bmod 4$. These five cases are C2, C7, D3, D16, or D20. If $D \equiv 1 \bmod 8$, then by [SW96, Thm 2], $\eta = \frac{1+\sqrt{A+B\sqrt{D}}}{2}$.

Now consider the case when $D \equiv 5 \bmod 8$. By [SW96, Thm 2 and p.190], if $A, B \in \mathbb{Z}$, then $\eta = \frac{1+\sqrt{A+B\sqrt{D}}}{2}$ and otherwise $A, B \in \frac{1}{2}\mathbb{Z} \setminus \mathbb{Z}$ and $\eta = \frac{2B+\sqrt{D}+2\sqrt{A+B\sqrt{D}}}{4}$. □

We will use this lemma to give simplified expressions for the quantities $d_u(n)$, $d_x(n)$, and $t_{xu^\vee}(n)$ defined in §3.

Proposition 4.2. *Assume that D and $\widetilde{D}$ are 1 modulo 4 and squarefree and that $\mathcal{O}_K$ is freely generated over $\mathcal{O}_F$. Let $\delta \in \mathbb{Z}_{>0}$ be such that $D - 4\delta$ is a square and let $n \in \mathbb{Z}$ be such that $2D$ divides $(n + c_K\delta)$ and such that $\frac{\delta^2\widetilde{D}-n^2}{4D}$ is a positive integer. Then*

$$d_u(n) = \frac{\delta(2n + \delta 2A)}{D},$$
$$d_x(n) = A - B\sqrt{D - 4\delta} - \frac{2n + \delta 2A}{D}, \quad \text{and}$$
$$t_x t_u - 2t_{xu^\vee}(n) = B\delta - \frac{\sqrt{D - 4\delta}(n + \delta A)}{D}.$$

Moreover, $c_K \equiv 1 \bmod 2$ and $2c_K \equiv 2A \bmod D$.

Proof. Lemma 4.1 gives us two possible choices for η. In each case, we can explicitly give the values of α_i, β_i. If $\eta = \frac{1+\sqrt{A+B\sqrt{D}}}{2}$, we have $\alpha_0 = 1, \alpha_1 = 0, \beta_0 = \frac{1-A+BD}{4}$, and $\beta_1 = -\frac{B}{2}$. If $\eta = \frac{2B+\sqrt{D}+2\sqrt{A+B\sqrt{D}}}{4}$, we have $\alpha_0 = B - \frac{D}{2}, \alpha_1 = 1, \beta_0 = \frac{4B^2+D-4A}{16}$, and $\beta_1 = 0$. Using these values, we calculate $d_u(n)$, $d_x(n)$, and $t_x t_u - 2t_{xu^\vee}(n)$ and find that they have the desired expressions in both cases.

To prove the congruence conditions, recall that

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

If $\alpha_0 = 1$ and $\alpha_1 = 0$, then $c_K \equiv 1 \bmod 2$. Otherwise, $D \equiv 5 \pmod 8$, and so $\frac{1}{4}(D^2 - D) \equiv 1 \bmod 2$. Then, $c_K \equiv (\alpha_0^2 + \alpha_0\alpha_1 + \alpha_1^2) \bmod 2$. Since $\alpha_1 = 1$ in this case, we see that, regardless of the parity of α_0, $c_K \equiv 1 \bmod 2$.

Calculating c_K explicitly in each case, we see that c_K is either equal to A or $A - \frac{D}{2}$. In either case, it is clear that $2c_K \equiv 2A \bmod D$. □

5. Equality of indices

The remainder of the paper will focus on proving, under slightly weaker assumptions than those in Theorems 2.2 and 3.1 and *without* using Theorems 3.1 and 2.2, that the expressions (2.1) and (3.1) agree. Precisely, we will show:

Theorem 5.1. *Assume that:*

- D *is prime, and hence congruent to* 1 *modulo* 4,
- $\widetilde{D}$ *is squarefree and congruent to* 1 *modulo* 4,
- $\mathrm{Norm}(\mathfrak{D}_{\widetilde{K}/\widetilde{F}}) = D$, *and*
- *for all* $\delta \in \mathbb{Z}_{>0}$ *such that* $D - 4\delta$ *is a square, and for all* $n \in \mathbb{Z}$ *such that* $2D | n + c_K\delta$ *and* $4D | \delta^2\widetilde{D} - n^2$, $d_u(n)$ *is a* fundamental *discriminant, i.e.,* $d_u(n)$ *is the discriminant of a quadratic field.*

Then (2.1) *and* (3.1) *are equal.*

Corollary 5.2. *Retain the assumptions of Theorem 5.1. Then, the Bruinier-Yang conjectural formula for* $(\mathrm{CM}(K).\mathrm{G}_1)_\ell$ *holds.*

Both formula (2.1) and (3.1) involve summands indexed by two integers denoted δ and n. The index δ ranges over the same quantities in both (2.1) and (3.1). While it is not obvious, the same statement is true for the index n.

Proposition 5.3. *Assume that* D *and* $\widetilde{D}$ *are congruent to* 1 *modulo* 4 *and squarefree and that* $\mathrm{Norm}(\mathfrak{D}_{\widetilde{K}/\widetilde{F}}) = D$. *Fix a positive integer* δ *such that* $D - 4\delta$ *is a square. Then for any* $n \in \mathbb{Z}$,

$$\delta^2\widetilde{D} - n^2 \in 4D\mathbb{Z} \text{ and } n \equiv -\delta c_K \pmod{2D}$$

if and only if

$$\frac{n + \delta\sqrt{\widetilde{D}}}{2D} \in \mathfrak{D}^{-1}_{\widetilde{K}/\widetilde{F}}.$$

Remark 5.4. If we work with a different CM-type of K so that

$$\widetilde{K} = \widetilde{F}(\sqrt{2A - 2\sqrt{A^2 - B^2D}}),$$

then the indices n are in one-to-one correspondance, but not necessarily equal. Indeed, the correspondence would be that

$$\delta^2\widetilde{D} - n^2 \in 4D\mathbb{Z} \text{ and } n \equiv -\delta c_K \pmod{2D}$$

if and only if

$$\frac{-n + \delta\sqrt{\widetilde{D}}}{2D} \in \mathfrak{D}^{-1}_{\widetilde{K}/\widetilde{F}}.$$

Proof. We will need the factorization of $\langle p \rangle$ in $\mathcal{O}_{\widetilde{F}}$ for any $p|D$, so we present this first. Recall that A and B are chosen to be in $\frac{1}{2}\mathbb{Z}$ such that $\widetilde{D} = A^2 - B^2D$. Since $2A$ is a solution of $X^2 - 4\widetilde{D}$ mod D and $2 \nmid D$, for any $p|D$, we can factor $\langle p \rangle$ in $\mathcal{O}_{\widetilde{F}}$ as $\mathfrak{p}_1\mathfrak{p}_2$ where $\mathfrak{p}_1 = (2A - 2\sqrt{\widetilde{D}}, p)$ and $\mathfrak{p}_2 = (2A + 2\sqrt{\widetilde{D}}, p)$. Note that $\mathfrak{p}_1 = \mathfrak{p}_2$ if and only if $p|\widetilde{D}$ as well as D. The norm of $\mathfrak{D}_{\widetilde{K}/\widetilde{F}}$ is equal to D and since $p|D$ one of $\mathfrak{p}_1$ or $\mathfrak{p}_2$ must ramify in $\widetilde{K}/\widetilde{F}$. Since D is squarefree, at most one of $\mathfrak{p}_1$ or $\mathfrak{p}_2$ ramifies and $\mathfrak{D}_{\widetilde{K}/\widetilde{F}}$ has $\mathfrak{p}_i$-adic valuation at most 1. Recall that $\widetilde{K} = \mathbb{Q}(\sqrt{2A + 2\sqrt{\widetilde{D}}})$, thus $\mathfrak{p}_2|\mathfrak{D}_{\widetilde{K}/\widetilde{F}}$.

First assume that $\delta^2\widetilde{D} - n^2 \in 4D\mathbb{Z}$ and that $n \equiv -\delta c_K \pmod{2D}$; we will show that $\frac{n+\delta\sqrt{\widetilde{D}}}{2D} \in \mathfrak{D}^{-1}_{\widetilde{K}/\widetilde{F}}$. Since $\delta^2\widetilde{D} - n^2$ is divisible by 4, n must be congruent to δ modulo 2 and thus $\frac{n+\delta\sqrt{\widetilde{D}}}{2}$ is integral. Further, since $\mathfrak{D}_{\widetilde{K}/\widetilde{F}}$ is integral, so is $(\frac{n+\delta\sqrt{\widetilde{D}}}{2})\mathfrak{D}_{\widetilde{K}/\widetilde{F}}$. To prove that

$\frac{n+\delta\sqrt{\widetilde{D}}}{2D} \in \mathfrak{D}_{\widetilde{K}/\widetilde{F}}^{-1}$, we will show that every prime lying over p for $p|D$ either divides $\frac{n+\delta\sqrt{\widetilde{D}}}{2}$ or $\mathfrak{D}_{\widetilde{K}/\widetilde{F}}$. In addition, if p also divides $\widetilde{D}$, then we will show that the unique prime $\mathfrak{p}$ lying over p divides $\mathfrak{D}_{\widetilde{K}/\widetilde{F}}$ and $\frac{n+\delta\sqrt{\widetilde{D}}}{2}$. Note that we have $p > 2$ since D and $\widetilde{D}$ are assumed to be 1 modulo 4.

By assumption, $2D|(n + c_K\delta)$ and by Proposition 4.2 we have $2c_K \equiv 2A \bmod D$, so

$$2n + 2\delta\sqrt{\widetilde{D}} \equiv -2\delta A + 2\delta\sqrt{\widetilde{D}} \equiv 0 \bmod \mathfrak{p}_1$$

and thus $v_{\mathfrak{p}_1}(\frac{n+\delta\sqrt{\widetilde{D}}}{2D}) > 0$. We have already seen that $\mathfrak{p}_2|\mathfrak{D}_{\widetilde{K}/\widetilde{F}}$. Therefore, $\frac{n+\delta\sqrt{\widetilde{D}}}{2D} \in \mathfrak{D}_{\widetilde{K}/\widetilde{F}}^{-1}$.

Now we prove the reverse direction. Assume that $\frac{n+\delta\sqrt{\widetilde{D}}}{2D} \in \mathfrak{D}_{\widetilde{K}/\widetilde{F}}^{-1}$. Taking the absolute norm, we have

$$\begin{aligned} N_{\widetilde{F}/\mathbb{Q}}\left(\left(\frac{n+\delta\sqrt{\widetilde{D}}}{2D}\right)\mathfrak{D}_{\widetilde{F}/\widetilde{K}}\right) &= \frac{n^2-\delta^2\widetilde{D}}{4D^2} \cdot N_{\widetilde{F}/\mathbb{Q}}(\mathfrak{D}_{\widetilde{K}/\widetilde{F}}) \\ &= \frac{n^2-\delta^2\widetilde{D}}{4D} \cdot \frac{N_{\widetilde{F}/\mathbb{Q}}(\mathfrak{D}_{\widetilde{K}/\widetilde{F}})}{D} \in \mathbb{Z}. \end{aligned}$$

Since $N_{\widetilde{F}/\mathbb{Q}}(\mathfrak{D}_{\widetilde{K}/\widetilde{F}}) = D$, we have $\delta^2\widetilde{D} - n^2 \in 4D\mathbb{Z}$.

To prove the congruence condition, we use the fact that $\mathfrak{p}_2|\mathfrak{D}_{\widetilde{K}/\widetilde{F}}$. Since $\mathrm{Norm}(\mathfrak{D}_{\widetilde{K}/\widetilde{F}})$ is squarefree and p divides $\frac{n+\delta\sqrt{\widetilde{D}}}{2}\mathfrak{D}_{\widetilde{K}/\widetilde{F}}$, this implies that $\mathfrak{p}_1|(n+\delta\sqrt{\widetilde{D}})/2$. Since $2n+2\delta\sqrt{\widetilde{D}} \equiv 2n + 2\delta A \pmod{\mathfrak{p}_1}$, the integer $2n + 2\delta A$ is contained in $\mathfrak{p}_1$ and hence is 0 modulo p, for all $p|D$. This implies that $n + \delta A \equiv n + c_K\delta \equiv 0 \bmod D$. We have already shown that $\delta^2\widetilde{D} - n^2 \in 4\mathbb{Z}$, which implies that $n \equiv \delta \pmod 2$. Finally, by Proposition 4.2, $c_K \equiv 1 \pmod 2$. Thus, $n \equiv \delta c_K \pmod 2$, and the proof is complete. □

6. Equality of summands

By the results of the previous section, both formula (2.1) and formula (3.1) sum over the same values δ and n. Thus, to prove that the formulas agree, it suffices to show that for a fixed δ and n, the corresponding summands of formula (2.1) and (3.1) are equal. The goal of the present section is to prove this equality.

Throughout, we work with a fixed positive integer δ and a fixed integer n such that

$$D - 4\delta = \square, \quad n + c_K\delta \equiv 0 \bmod 2D, \quad \text{and } N := \frac{\delta^2\widetilde{D} - n^2}{4D} \in \mathbb{Z}_{>0}.$$

For simplicity, we write $d_u := d_u(n)$ and $d_x := d_x(n)$. We let $\mathcal{O}_{d_u}$ and $\mathcal{O}_{d_x}$ denote the quadratic imaginary orders of discriminant d_u and d_x respectively.

Precisely, in this section we prove:

Theorem 6.1. *Retain the assumptions from Theorem 5.1. Then for any prime ℓ,*

$$\mu(n)R_{d_u}(\ell^{-1}N)\tilde{\rho}_{d_u}(N) = \sum_{\mathfrak{l}|\ell} \begin{cases} 0 & \text{if } \mathfrak{l} \text{ splits in } \widetilde{K} \\ \frac{v_{\mathfrak{l}}(\mathfrak{N})+1}{2} f(\mathfrak{l}/\ell) R_{\widetilde{K}/\widetilde{F}}(\mathfrak{l}^{-1}\mathfrak{N}\mathfrak{D}_{\widetilde{K}/\widetilde{F}}) & \text{otherwise,} \end{cases} \tag{6.1}$$

where $\mathfrak{N} = (\frac{n+\delta\sqrt{\widetilde{D}}}{2D})$.

In §6.1, we prove restrictions on the prime divisors of N. These restrictions will prove useful in later sections, and they also allow us to give a simplified formula for $\mu(n)$. In §6.2, we consider the splitting behavior in $\mathcal{O}_{d_u}$ and $\mathcal{O}_{d_x}$ of primes p dividing N and relate it to the splitting behavior in $\widetilde{K}$ of primes $\mathfrak{p}$ dividing $\mathfrak{N}$. We use this in §6.3 to show that for each prime $p \neq \ell$, the local factor at p in formula (2.2) agrees with the local factor at p in formula (3.2). Finally, in §6.4, we explain how these ingredients come together to prove Theorem 6.1.

6.1. **Reduction steps.**

Lemma 6.2. *Retain the assumptions from Theorem 5.1. Then* δ *and* $N = \frac{\delta^2\widetilde{D}-n^2}{4D}$ *are relatively prime.*

Proof. First suppose that p is an odd prime. If p divides both δ and $\frac{\delta^2\widetilde{D}-n^2}{4D}$, p must also divide n. Since D is prime and $p \leq \delta < D$, p cannot divide D, and so p^2 must divide $d_u(n) = \frac{\delta(2n+\delta 2A)}{D}$. This violates the hypothesis that $d_u(n)$ is the discriminant of an imaginary quadratic field.

Now let $p = 2$ and assume that $p|N$ and $p|\delta$. Then since $D - 4\delta$ is a square, D must be congruent to 1 modulo 8. Since $\widetilde{D} = A^2 - B^2D$ is 1 modulo 4, A and B must be integers and A must be odd. By assumption, $8|\delta^2\widetilde{D} - n^2$ and $2|\delta$, so $n \equiv \delta \equiv \delta A \bmod 4$. Thus $d_u(n) = 2\delta(n + \delta A)/D$ is 0 modulo 16, which gives a contradiction. □

Proposition 6.3. *Assume that* $\widetilde{D}$ *is squarefree and fix a prime* p *that does not divide* δ*. If* $p|N$*, then* p *cannot divide both* $d_u(n)$ *and* $d_x(n)$*.*

Proof. Suppose p divides both $d_u(n)$ and $d_x(n)$. Recall that we have

$$\delta^2\widetilde{D} - n^2 = D\left(d_x(n)d_u(n) - (t_xt_u - 2t_{xu^\vee}(n))^2\right). \tag{6.2}$$

If $4pD$ divides the left hand side of this equation, then p must also divide $(t_xt_u - 2t_{xu^\vee}(n))$. Using the formulations for this quantity, $d_u(n)$, and $d_x(n)$ given in Proposition 4.2, we see that if $p|d_u(x)$, then $p|\frac{2n+\delta 2A}{D}$. If $p|\frac{n+\delta A}{D}$ and $p|(t_xt_u - 2t_{xu^\vee}(n))$, then $p|2B$. But, if p divides all of these quantities, by considering the expression for $d_x(n)$ in Proposition 4.2, we see that p must also divide $2A$. Furthermore, if $p = 2$, then this argument can be strengthened to show that A and B are even integers. However, A and B must be relatively prime, because $\widetilde{D} = A^2 - B^2D$ is assumed to be squarefree. Thus, p cannot divide both $d_u(n)$ and $d_x(n)$. □

Corollary 6.4. *Retain the assumptions from Theorem 5.1. If* $\ell|N$*, then* $\mu(n) = \frac{1}{2}(v_\ell(N)+1)$.

6.2. **Comparing valuations and splitting behavior.**

Lemma 6.5. *Retain the assumptions from Theorem 5.1. Let* $n \in \mathbb{Z}$ *be such that* $2D|(n+c_K\delta)$ *and that* $\frac{\delta^2\widetilde{D}-n^2}{4D} \in \mathbb{Z}_{>0}$*. Let* p *be a prime that divides* $\frac{\delta^2\widetilde{D}-n^2}{4D}$*. Then there is a unique prime* $\mathfrak{p} \in \mathcal{O}_{\widetilde{F}}$ *lying over* p *such that* $v_{\mathfrak{p}}\left(\frac{n+\delta\sqrt{\widetilde{D}}}{2D}\mathfrak{D}_{\widetilde{K}/\widetilde{F}}\right)$ *is positive. This prime* $\mathfrak{p}$ *is unramified in* $\widetilde{K}$*,* $f(\mathfrak{p}/p) = 1$*, and we have*

$$v_p\left(\frac{\delta^2\widetilde{D} - n^2}{4D}\right) = v_{\mathfrak{p}}\left(\frac{n+\delta\sqrt{\widetilde{D}}}{2D}\right) = v_{\mathfrak{p}}\left(\frac{n+\delta\sqrt{\widetilde{D}}}{2D}\mathfrak{D}_{\widetilde{K}/\widetilde{F}}\right).$$

Remark 6.6. This lemma shows that the assumptions in Theorem 5.1 imply the assumptions in Theorem 2.5.

Proof. By Lemma 6.2, $p \nmid \delta$, so there is at most one prime in $\mathcal{O}_{\widetilde{F}}$ lying over p that divides $\frac{n+\delta\sqrt{\widetilde{D}}}{2}$ and this prime has inertial degree 1 over p. First consider the case when $p \nmid D$. Since $\mathrm{Norm}(\mathfrak{D}_{\widetilde{K}/\widetilde{F}}) = D$, we have that for all $\mathfrak{p}|p$, $\mathfrak{p}$ is unramified in $\widetilde{K}$ and $v_{\mathfrak{p}}\left(\frac{n+\delta\sqrt{\widetilde{D}}}{2D}\mathfrak{D}_{\widetilde{K}/\widetilde{F}}\right) = v_{\mathfrak{p}}\left(\frac{n+\delta\sqrt{\widetilde{D}}}{2}\right)$. As

$$v_p\left(\frac{\delta^2\widetilde{D}-n^2}{4D}\right) = \sum_{\mathfrak{p}|p} v_{\mathfrak{p}}\left(\frac{n+\delta\sqrt{\widetilde{D}}}{2D}\mathfrak{D}_{\widetilde{K}/\widetilde{F}}\right), \tag{6.3}$$

this completes the proof.

Now consider the case when $p|D$. If p is ramified in $\widetilde{F}$, then $p|\widetilde{D}$. However, this contradicts the assumption that $\frac{\delta^2\widetilde{D}-n^2}{4D} \in p\mathbb{Z}_{>0}$ because $\widetilde{D}$ is squarefree and $p \nmid \delta$. Thus p is split in $\widetilde{F}$. Let $\mathfrak{p}_1$ and $\mathfrak{p}_2$ denote the two primes lying over p. Since $\mathrm{Norm}(\mathfrak{D}_{\widetilde{K}/\widetilde{F}}) = D$ and D is a prime, there is at most one prime lying over p that divides $\mathfrak{D}_{\widetilde{K}/\widetilde{F}}$; we may assume that this prime is $\mathfrak{p}_2$. Hence $v_{\mathfrak{p}_1}\left(\frac{n+\delta\sqrt{\widetilde{D}}}{2D}\mathfrak{D}_{\widetilde{K}/\widetilde{F}}\right) = v_{\mathfrak{p}_1}\left(\frac{n+\delta\sqrt{\widetilde{D}}}{2}\right) - 1$. By the assumption on n and Proposition 5.3, $\frac{n+\delta\sqrt{\widetilde{D}}}{2D}\mathfrak{D}_{\widetilde{K}/\widetilde{F}}$ is integral, and thus $v_{\mathfrak{p}_1}\left(\frac{n+\delta\sqrt{\widetilde{D}}}{2}\right) > 0$. This in turn implies that $\frac{1}{2}(n+\delta\sqrt{\widetilde{D}})$ is a $\mathfrak{p}_2$-adic unit. Combining this with (6.3), we see that $v_p\left(\frac{\delta^2\widetilde{D}-n^2}{4D}\right) = v_{\mathfrak{p}_1}\left(\frac{n+\delta\sqrt{\widetilde{D}}}{2D}\right)$ and $\mathfrak{p}_1 \nmid \mathfrak{D}_{\widetilde{K}/\widetilde{F}}$ as desired. □

Proposition 6.7. *Retain the assumptions from Theorem 5.1. Fix a prime p that divides $\frac{\delta^2\widetilde{D}-n^2}{4D}$ and let $\mathfrak{p}|p$ be the unique prime given in Lemma 6.5. The prime ideal $\mathfrak{p}$ splits in $\widetilde{K}$ if and only if p splits in at least one of $\mathcal{O}_{d_x}$ or $\mathcal{O}_{d_u}$. Similarly, $\mathfrak{p}$ is inert in $\widetilde{K}$ if and only if p is inert in at least one of $\mathcal{O}_{d_x}$ or $\mathcal{O}_{d_u}$.*

Proof. By Lemma 6.2 and Proposition 6.3, p does not ramify in both $\mathcal{O}_{d_u}$ and $\mathcal{O}_{d_x}$. Therefore, if p is not split in either $\mathcal{O}_{d_x}$ or $\mathcal{O}_{d_u}$, then p is inert in at least one of $\mathcal{O}_{d_u}$ and $\mathcal{O}_{d_x}$. Thus, the second claim of the lemma follows from the first claim.

As noted above, $\frac{\delta^2\widetilde{D}-n^2}{4D} = \frac{d_u d_x - (t_x t_u - 2t_{xu^\vee})^2}{4}$. Since $4Dp|(\delta^2\widetilde{D}-n^2)$, the product $d_u d_x$ is congruent to a square modulo p. Therefore, if p is split in one of $\mathcal{O}_{d_x}$ or $\mathcal{O}_{d_u}$, then p cannot be inert in the other order. If $p > 2$, the proof breaks into cases depending on whether or not p ramifies in $\mathcal{O}_{d_u}$. Recall, $d_u = \frac{2\delta(n+\delta A)}{D}$. Assume that $p|d_u$ and $p > 2$. Then, since $p \nmid \delta$ (Lemma 6.2), $2n + 2A\delta$ and $n + \delta\sqrt{\widetilde{D}}$ both have $\mathfrak{p}$-adic valuation strictly greater than $v_p(D)$, and hence so does $2A - 2\sqrt{\widetilde{D}}$. This in turn implies that p divides $2B$ and so $d_x = A - B\sqrt{D-4\delta} - \frac{2(n+\delta A)}{D} \equiv A \bmod p$. Recall that $\sqrt{2A+2\sqrt{\widetilde{D}}}$ generates the extension $\widetilde{K}/\widetilde{F}$. Consider the product

$$(2A + 2\sqrt{\widetilde{D}})d_x \equiv 4A \cdot A \pmod{\mathfrak{p}}. \tag{6.4}$$

Since $\widetilde{D}$ is squarefree, $4A^2$ is a nonzero square modulo $\mathfrak{p}$. Then (6.4) implies that $2A+2\sqrt{\widetilde{D}}$ and d_x are nonzero modulo $\mathfrak{p}$ and that $2A+2\sqrt{\widetilde{D}}$ is a square modulo $\mathfrak{p}$ if and only if d_x is a square modulo p. This shows that $\mathfrak{p}$ splits in $\widetilde{K}$ if and only if p splits in $\mathcal{O}_{d_x}$.

Suppose that $p \nmid d_u$ and $p > 2$. Then by the argument above, $2A-2\sqrt{\widetilde{D}}$ is a $\mathfrak{p}$-adic unit. Thus, if $p|2B$, we must have that $\mathfrak{p}|(2A+2\sqrt{\widetilde{D}})$. We will show that $(2A+2\sqrt{\widetilde{D}})d_u$ is congruent to a nonzero square modulo $\mathfrak{p}^{2v_p(2B)+1}$. This will show that $\mathfrak{p}$ splits in $\widetilde{K}$ if and only if p splits in $\mathcal{O}_{d_u}$.

Since $2A-2\sqrt{\widetilde{D}}$ is a $\mathfrak{p}$-adic unit, $v_{\mathfrak{p}}(2A+2\sqrt{\widetilde{D}}) = 2v_p(2B)$. By assumption, we also have that $v_{\mathfrak{p}}(\frac{n+\delta\sqrt{\widetilde{D}}}{2D})$ is positive, so

$$(2A+2\sqrt{\widetilde{D}})\delta^2\frac{2n/\delta+2\sqrt{\widetilde{D}}}{D} \in \mathfrak{p}^{2v_p(2B)+1}.$$

From this, we see that

$$(2A+2\sqrt{\widetilde{D}})d_u \equiv \frac{\delta^2}{D}(2A+2\sqrt{\widetilde{D}})(2A-2\sqrt{\widetilde{D}}) \equiv \delta^2(2B)^2 \bmod \mathfrak{p}^{2v_p(2B)+1}.$$

By Lemma 6.2, $p \nmid \delta$, so we obtain our result.

Henceforth, we assume that $p = 2$. Suppose that A and B are half-integers, i.e., that $2A$ and $2B$ are odd integers. Then $\frac{2n+2\delta\sqrt{\widetilde{D}}}{D}$ is zero modulo $\mathfrak{p}^3$, so $d_u = \delta^2\frac{2A+2n/\delta}{D} \equiv \delta^2\frac{2A-2\sqrt{\widetilde{D}}}{D} \bmod \mathfrak{p}^3$. Thus

$$(2A+2\sqrt{\widetilde{D}})d_u \equiv \delta^2(2B)^2 \bmod \mathfrak{p}^3.$$

Since $\delta 2B$ is odd, this shows that $\mathfrak{p}$ splits in $\widetilde{K}$ if and only if p splits in $\mathcal{O}_{d_u}$.

If A and B are integers, then d_u is necessarily divisible by 2 and $\frac{A+\sqrt{\widetilde{D}}}{2} \in \mathcal{O}_{\widetilde{F}}$. Suppose that $d_u \equiv 8 \bmod 16$ so $\frac{A+n/\delta}{2} \equiv 0 \bmod 2$. Then $\frac{A-\sqrt{\widetilde{D}}}{2} = \frac{A+n/\delta}{2} - \frac{n/\delta+\sqrt{\widetilde{D}}}{2}$ is 0 modulo $\mathfrak{p}$. The discriminants D and $\widetilde{D} = A^2 - B^2D$ are 1 modulo 4, so A must be odd and B must be even. Since $\frac{A-\sqrt{\widetilde{D}}}{2} \in \mathfrak{p}$, $A^2 \equiv \widetilde{D} \bmod 8$ and so B must be divisible by 4. Thus $\frac{A+\sqrt{\widetilde{D}}}{2}$ is a $\mathfrak{p}$-adic unit. Consider

$$\frac{A+\sqrt{\widetilde{D}}}{2} - d_x \equiv \frac{-A+\sqrt{\widetilde{D}}}{2} + B\sqrt{D-4\delta} \bmod \mathfrak{p}^3.$$

Since $\mathrm{Norm}(\frac{-A+\sqrt{\widetilde{D}}}{2}) = B^2D/4$ and D is 1 modulo 4, $v_{\mathfrak{p}}(\frac{-A+\sqrt{\widetilde{D}}}{2}) = v_p(B^2/4)$. If $v_p(B) \geq 3$, then $\frac{A+\sqrt{\widetilde{D}}}{2} \equiv d_x \bmod \mathfrak{p}^3$. If $v_p(B) = 2$, then $v_{\mathfrak{p}}(\frac{-A+\sqrt{\widetilde{D}}}{2})$ is also 2, so the sum $\frac{-A+\sqrt{\widetilde{D}}}{2} + B\sqrt{D-4\delta}$ has $\mathfrak{p}$-adic valuation at least 3. Therefore, in all cases, $\frac{A+\sqrt{\widetilde{D}}}{2} \equiv d_x \bmod \mathfrak{p}^3$ and so $\mathfrak{p}$ splits in $\widetilde{K}$ if and only if p splits in $\mathcal{O}_{d_u}$.

Finally we suppose that $d_u \equiv 4 \bmod 8$. By assumption, d_u is fundamental which implies that $\frac{A+n/\delta}{2}$ is 3 modulo 4. Since d_x is a quadratic discriminant and congruent to A modulo 4, A must be congruent to 1 modulo 4, so $\frac{A-n/\delta}{2}$ is 2 modulo 4. Both $\frac{A-n/\delta}{2}$ and $\frac{n/\delta+\sqrt{\widetilde{D}}}{2}$ are $\mathfrak{p}$-adic uniformizers, hence their sum and difference both have $\mathfrak{p}$-adic valuation at least

2. Moreover, at most one of the sum and difference have $\mathfrak{p}$-adic valuation exactly equal to 2. In particular, $\frac{A+\sqrt{\widetilde{D}}}{2}$ has positive valuation, so $v_p(B^2/4)$ must be positive (so B is 0 modulo 4) and $v_p(B^2/4) = v_{\mathfrak{p}}(\frac{A+\sqrt{\widetilde{D}}}{2})$. From this, we can see that $\mathfrak{p}$ splits in $\widetilde{K}$ if

$$\left(\frac{A+\sqrt{\widetilde{D}}}{2}\right)\left(\frac{A-\sqrt{\widetilde{D}}}{2}\right)^2 4B^{-2} = \left(\frac{A-\sqrt{\widetilde{D}}}{2}\right)D \tag{6.5}$$

is a square modulo $\mathfrak{p}^3$, and that $\mathfrak{p}$ is inert in $\widetilde{K}$ if (6.5) is a non-square modulo $\mathfrak{p}^3$.

If $B \equiv 4 \bmod 8$, then $v_{\mathfrak{p}}(\frac{A+\sqrt{\widetilde{D}}}{2}) = 2$ and $v_{\mathfrak{p}}(\frac{-A+2n/\delta+\sqrt{\widetilde{D}}}{2}) \geq 3$. Therefore

$$\frac{A-\sqrt{\widetilde{D}}}{2} \equiv n/\delta \equiv A+4 \bmod \mathfrak{p}^3,$$

and

$$d_x = A - B\sqrt{D-4\delta} - d_u/\delta \equiv A+4+4 \equiv A \bmod \mathfrak{p}^3,$$

so $\left(\frac{A-\sqrt{\widetilde{D}}}{2}\right) D \cdot d_x$ is equivalent to $D(A^2+4A)$ modulo $\mathfrak{p}^3$. Since $D-4\delta$ is a square and δ is odd, D must be 5 modulo 8. Thus $D(A^2+4A) \equiv 5(1+4) \equiv 1 \bmod 8$, so $\mathfrak{p}$ splits in $\widetilde{K}$ if and only if p splits in $\mathcal{O}_{d_x}$. If $B \equiv 0 \bmod 8$, then $v_{\mathfrak{p}}(\frac{A+\sqrt{\widetilde{D}}}{2}) \geq 3$ and so $\frac{A-\sqrt{\widetilde{D}}}{2} \equiv A \bmod \mathfrak{p}^3$. We also have $d_x \equiv A+4 \bmod 8$. Thus, as above, $\left(\frac{A-\sqrt{\widetilde{D}}}{2}\right) D \cdot d_x \equiv D(A^2+4A) \equiv 1 \bmod \mathfrak{p}^3$. This completes the proof. □

6.3. Comparing ε_{d_u} and $\varepsilon_{\widetilde{K}/\widetilde{F}}$.

Proposition 6.8. *Retain the assumptions from Theorem 5.1. Let $n \in \mathbb{Z}$ be such that $2D|(n+c_K\delta)$ and that $\frac{\delta^2\widetilde{D}-n^2}{4D} \in \ell\mathbb{Z}_{>0}$. Fix a prime $p \neq \ell$ that divides $N := \frac{\delta^2\widetilde{D}-n^2}{4D}$. Then*

$$\varepsilon_{d_u}(p,N) = \varepsilon_{\widetilde{K}/\widetilde{F}}(p, \mathfrak{ND}_{\widetilde{K}/\widetilde{F}}).$$

Proof. By Lemma 6.5, there is a unique prime $\mathfrak{p}$ lying over p such that $v_{\mathfrak{p}}(\mathfrak{ND}_{\widetilde{K}/\widetilde{F}})$ is positive. Thus,

$$\varepsilon_{\widetilde{K}/\widetilde{F}}(p, \mathfrak{ND}_{\widetilde{K}/\widetilde{F}}) = \begin{cases} \frac{1}{2}(1+(-1)^{v_{\mathfrak{p}}(\mathfrak{ND}_{\widetilde{K}/\widetilde{F}})}) & \text{if } \mathfrak{p} \text{ is inert in } \widetilde{K} \\ v_{\mathfrak{p}}(\mathfrak{ND}_{\widetilde{K}/\widetilde{F}})+1 & \text{if } \mathfrak{p} \text{ is split in } \widetilde{K} \\ 1 & \text{otherwise.} \end{cases}$$

Assume that $\mathfrak{p}$ is inert in $\widetilde{K}$. Then, by Proposition 6.7, p is inert in at least one of $\mathcal{O}_{d_u}$ or $\mathcal{O}_{d_x}$. If p is inert in $\mathcal{O}_{d_u}$, then

$$\varepsilon_{d_u}(p,N) = \frac{1}{2}(1+(-1)^{v_p(N)}) = \frac{1}{2}(1+(-1)^{v_{\mathfrak{p}}(\mathfrak{ND}_{\widetilde{K}/\widetilde{F}})}) = \varepsilon_{\widetilde{K}/\widetilde{F}}(p, \mathfrak{ND}_{\widetilde{K}/\widetilde{F}}),$$

as desired. (The middle equality follows from Lemma 6.5.) If p is not inert in $\mathcal{O}_{d_u}$, then p must be inert in $\mathcal{O}_{d_x}$. The equality $\frac{\delta^2\widetilde{D}-n^2}{4D} = \frac{d_u d_x - (t_x t_u - 2t_{xu^\vee})^2}{4}$, shows that $d_u d_x$ is congruent

to a square modulo p. Thus p is ramified in $\mathcal{O}_{d_u}$. In addition, by Lemma 6.5 and since p^2 does not divide d_u,

$$v_p\left(\frac{\delta^2\widetilde{D}-n^2}{4D}\right) = v_{\mathfrak{p}}(\mathfrak{N}\mathfrak{D}_{\widetilde{K}/\widetilde{F}}) = 1.$$

Since d_x is not a square modulo p and the p-valuation of N is odd, it follows again from [Ser70, Ch III, Thm 1] that

$$\left(d_u, \frac{n^2-\delta^2\widetilde{D}}{4D}\right)_p = \left(d_x, \frac{n^2-\delta^2\widetilde{D}}{4D}\right)_p = -1.$$

Thus $\varepsilon_{d_u}(p, \ell^{-1}N) = 0 = \frac{1}{2}(1+(-1)^{v_{\mathfrak{p}}(\mathfrak{N}\mathfrak{D}_{\widetilde{K}/\widetilde{F}})}) = \varepsilon_{\widetilde{K}/\widetilde{F}}(p, \mathfrak{N}\mathfrak{D}_{\widetilde{K}/\widetilde{F}})$.

If $\mathfrak{p}$ is not inert in $\widetilde{K}$, then, by Lemma 6.5, $\mathfrak{p}$ is split in $\widetilde{K}$. By Proposition 6.7, this implies that p is split in at least one of $\mathcal{O}_{d_x}$ or $\mathcal{O}_{d_u}$. If p is split in $\mathcal{O}_{d_u}$, then

$$\varepsilon_{d_u}(p, N) = v_p(N)+1 = v_{\mathfrak{p}}(\mathfrak{N}\mathfrak{D}_{\widetilde{K}/\widetilde{F}})+1 = \varepsilon_{\widetilde{K}/\widetilde{F}}(p, \mathfrak{N}\mathfrak{D}_{\widetilde{K}/\widetilde{F}}).$$

If p is not split in $\mathcal{O}_{d_u}$, then p is split in $\mathcal{O}_{d_x}$, and the same arguments as above show that p is ramified in $\mathcal{O}_{d_u}$, $v_p(\frac{\delta^2\widetilde{D}-n^2}{4D}) = 1$. Furthermore,

$$\left(d_u, \frac{n^2-\delta^2\widetilde{D}}{4D}\right)_p = \left(d_x, \frac{n^2-\delta^2\widetilde{D}}{4D}\right)_p = 1$$

and so $\varepsilon_{d_u}(p, N) = 2 = v_p(N)+1 = v_{\mathfrak{p}}(\mathfrak{N}\mathfrak{D}_{\widetilde{K}/\widetilde{F}})+1 = \varepsilon_{\widetilde{K}/\widetilde{F}}(p, \mathfrak{N}\mathfrak{D}_{\widetilde{K}/\widetilde{F}})$. This completes the proof. □

6.4. **Proof of Theorem 6.1.** Let $\mathfrak{l}$ denote the prime lying over ℓ such that $v_{\mathfrak{l}}(\frac{n+\delta\sqrt{\widetilde{D}}}{2D}\mathfrak{D}_{\widetilde{K}/\widetilde{F}})$ is positive; this is unique by Lemma 6.5. If $\mathfrak{l}$ is split in $\widetilde{K}$, then by Theorem 2.5 the right-hand side of (6.1) is zero. Additionally, by Proposition 6.7, if $\mathfrak{l}$ is split in $\widetilde{K}$, then ℓ is split in $\mathcal{O}_{d_u}$ or $\mathcal{O}_{d_x}$. By Theorem 3.3, this implies that the left-hand side of (6.1) is zero.

Since, by Lemma 6.5, $\mathfrak{l}$ is unramified in $\widetilde{K}$, we are left to consider the case when $\mathfrak{l}$ is inert in $\widetilde{K}$. By Proposition 6.7 this coincides with the case when ℓ is inert in at least one of $\mathcal{O}_{d_u}$ and $\mathcal{O}_{d_x}$. First assume that $v_{\mathfrak{l}}(\mathfrak{N})$ is even; by Lemma 6.5, $v_\ell(N)$ is also even. Then, by Theorems 2.5 and 3.3, both sides of (6.1) are 0.

Now suppose that $\mathfrak{l}$ is inert in $\widetilde{K}$ and that $v_{\mathfrak{l}}(\mathfrak{N})$ is odd. By Lemma 6.5, if $\mathfrak{l}'|\ell$ is a prime in $\widetilde{F}$ different from $\mathfrak{l}$, then $\mathfrak{l}'^{-1}\mathfrak{N}\mathfrak{D}_{\widetilde{K}/\widetilde{F}}$ is *not* integral. Therefore, $R(\mathfrak{l}'^{-1}\mathfrak{N}\mathfrak{D}_{\widetilde{K}/\widetilde{F}}) = 0$ and the right-hand side of (6.1) reduces to

$$\frac{v_{\mathfrak{l}}(\mathfrak{N})+1}{2}\cdot f(\mathfrak{l}/\ell)\cdot R_{\widetilde{K}/\widetilde{F}}(\mathfrak{l}^{-1}\mathfrak{N}\mathfrak{D}_{\widetilde{K}/\widetilde{F}}).$$

Using Theorems 2.5 and 3.3, Corollary 6.4, and Lemma 6.5 we deduce

$$\frac{v_{\mathfrak{l}}(\mathfrak{N})+1}{2}\cdot f(\mathfrak{l}/\ell)\cdot R_{\widetilde{K}/\widetilde{F}}(\mathfrak{l}^{-1}\mathfrak{N}\mathfrak{D}_{\widetilde{K}/\widetilde{F}}) = \frac{v_{\mathfrak{l}}(\mathfrak{N})+1}{2}\prod_{p|N, p\neq\ell}\varepsilon_{\widetilde{K}/\widetilde{F}}(p, \mathfrak{N}\mathfrak{D}_{\widetilde{K}/\widetilde{F}})$$

$$\mu(n)R_{d_u}(\ell^{-1}N)\tilde{\rho}_{d_u}(N) = \frac{v_\ell(N)+1}{2}\prod_{p|N, p\neq\ell}\varepsilon_{d_u}(p, N).$$

We apply Lemma 6.5 to show that $\frac{v_{\mathfrak{l}}(\mathfrak{N})+1}{2} = \frac{v_\ell(N)+1}{2}$ and Proposition 6.8 to give

$$\varepsilon_{\widetilde{K}/\widetilde{F}}(p, \mathfrak{ND}_{\widetilde{K}/\widetilde{F}}) = \varepsilon_{d_u}(p, N).$$

This completes the proof of Theorem 6.1. □

6.5. **Proof of Theorem 5.1.** Theorem 5.1 follows immediately from Proposition 5.3 and Theorem 6.1. □

6.6. **Proof of Corollary 5.2.** By Lemma 6.2, the assumptions of Theorem 5.1 imply the assumptions of Theorem 3.1. Thus, Theorems 3.1 and 5.1 complete the proof. □

References

[BY06] Jan Hendrik Bruinier and Tonghai Yang, *CM-values of Hilbert modular functions*, Invent. Math. **163** (2006), no. 2, 229–288, DOI 10.1007/s00222-005-0459-7. MR2207018 (2008b:11053) ↑1, 2, 2

[vdG88] Gerard van der Geer, *Hilbert modular surfaces*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], vol. 16, Springer-Verlag, Berlin, 1988. MR930101 (89c:11073) ↑4

[GL07] Eyal Z. Goren and Kristin E. Lauter, *Class invariants for quartic CM fields*, Ann. Inst. Fourier (Grenoble) **57** (2007), no. 2, 457–480. MR2310947 (2008i:11075) ↑1

[GL11] ———, *Genus 2 Curves with Complex Multiplication*, Int. Math. Res. Not., posted on 2011, 75 pp., DOI 10.1093/imrn/rnr052. ↑1

[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. ↑1

[HSW95] J. G. Huard, B. K. Spearman, and K. S. Williams, *Integral bases for quartic fields with quadratic subfields*, J. Number Theory **51** (1995), no. 1, 87–102, DOI 10.1006/jnth.1995.1036. MR1321725 (96a:11115) ↑4

[KW89] Luise-Charlotte Kappe and Bette Warren, *An Elementary Test for the Galois Group of a Quartic Polynomial*, Amer. Math. Monthly **96** (1989), 133–137. ↑1

[LV] Kristin Lauter and Bianca Viray, *An arithmetic intersection number for denominators of Igusa class polynomials*. Preprint, `arXiv:1210.7841`. ↑1, 3, 3.1, 3.1, 3.2

[Ser70] Jean-Pierre Serre, *Cours d'arithmétique*, Presses Universitaires de France, 1970. ↑3.2, 6.3

[Shi98] Goro Shimura, *Abelian Varieties with Complex Multiplication and Modular Functions*, Princeton, 1998. ↑1.3

[SW96] B. K. Spearman and K. S. Williams, *Relative integral bases for quartic fields over quadratic subfields*, Acta Math. Hungar. **70** (1996), no. 3, 185–192, DOI 10.1007/BF02188204. MR1374384 (97d:11156) ↑4

[Yan10] Tonghai Yang, *An arithmetic intersection formula on Hilbert modular surfaces*, Amer. J. Math. **132** (2010), no. 5, 1275–1309, DOI 10.1353/ajm.2010.0002. MR2732347 (2012a:11078) ↑1, 3

[Yan] ———, *Arithmetic intersection on a Hilbert modular surface and the Faltings height*. Preprint, 2007. ↑1, 2, 2.2

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

Department of Mathematics, Harvard University, 1 Oxford Street, Cambridge, MA 02138, USA
E-mail address: jen@math.harvard.edu
URL: http://www.math.harvard.edu/~jen/

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, MIT, 77 Massachusetts Avenue, Cambridge, MA 02139, USA
E-mail address: jmypark@math.mit.edu
URL: http://math.mit.edu/~jmypark/

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