ASIAN J. MATH.
Vol. 17, No. 2, pp. 335–382, June 2013

004

# ARITHMETIC INTERSECTION ON A HILBERT MODULAR SURFACE AND THE FALTINGS HEIGHT[*]

TONGHAI YANG[†]

**Abstract.** In this paper, we prove an explicit arithmetic intersection formula between arithmetic Hirzebruch-Zagier divisors and arithmetic CM cycles on a Hilbert modular surface over $\mathbb{Z}$. As applications, we obtain the first 'non-abelian' Chowla-Selberg formula, which is a special case of Colmez's conjecture; an explicit arithmetic intersection formula between arithmetic Humbert surfaces and CM cycles in the arithmetic Siegel modular variety of genus two; Lauter's conjecture about the denominators of CM values of Igusa invariants; and a result about bad reduction of CM genus two curves.

**Key words.** Hilbert modular surface, Hirzebruch-Zagier divisor, arithmetic intersection, Colmez conjecture, Igusa invariants, Faltings' height.

**AMS subject classifications.** 11G15, 11F41, 14K22.

## 1. Introduction.

Intersection theory has played a central role not only in algebraic geometry but also in number theory and arithmetic geometry, such as Arakelov theory, Faltings's proof of Mordell conjecture, the Birch and Swinnerton-Dyer conjecture, and the Gross-Zagier formula, to name a few. In a lot of cases, explicit intersection formulae are needed as in the Gross-Zagier formula ([GZ1]), its generalization to totally real number fields by Shou-Wu Zhang ([Zh1], [Zh2], [Zh3]), recent work on arithmetic Siegel-Weil formula by Kudla, Rapoport, and the author (e.g., [Ku1], [KR1], [KR2], [KRY1], [KRY2]), and Bruinier, Burgos-Gil, and Kühn's work on arithmetic Hilbert modular surfaces. In other cases, the explicit formulae are simply beautiful as in the work of Gross and Zagier on singular moduli [GZ2], the work of Gross and Keating on modular polynomials [GK](not to mention the really classical Bézout's theorem). In all these works, intersecting cycles are of the same type and symmetric.

In this paper, we consider the arithmetic intersection of two natural families of cycles of *different type* in a Hilbert modular surface over $\mathbb{Z}$, arithmetic Hirzebruch-Zagier divisors and arithmetic CM cycles associated to non-biquadratic quartic CM fields. They intersect properly and have a conjectured arithmetic intersection formula [BY]. The main purpose of this paper is to prove the conjectured formula under a minor technical condition on the CM number field. As an application, we prove the first *non-abelian* Chowla-Selberg formula [Co], which is also a special case of Colmez's conjecture on the Faltings height of CM abelian varieties. As another application, we obtain an explicit intersection formula between (arithmetic) Humbert surfaces and CM cycles in the (arithmetic) Siegel modular 3-fold, which has itself two applications: confirming Lauter's conjecture on the denominators of Igusa invariants valued at CM points [La], [Ya5], and bad reduction of CM genus two curves. We also use the formula to verify a variant of a conjecture of Kudla on arithmetic Siegel-Weil formula. We now set up notation and describe this work in a little more detail.

Let $D \equiv 1 \mod 4$ be a prime number, and let $F = \mathbb{Q}(\sqrt{D})$ with the ring of integers $\mathcal{O}_F = \mathbb{Z}[\frac{D+\sqrt{D}}{2}]$ and different $\partial_F = \sqrt{D}\mathcal{O}_F$. Let $\mathcal{M}$ be the Hilbert moduli

[*] Received July 8, 2010; accepted for publication April 3, 2012.

[†] Department of Mathematics, University of Wisconsin Madison, Van Vleck Hall, Madison, WI 53706, USA (thyang@math.wisc.edu). Partially supported by grants DMS-0302043, DMS-0354353, DMS-0555503, NSFC-10628103, and Vilas Life Cycle Professorship (Univ. Wisconsin).

stack of assigning to a base scheme $S$ over $\mathbb{Z}$ the set of the triples $(A, \iota, \lambda)$, where ([Go, Chapter 3] and [Vo, Section 3])

(1) $A$ is a abelian surface over $S$.

(2) $\iota : \mathcal{O}_F \hookrightarrow \mathrm{End}_S(A)$ is real multiplication of $\mathcal{O}_F$ on $A$.

(3) $\lambda : \partial_F^{-1} \to P(A) = \mathrm{Hom}_{\mathcal{O}_F}(A, A^\vee)^{\mathrm{sym}}$ is a $\partial_F^{-1}$-polarization (in the sense of Deligne-Papas) satisfying the condition:

$$\partial_F^{-1} \otimes A \to A^\vee, \quad r \otimes a \mapsto \lambda(r)(a)$$

is an isomorphism.

Next, for an integer $m \geq 1$, let $\mathcal{T}_m$ be the integral Hirzebruch-Zagier divisor in $\mathcal{M}$ defined in [BBK, Section 5], which is the flat closure of the classical Hirzebruch-Zagier divisor $T_m$ in $\mathcal{M}$. We refer to Section 3 for the modular interpretation of $\mathcal{T}_m$ when $m$ is a prime split in $F$.

Finally, let $K = F(\sqrt{\Delta})$ be a quartic non-biquadratic CM number field with real quadratic subfield $F$. Let $\mathcal{CM}(K)$ be the moduli stack over $\mathbb{Z}$ representing the moduli problem which assigns to a base scheme $S$ the set of the triples $(A, \iota, \lambda)$ where $\iota : \mathcal{O}_K \hookrightarrow \mathrm{End}_S(A)$ is an CM action of $\mathcal{O}_K$ on $A$, and $(A, \iota|_{\mathcal{O}_F}, \lambda) \in \mathcal{M}(S)$ such that the Rosati involution associated to $\lambda$ induces the complex conjugation on $\mathcal{O}_K$. The map $(A, \iota, \lambda) \mapsto (A, \iota|_{\mathcal{O}_F}, \lambda)$ is a finite proper map from $\mathcal{CM}(K)$ into $\mathcal{M}$, and we denote its direct image in $\mathcal{M}$ still by $\mathcal{CM}(K)$ by abuse of notation. Since $K$ is non-biquadratic, $\mathcal{T}_m$ and $\mathcal{CM}(K)$ intersect properly. A basic question is to compute their arithmetic intersection number (see Section 3 for definition). Let $\Phi$ be a CM type of $K$ and let $\tilde{K}$ be the reflex field of $(K, \Phi)$. It is also a quartic non-biquadratic CM field with real quadratic field $\tilde{F} = \mathbb{Q}(\sqrt{\mathrm{N}_{F/\mathbb{Q}}(d_{K/F})})$ where $d_{K/F}$ is the relative discriminant of $K/F$.

Conjecture 1.1. *(Bruinier and Yang) Let the notation be as above and let $\tilde{D} = d_{\tilde{F}}$ be the discriminant of $\tilde{F}$. Then*

$$\mathcal{T}_m.\mathcal{CM}(K) = \frac{1}{2} b_m \tag{1.1}$$

*or equivalently*

$$(\mathcal{T}_m.\mathcal{CM}(K))_p = \frac{1}{2} b_m(p) \tag{1.2}$$

*for every prime $p$. Here*

$$b_m = \sum_p b_m(p) \log p$$

*is defined as follows:*

$$b_m(p) \log p = \sum_{\mathfrak{p}|p} \sum_{\substack{t = \frac{n + m\sqrt{\tilde{D}}}{2D} \in d_{\tilde{K}/\tilde{F}}^{-1} \\ |n| < m\sqrt{\tilde{D}}}} B_t(\mathfrak{p}) \tag{1.3}$$

*where*

$$B_t(\mathfrak{p}) = \begin{cases} 0 & \textit{if } \mathfrak{p} \textit{ is split in } \tilde{K}, \\ (\mathrm{ord}_{\mathfrak{p}} t + 1)\rho(t d_{\tilde{K}/\tilde{F}} \mathfrak{p}^{-1}) \log |\mathfrak{p}| & \textit{if } \mathfrak{p} \textit{ is not split in } \tilde{K}, \end{cases} \tag{1.4}$$

$|\mathfrak{p}|$ *is the norm of the ideal* $\mathfrak{p}$ *of* $\tilde{F}$*, and*

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

Notice that the conjecture implies that $(\mathcal{T}_m.\mathcal{CM}(K))_p = 0$ unless $4Dp \mid m^2\tilde{D} - n^2$ for some integer $0 \le n < m\sqrt{\tilde{D}}$. In particular, $\mathcal{T}_m.\mathcal{CM}(K) = 0$ if $m^2\tilde{D} \le 4D$.

Throughout this paper, we assume that $K$ satisfies the following condition

$$\mathcal{O}_K = \mathcal{O}_F + \mathcal{O}_F \frac{w + \sqrt{\Delta}}{2} \tag{1.5}$$

is free over $\mathcal{O}_F (w \in \mathcal{O}_F)$ and that $\Delta\Delta'$ is odd, where $\Delta'$ is the Galois conjugate of $\Delta$ in $F$. In such a case, one can show that $\tilde{D} = \Delta\Delta'$ is square-free and $d_K = D^2\tilde{D}$. The main result of this paper is the following theorem.

Theorem 1.2. *Assume* (1.5) *and that* $\tilde{D} \equiv 1 \mod 4$ *is a prime. Then Conjecture 1.1 holds.*

The special case $m = 1$ is proved in [Ya4]. Now we describe its application to the generalized Chowla-Selberg formula. In proving the famous Mordell conjecture, Faltings introduces the so-called Faltings height $h_{\mathrm{Fal}}(A)$ of an Abelian variety $A$, measuring the complexity of $A$ as a point in a Siegel modular variety. When $A$ has complex multiplication, it only depends on the CM type of $A$ and has a simple description as follows. Assume that $A$ is defined over a number field $L$ with good reduction everywhere, and let $\omega_A \in \Lambda^g\Omega_A$ be a Néron differential of $A$ over $\mathcal{O}_L$, non-vanishing everywhere. Then the Faltings height of $A$ is defined as (our normalization is slightly different from that of [Co])

(1.6)

$$h_{\mathrm{Fal}}(A) = -\frac{1}{2[L:\mathbb{Q}]} \sum_{\sigma: L \hookrightarrow \mathbb{C}} \log \left| (\frac{1}{2\pi i})^g \int_{\sigma(A)(\mathbb{C})} \sigma(\omega_A) \wedge \overline{\sigma(\omega_A)} \right| + \log \#\Lambda^g\Omega_A/\mathcal{O}_L\omega_A.$$

Here $g = \dim A$. Colmez gives a beautiful conjectural formula to compute the Faltings height of a CM abelian variety in terms of the log derivative of certain Artin L-series associated to the CM type [Co], which is a consequence of his product formula conjecture of $p$-adic periods in the same paper. When $A$ is a CM elliptic curve, the height conjecture is a reformulation of the well-known Chowla-Selberg formula relating the CM values of the usual Delta function $\Delta$ with the values of the Gamma function at rational numbers. Colmez proved his conjecture up to a multiple of $\log 2$ when the CM field (which acts on $A$) is abelian, refining Gross's [Gr] and Anderson's [An] work. A key point is that such CM abelian varieties are isogenous to quotients of the Jacobians of the Fermat curves, so one has explicit models to work with. Köhler and Roessler gave a different proof of a weaker version of Colmez's result using their Lefschetz fixed point theorem in Arakelov geometry [KRo] without using explicit model of CM abelian varieties. They still relied on the action of $\mu_n$ on product of copies of these CM abelian varieties, and did not thus break the barrier of non-abelian CM number fields. V. Maillot and Roessler gave a more general conjecture relating logarithmtic derivatives of (virtual) Artin L-function with motives and provided some evidence in [MR] (weaker than the Colmez conjecture when restricting to CM abelian varieties) and Yoshida independently developed a conjecture about absolute CM periods which is very close to Colmez's conjecture and provided some non-trivial numerical evidence as well as partial results [Yo]. We should also mention that Kontsevich and Zagier [KZ] put these conjectures in different perspective in the framework of periods, and for example rephrased the Colmez conjecture (weaker form) as saying the log derivative of Artin L-functions is a period.

When the CM number field is *non-abelian*, nothing is known about Colmez's conjecture. In this paper we consider the case that $K$ is a non-biquadratic quartic CM number field (with real quadratic subfield $F$), in which case Colmez's conjecture can be stated precisely as follows. Let $\chi$ be the quadratic Hecke character of $F$ associated to $K/F$ by global class field theory, and let

$$\Lambda(s,\chi) = C(\chi)^{\frac{s}{2}}\pi^{-s-1}\Gamma(\frac{s+1}{2})^2 L(s,\chi) \tag{1.7}$$

be the complete L-function of $\chi$ with $C(\chi) = DN_{F/\mathbb{Q}}d_{K/F}$. Let

$$\beta(K/F) = \frac{\Gamma'(1)}{\Gamma(1)} - \frac{\Lambda'(0,\chi)}{\Lambda(0,\chi)} - \log 4\pi. \tag{1.8}$$

In this case, the conjectured formula of Colmez on the Faltings height of a CM abelian variety $A$ of type $(K,\Phi)$ does not even depend on the CM type $\Phi$ and is given by (see [Ya3])

$$h_{\mathrm{Fal}}(A) = \frac{1}{2}\beta(K/F). \tag{1.9}$$

In Section 8, we will prove the following result using Theorem 1.2, and [BY, Theorem 1.4], which breaks the barrier of 'non-abelian' CM number fields. Our proof is totally different.

Theorem 1.3. *Assume that $K$ satisfies the conditions in 1.2. Then Colmez's conjecture (1.9) holds.*

Kudla initiated a program to relate the arithmetic intersections on Shimura varieties over $\mathbb{Z}$ with the derivatives of Eisenstein series—*arithmetic Siegel-Weil Formula* in 1990's, see [Ku1], [Ku3], [KRY2] and references there for example. Roughly speaking, let

$$\hat{\phi}(\tau) = -\frac{1}{2}\hat{\omega} + \sum_{m>0} \hat{\mathcal{T}}_m q^m \tag{1.10}$$

be the modular form of weight 2, level $D$, and character $(\frac{D}{})$ with values in the arithmetic Chow group defined by Bruinier, Burgos Gil, and Kühn [BBK] (see also Section 8), where $\hat{\omega}$ is the metrized Hodge bundle on $\tilde{M}$ with Peterson metric defined in Section 8 and can be viewed as an arithmetic Chow cycle, and $\hat{\mathcal{T}}_m$ is some arithmetic Chow cycle related to $\mathcal{T}_m$. Then we have the following result, which can be viewed as a variant of Kudla's conjecture in this case. We refer to Theorem 8.2 for a more precise statement of the result.

Theorem 1.4. *Let the notation and assumption be as in Theorem 1.2. Then $h_{\hat{\phi}}(\mathcal{CM}(K)) + \frac{1}{4}\Lambda(0,\chi)\beta(K/F)E_2^+(\tau)$ is the holomorphic projection of the diagonal restriction of the central derivative of some (incoherent) Hilbert Eisenstein series on $\tilde{F}$. Here $E_2^+(\tau)$ is an Eisenstein series of weight 2.*

Let $\mathcal{A}_2$ be the moduli stack of principally polarized abelian surfaces [CF]. $\mathcal{A}_2(\mathbb{C}) = \mathrm{Sp}_2(\mathbb{Z})\backslash\mathbb{H}_2$ is the Siegel modular variety of genus 2. For each integer $m$, let

$G_m$ be the Humbert surface in $\mathcal{A}_2(\mathbb{C})$ ([Ge, Chapter 9], see also Section 9), which is actually defined over $\mathbb{Q}$. Let $\mathcal{G}_m$ be the flat closure of $G_m$ in $\mathcal{A}_2$. For a quartic CM number field $K$, let $\mathcal{CM}_S(K)$ be the moduli stack of principally polarized CM abelian surfaces by $\mathcal{O}_K$. We use subscript $S$ to indicate that it is a CM cycle $\mathcal{A}_2$. The stack $\mathcal{CM}_S(K)$ is isomorphic to $\mathcal{CM}(K)$ by (9.4). In Section 9, we will prove the following theorem using Theorem 1.2 and a natural map from $\mathcal{M}$ to $\mathcal{A}_2$.

Theorem 1.5. *Assume $K$ satisfies the condition in Theorem 1.2, and that $Dm$ is not a square. Then $\mathcal{CM}_S(K)$ and $\mathcal{G}_m$ intersect properly, and*

$$\mathcal{CM}_S(K).\mathcal{G}_m = \frac{1}{2} \sum_{n>0,\, \frac{Dm-n^2}{4} \in \mathbb{Z}_{>0}} b_{\frac{Dm-n^2}{4}}. \tag{1.11}$$

Since $\mathcal{G}_1$ is the moduli space of principally polarized abelian surfaces which are not Jacobians of genus two curves, the above theorem, together with lifting theorem of principally polarized CM abelian varieties by maximal order of a CM number field (see for example, [Ho] or proof of [GL, Theorem 4.2.1]), has the following consequence. The corollary also solves Goren and Lauter's embedding problem in [GL, Section 3]. Our approach is different in two senses. First we work on Hilbert modular surfaces instead of Siegel modular 3-folds and reduce the 'difficulty' by 'one dimension'. Second, we count instead of proving existence.

Corollary 1.6. *Let $K$ be a quartic CM number field as in Theorem 1.2. Let $C$ be a genus two curve over a number field $L$ such that its Jacobian $J(C)$ has CM by $\mathcal{O}_K$ and has good reduction everywhere. Let $l$ be a prime. If $C$ has bad reduction at a prime $\mathfrak{l}|l$ of $L$, then*

$$\sum_{0<n<\sqrt{D}, odd} b_{\frac{D-n^2}{4}}(l) \neq 0 \tag{1.12}$$

*In particular, $l \leq \frac{D\tilde{D}}{64}$. Conversely, if (1.12) holds for a prime $l$, then there is a genus two curve $C$ over some number field $L$ such that*

*(1) $J(C)$ has CM by $\mathcal{O}_K$ and has good reduction everywhere, and*

*(2) $C$ has bad reduction at a prime $\mathfrak{l}$ above $l$.*

Finally we recall that Igusa defines 10 invariants which characterize genus two curves over $\mathbb{Z}$ in [Ig2]. They are Siegel modular forms of genus 2 (level 1) [Ig1]. One needs three of them, commonly called $j_1$, $j_2$, and $j_3$, which determine genus two curves over $\bar{\mathbb{Q}}$ and over $\bar{\mathbb{F}}_p$ when $p > 5$ and $j_1 \neq 0$. Recently, Cohn and Lauter ([CL]), and Weng [Wen] among others started to use genus two curves over finite fields for cryptosystems. For this purpose, they need to compute the CM values of the Igusa invariants associated to a quartic non-biquadratic CM field. Similar to the classical $j$-invariant, these CM values are algebraic numbers. However, they are in general not algebraic integers. It is very desirable to at least bound the denominators of these numbers for this purpose and also in theory. Lauter gives an inspiring conjecture about the denominator in [La] based on her calculation and Gross and Zagier's work on singular moduli [GZ1]. In Section 9, we will prove the following refinement of her conjecture subject to the condition in Theorem 1.2.

Theorem 1.7. *(Lauter's conjecture). Let $j_i'$, $i = 1, 2, 3$ be the slightly renormalized Igusa invariants in Section 9, and let $\tau$ be a CM point in $X_2$ such that the* *associated abelian surface $A_\tau$ has endomorphism ring $\mathcal{O}_K$, and let $H_i(x)$ be the minimal polynomial of $j_i'(\tau)$ over $\mathbb{Q}$. Assume $K$ satisfies the condition in Theorem 1.2. Let $A_i$ be positive integers given by*

$$A_i = \begin{cases} e^{3W_K \sum_{0<n<\sqrt{D}, odd} b_{\frac{D-n^2}{4}}} & \text{if } i = 1, \\ e^{2W_K \sum_{0<n<\sqrt{D}, odd} b_{\frac{D-n^2}{4}}} & \text{if } i = 2, 3. \end{cases}$$

*Here $W_K$ is the number of roots of unity in $K$. Then $A_i H_i(x)$ is defined over $\mathbb{Z}$. In particular, $A_i \operatorname{N}(j_i'(\tau))$ is a rational integer.*

Now we describe briefly how to prove Theorem 1.2 and its consequences. The major effort is to prove the following weaker version of the main theorem, which covers Sections 3-7.

Theorem 1.8. *Assume (1.5) and that $\tilde{D} \equiv 1 \mod 4$ is square free, and that $m = q$ is an odd prime split in $F$. Then*

$$\mathcal{T}_q.\mathcal{CM}(K) = \frac{1}{2} b_q + c_q \log q \tag{1.13}$$

*for some rational number $c_q$. Equivalently, one has for any prime $p \neq q$,*

$$(\mathcal{T}_q.\mathcal{CM}(K))_p = \frac{1}{2} b_q(p). \tag{1.14}$$

The starting point is a proper map from the moduli stack $\mathcal{Y}_0(q)$ of cyclic isogeny $(\phi : E \to E')$ of degree $q$ of elliptic curves to $\mathcal{T}_q$ constructed by Bruinier, Burgos-Gil, and Kühn in [BBK], see also Section 3. Let $(B, \iota, \lambda)$ be the image of $(\phi : E \to E')$ in $\mathcal{T}_q$, we first compute the endomorphism ring of $(B, \iota)$ in terms of a pair of quasi-endomorphisms $\alpha, \beta \in \phi^{-1} \operatorname{Hom}(E, E')$ satisfying some local condition at $q$. This is quite different from the special case $q = 1$ considered in [Ya4]: we can not describe the endomorphism ring of $(E, \iota)$ globally. The upshot is the following: associated to a geometric intersection point in $\mathcal{T}_q.\mathcal{CM}(K)(\bar{\mathbb{F}}_p)$ is a triple $(\phi, \phi\alpha, \phi\beta : E \to E')$ satisfying certain *local* condition at $q$. Using a beautiful formula of Gross and Keating [GK] on deformation of isogenies, we are able to compute the local intersection index and prove the following theorem.

Theorem 1.9. *(Theorem 3.6) For $p \neq q$, one has*

$$(\mathcal{T}_q.\mathcal{CM}(K))_p = \frac{1}{4} \sum_{\substack{0<n<q\sqrt{\tilde{D}} \\ \frac{q^2\tilde{D}-n^2}{4D} \in p\mathbb{Z}_{>0}}} \left( \operatorname{ord}_p \frac{q^2\tilde{D}-n^2}{4D} + 1 \right) \sum_{\mu} \sum_{[\phi: E \to E']} \frac{R(\phi, T_q(\mu n))}{\# Aut(\phi)}.$$

*Here $\mu = \pm 1$, $T_q(\mu n)$ is a positive definite $2 \times 2$ matrix with entries in $\frac{1}{q}\mathbb{Z}$ determined by $n$ and $\mu$ as in Lemma 4.1. $R(\phi, T_q(\mu n))$ is the number of pairs $(\delta, \beta) \in (\phi^{-1} \operatorname{Hom}(E, E'))^2$ satisfying certain local conditions at $q$ and $2$ such that*

$$T(\delta, \beta) := \frac{1}{2} \begin{pmatrix} (\delta,\delta) & (\delta,\beta) \\ (\delta,\beta) & (\beta,\beta) \end{pmatrix} = T_q(\mu n).$$

*Finally, $Aut(\phi)$ is the set of automorphisms $f \in Aut(E)$ such that $\phi \circ f \circ \phi^{-1} \in Aut(E')$, and the summation is over the equivalence classes of all isogenies $[\phi : E \to E']$ of degree $q$ of supersingular elliptic curves over $\bar{\mathbb{F}}_p$.*

The next step is to compute the summation

$$\beta(p, \mu n) = \sum_{[\phi: E \to E']} \frac{R(\phi, T_q(\mu n))}{\#\mathrm{Aut}(\phi)}$$

which counts the 'number' of geometric intersection points between $\mathcal{CM}(K)$ and $\mathcal{T}_q$ at $p$. The sum can be written as a product of local Whittaker integrals and can be viewed as a generalization of quadratic local density. In theory, the idea in [Ya1], [Ya2] can be generalized to compute these local integrals, but it is very complicated. In Section 5, we take advantage of the relation between supersingular elliptic curves and maximal orders of the quaternion algebra $\mathbb{B}$ which ramifies only at $p$ and $\infty$, and known structure of quaternions, and transfer the summation into product of local integral over $\mathbb{B}_l^*$ instead of usual local density integral as in [Ya1], [Ya2]:

$$\beta(p, \mu n) = \frac{1}{2} \int_{\mathbb{Q}_f^* \backslash \mathbb{B}_f^* / \mathcal{K}} \Psi(g^{-1}.\vec{x}_0) dg \tag{1.15}$$

if there is $\vec{x}_0 = V(\mathbb{A}_f)^2$ with $T(\vec{x}_0) = T_q(\mu n)$. Otherwise, $\beta(p, \mu n) = 0$. Here

$$g.\vec{x} = (g.X_1, g.X_2) = (gX_1g^{-1}, gX_2g^{-1}), \quad \vec{x} = {}^t(X_1, X_2),$$

and $\Psi = \prod \Psi_l \in S(V(\mathbb{A}_f))^2$ and $V$ is the quadratic space of trace zero elements in $\mathbb{B}$. In Section 6, we compute these local integrals which is quite technical at $q$ due to the local condition mentioned above, and obtain an explicit formula for $\beta(p, \mu n)$ (Theorems 6.1 and 6.2). In Section 7, we compute $b_m(p)$ and proves Theorem 1.8. The computation also gives a more explicit formula for the intersection number.

In Section 8, we use the height pairing function and [BY, Theorem 1.4] to derive the main theorem from the weaker version. we also derive Theorem 1.3 from Theorem 1.2 using the same idea. Theorem 1.4 is a consequence of the main theorem and [BY, Theorem 8.1]. In Section 9, we briefly review the natural modular 'embedding' from Hilbert modular surfaces to the Siegel modular 3-fold, and prove Theorems 1.5, 1.6, and 1.7.

**Acknowledgments.** I received a lot of help for this project from a lot of people, which I appreciate very much. In particular, I would like to thank J. Bruinier, K. Lauter, S. Kudla, U. Kühn, M. Olsson, M. Rapoport, K. Ribet, M. Streng, and S. W. Zhang for their help and inspiring discussion. Part of this work was done when I visited MPIM at Bonn Germany (2006), MSRI (2007), AMASS and Morningside Center of Mathematics at Beijing, China (2007). I thank these institutes for providing wonderful working environment and financial support. Finally, I thank the referees for their careful reading of the paper and suggestion, which improves the exposition of the paper.

## 2. A brief review of the case $q = 1$.

For the convenience of the reader, we briefly review the computation of the arithmetic intersection between $\mathcal{CM}(K)$ and $\mathcal{T}_q$ in the very special case $q = 1$ to give a rough idea and motivation to the general case considered in this paper. We also briefly describe how Gross and Zagier's beautiful factorization formula for singular moduli can be derived this way. We refer to [Ya4] for detail, and to Section 3 for notation.

Let $\mathcal{E}$ be the moduli stack over $\mathbb{Z}$ of elliptic curves. Then there is a natural isomorphism between $\mathcal{E}$ and $\mathcal{T}_1$ given by $E \mapsto (E \otimes \mathcal{O}_F, \iota, \lambda)$. A simple but critical fact is that $\mathrm{End}_{\mathcal{O}_F}(E \otimes \mathcal{O}_F) \cong \mathrm{End}(E) \otimes \mathcal{O}_F$ is easy to understand (it is much more complicated even in the split prime $q$ case considered in Section 3). So a geometric intersection point in $\mathcal{T}_1.\mathcal{CM}(K)(\bar{\mathbb{F}}_p)$ is determined by a pair $(E, \iota)$ where

$$\iota : \mathcal{O}_K \hookrightarrow \mathrm{End}(E) \otimes \mathcal{O}_F$$

such that the main involution on $\mathbb{O}_E = \mathrm{End}(E)$ gives the complex conjugation on $\mathcal{O}_K$, which implies in particular that $E$ is supersingular and $p$ is inert in $F$. Since we assume that $\mathcal{O}_K = \mathcal{O}_F + \mathcal{O}_F \frac{w+\sqrt{\Delta}}{2}$, $\iota$ is determined by

$$\iota(\frac{w+\sqrt{\Delta}}{2}) = \alpha_0 + \beta_0 \frac{D+\sqrt{D}}{2}, \quad \iota(\sqrt{\Delta}) = \delta + \beta \frac{D+\sqrt{D}}{2},$$

with $\alpha_0, \beta_0 \in \mathbb{O}_E$, and

$$\delta = 2\alpha_0 - w_0, \beta = 2\beta_0 - w_1 \in L_E = \{x \in \mathbb{Z} + 2\mathbb{O}_E : \mathrm{tr}\, x = 0\}.$$

Here $w = w_0 + w_1 \frac{D+\sqrt{D}}{2}$ with $w_i \in \mathbb{Z}$. Set for $\delta, \beta \in L_E$

$$T(\delta, \beta) = \frac{1}{2} \begin{pmatrix} (\delta,\delta) & (\delta,\beta) \\ (\delta,\beta) & (\beta,\beta) \end{pmatrix} \in \mathrm{Sym}_2(\mathbb{Z}).$$

One shows that $T(\delta, \beta)$ is a positive definite integral matrix of the form $T_1(\mu n)$ (in the notation of Lemma 4.1) for a unique positive integer $n$ with $\det T_1(\mu n) = \frac{\tilde{D}-n^2}{D} \in 4p\mathbb{Z}_{>0}$ and a unique sign $\mu = \pm 1$.

Applying a beautiful deformation result of Gross and Keating to 1, $\alpha_0$, and $\beta_0$, we show in [Ya4, Section 4] that the local intersection index of $\mathcal{T}_1$ and $\mathcal{CM}(K)$ at $(E, \iota)$ is given by

$$\iota_p(E, \iota) = \frac{1}{2}(\mathrm{ord}_p \frac{\tilde{D}-n^2}{4D} + 1)$$

which depends only on $n$. So the intersection number of $\mathcal{T}_1$ and $\mathcal{CM}(K)$ at $p$ is

$$(\mathcal{T}_1.\mathcal{CM}(K))_p = \frac{1}{2} \sum_{\frac{\tilde{D}-n^2}{4D} \in p\mathbb{Z}_{>0}} (\mathrm{ord}_p \frac{\tilde{D}-n^2}{4D} + 1) \sum_{\mu} \sum_{E s.s.} \frac{R(L_E, T_1(\mu n))}{\#\mathrm{Aut}(E)}$$

where the sum is running over all supersingular elliptic curves over $\bar{\mathbb{F}}_p$ (up to isomorphism), and $R(L_E, T_1(\mu n))$ is the representation number of the ternary quadratic form $L_E$ representing the matrix $T_1(\mu n)$.

Finally the last sum can be proved to be the product of local densities, and can be computed using the formulae in [Ya1] and [Ya2]. However, the case $p = 2$ is extremely complicated. In [Ya4], we used a trick together with a beautiful result in [GK] to deal with this delicate issue. However, this trick only works in this special case. In this paper, we use a new idea to deal with the case $q \neq 1$ in Sections 5 and 6. The upshot is then the following formula:

$$(\mathcal{T}_1.\mathcal{CM}(K))_p = \frac{1}{2} \sum_{\frac{\tilde{D}-n^2}{4D} \in p\mathbb{Z}_{>0}} (\mathrm{ord}_p \frac{\tilde{D}-n^2}{4D} + 1) \sum_{\mu} \beta(p, \nu n)$$

where

$$\beta(p, \mu n) = \prod_{l \mid \frac{\tilde{D}-n^2}{4D}} \beta_l(p, \mu n)$$

and $\beta_l(p, \mu n)$ is given by the right hand side of the formula in Theorem 6.1. This finishes the computation at the geometric side. On the algebraic side, the computation of $b_1(p)$ is similar to that of $b_m(p)$ in Section 7(of course simpler) and shows that $b_1(p)$ is equal to the right hand side of the above formula without the factor $\frac{1}{2}$. That proves the case $q = 1$.

If we further allow $D = 1$, i.e., $F = \mathbb{Q} \oplus Q$, and $K = \mathbb{Q}(\sqrt{d_1}) \oplus \mathbb{Q}(\sqrt{d_2})$, one has $\mathcal{M} = \mathcal{E} \times \mathcal{E}$ and $\mathcal{CM}(K) = \mathcal{CM}(d_1) \times \mathcal{CM}(d_2)$ where $\mathcal{CM}(d_i)$ is the moduli stack of CM elliptic curves of (fundamental) discriminant $d_i < 0$. Furthermore, $\mathcal{T}_1$ is just the diagonal embedding of $\mathcal{E}$. From this, it is easy to see

$$\begin{aligned} \mathcal{T}_1.\mathcal{CM}(K) &= \mathcal{CM}(K_1).\mathcal{CM}(K_2) \quad \text{in} \quad \mathcal{M}_1 \\ &= \sum_{\mathrm{disc}[\tau_i]=d_i} \frac{4}{w_1 w_2} \log |j(\tau_1) - j(\tau_2)| \end{aligned} \tag{2.1}$$

where $w_i$ is number of roots of unity of imaginary quadratic field of discriminant $d_i$, and $\tau_i$ are Heegner points in $\mathcal{M}_1(\mathbb{C})$ of discriminant $d_i$. Now the beautiful factorization of Gross-Zagier on singular moduli follows from the arithmetic intersection formula for $\mathcal{T}_1.\mathcal{CM}(K)$. We refer to [Ya4, Section 3] for detail.

**3. Modular Interpretation of $\mathcal{T}_q$ and Endomorphisms of Abelian varieties.** Let $F = \mathbb{Q}(\sqrt{D})$ with $D \equiv 1 \mod 4$ prime. Let $\mathcal{M}$ be the Hilbert modular stack defined in the introduction, and let $\tilde{\mathcal{M}}$ be a fixed Toroidal compactification. Let $K = F(\sqrt{\Delta})$ be a non-biquadratic quartic CM number field with real quadratic subfield $F$, and let $\mathcal{CM}(K)$ be the CM cycle defined in the introduction. Notice that $\mathcal{CM}(K)$ is closed in $\tilde{\mathcal{M}}$. $K$ has four different CM types $\Phi_1$, $\Phi_2$, $\rho\Phi_1 = \{\rho\sigma : \sigma \in \Phi_1\}$, and $\rho\Phi_2$, where $\rho$ is the complex conjugation in $\mathbb{C}$. If $x = (A, \iota, \lambda) \in \mathcal{CM}(K)(\mathbb{C})$, then $(A, \iota, \lambda)$ is a CM abelian surface over $\mathbb{C}$ of exactly one CM type $\Phi_i$ in $\mathcal{M}(\mathbb{C}) = \mathrm{SL}_2(\mathcal{O}_F)\backslash\mathbb{H}^2$ as defined in [BY, Section 3]. Let $\mathrm{CM}(K, \Phi_i)$ be set of (isomorphism classes) of CM abelian surfaces of CM type $(K, \Phi_i)$ as in [BY], viewed as a cycle in $\mathcal{M}(\mathbb{C})$. Then it was proved in [BY]

$$\mathrm{CM}(K) = \mathrm{CM}(K, \Phi_1) + \mathrm{CM}(K, \Phi_2) = \mathrm{CM}(K, \rho\Phi_1) + \mathrm{CM}(K, \rho\Phi_2)$$

is defined over $\mathbb{Q}$. So we have

Lemma 3.1. *One has*

$$\mathcal{CM}(K)(\mathbb{C}) = 2\,\mathrm{CM}(K)$$

*in* $\mathcal{M}(\mathbb{C})$.

Next for an integer $m > 0$, let $T_m$ be the Hirzebruch-Zagier divisor $T_m$ is given by [HZ]

$$T_m(\mathbb{C}) = \mathrm{SL}_2(\mathcal{O}_F)\backslash\{(z_1, z_2) \in \mathbb{H}^2 : (z_2, 1)A\left(\begin{smallmatrix} z_1 \\ 1 \end{smallmatrix}\right) = 0 \text{ for some } A \in L_m\},$$

where

$$L_m = \{A = \left(\begin{smallmatrix} a & \lambda \\ \lambda' & b \end{smallmatrix}\right) : a, b \in \mathbb{Z}, \lambda \in \partial_F^{-1}, ab - \lambda\lambda' = \frac{m}{D}\}.$$

$T_m$ is empty if $(\frac{D}{m}) = -1$. Otherwise, it is a finite union of irreducible curves and is actually defined over $\mathbb{Q}$. Following [BBK], let $\mathcal{T}_m$ be the flat closure of $T_m$ in $\mathcal{M}$, and let $\tilde{\mathcal{T}}_m$ be the closure of $\mathcal{T}_m$ in $\tilde{\mathcal{M}}$. When $m = q$ is a prime split in $F$, $\mathcal{T}_m$ has the following modular interpretation, which is different from that given in in [KR1]. We identify it with modular curves in this special case while Kudla and Rapoport define it for all $m$. For the rest of this section, we assume $m = q$ is a prime split in $F$.

Let $q$ be a prime number split in $F$, and let $\mathfrak{q}$ be a fixed prime of $F$ over $q$. In this paper, we will fix an identification $F \hookrightarrow F_{\mathfrak{q}} \cong \mathbb{Q}_q$, and let $\sqrt{D} \in \mathbb{Q}_q$ be the image of $\sqrt{D} \in F$ under the identification. Following [BBK], we write $\mathfrak{q} = r\mathfrak{c}^2$ with some $r \in F^*$ of norm being a power of $q$ and some fractional ideal $\mathfrak{c}$ of $F$. For a cyclic isogeny $\phi : E \to E'$ of elliptic curves of degree $q$ over a scheme $S$ over $\mathbb{Z}[\frac{1}{q}]$, Bruinier, Burgos, and Kühn constructed a triple $(B, \iota, \lambda)$ as follows. First let $A = E \otimes \mathfrak{c}$, and $B = A/H$ with $H = (\ker \phi \otimes \mathfrak{c}) \cap A[\mathfrak{q}]$. We have the following commutative diagram:

$$\begin{tikzcd}
A = E \otimes \mathfrak{c} \arrow[rr, "\pi_{\mathfrak{q}}"] \arrow[dr, "\pi"] \arrow[dd, "\phi\otimes 1"'] & & A/A[\mathfrak{q}] \\
& B = A/H \arrow[ur, "\pi_2"] \arrow[dl, "\pi_1"] & \\
A' = E' \otimes \mathfrak{c} & &
\end{tikzcd} \tag{3.1}$$

The natural action of $\mathcal{O}_F$ on $A$ induces an action $\iota : \mathcal{O}_F \hookrightarrow \mathrm{End}(B)$. It is clear

$$P(A) = \mathrm{Hom}_{\mathcal{O}_F}(A, A^\vee)^{\mathrm{Sym}} = \mathfrak{c}^{-2}\partial_F^{-1} \tag{3.2}$$

naturally. They proved that under the natural injection

$$P(B) \hookrightarrow P(A), \quad g \mapsto \pi^\vee g \pi$$

the image of $P(B)$ is $\partial_F^{-1}$. This gives the Deligne-Pappas $\partial^{-1}$-polarization map

$$\lambda : \partial_F^{-1} \to P(B)$$

satisfying the Deligne-Papas condition. Furthermore, they proved [BBK, Proposition 5.12] that

$$\Phi : (\phi : E \to E') \mapsto (B, \iota, \lambda) \tag{3.3}$$

is a proper map from the moduli stack $\mathcal{Y}_0(q)$ over $\mathbb{Z}[\frac{1}{q}]$ to $\mathcal{M}$, and $\mathcal{T}_q = \Phi_*\mathcal{Y}_0(q)$. The map $\Phi$ is generically an isomorphism. This proper map extends to a proper map from $\mathcal{X}_0(q)$ to $\tilde{\mathcal{M}}$, whose direct image is the closure $\tilde{\mathcal{T}}_q$ of $\mathcal{T}_q$ in $\tilde{\mathcal{M}}$.

Recall [Gi], [Ho, Section 1], [KRY2, Chapter 2], [Vi], and [Ya4, Section 2] that two cycles $\mathcal{Z}_i$ in a DM-stack $\mathcal{X}$ of codimension $p_i$, $p_1 + p_2 = \dim \mathcal{X}$, intersect properly if $\mathcal{Z}_1 \cap \mathcal{Z}_1 = \mathcal{Z}_1 \times_{\mathcal{X}} \mathcal{Z}_2$ is a DM-stack of dimension 0. In such a case, we define their (arithmetic) intersection number as

$$\begin{aligned} \mathcal{Z}_1.\mathcal{Z}_2 &= \sum_p \sum_{x \in \mathcal{Z}_1 \cap \mathcal{Z}_2(\bar{\mathbb{F}}_p)} \frac{1}{\#\mathrm{Aut}(x)} \log \#\tilde{\mathcal{O}}_{\mathcal{Z}_1 \cap \mathcal{Z}_2, x} \\ &= \sum_p \sum_{x \in \mathcal{Z}_1 \cap \mathcal{Z}_2(\bar{\mathbb{F}}_p)} \frac{1}{\#\mathrm{Aut}(x)} i_p(\mathcal{Z}_1, \mathcal{Z}_2, x) \log p \end{aligned} \tag{3.4}$$

where $\tilde{\mathcal{O}}_{\mathcal{Z}_1\cap\mathcal{Z}_2,x}$ is the strictly local henselian ring of $\mathcal{Z}_1 \cap \mathcal{Z}_2$ at $x$,

$$i_p(\mathcal{Z}_1, \mathcal{Z}_2, x) = \operatorname{Length} \tilde{\mathcal{O}}_{\mathcal{Z}_1\cap\mathcal{Z}_2,x}$$

is the local intersection index of $\mathcal{Z}_1$ and $\mathcal{Z}_2$ at $x$. If $\phi : \mathcal{Z} \to \mathcal{M}$ is a finite proper and flat map from stack $\mathcal{Z}$ to $\mathcal{M}$, we will identify $\mathcal{Z}$ with its direct image $\phi_*\mathcal{Z}$ as a cycle of $\mathcal{M}$, by abuse of notation.

Now come back to our special case. Let $p \neq q$ be a fixed prime. consider the diagram over $\mathbb{Z}_p$

$$\begin{tikzcd} \mathcal{CM}(K) \times_{\mathcal{M}} \mathcal{Y}_0(q) \arrow[r] \arrow[d] & \mathcal{Y}_0(q) \arrow[d] \\ \mathcal{CM}(K) \arrow[r] & \mathcal{M} \end{tikzcd} \tag{3.5}$$

One sees that a geometric point in $\mathcal{CM}(K) \cap \mathcal{T}_q$ is indexed by a pair $x = (\phi : E \to E', \iota)$ with $\phi \in \mathcal{Y}_0(\bar{\mathbb{F}}_p)$ and $\iota : \mathcal{O}_K \hookrightarrow \operatorname{End}_{\mathcal{O}_F}(B)$ is an $\mathcal{O}_K$-action on $B$ such that the Rosati involution associated to $\lambda$ gives the complex conjugation on $K$. Since $K$ is a quartic non-biquadratic CM number field, one sees immediately that such a geometric point does not exist unless $p$ is nonsplit in $F$ and $E$ is supersingular. In such a case, write $I(\phi)$ for all $\mathcal{O}_K$ action $\iota$ satisfying the above condition. Then the intersection number of $\mathcal{CM}(K)$ and $\mathcal{T}_q$ at $p$ is given by

$$(\mathcal{CM}(K).\mathcal{T}_q)_p = \sum_{\phi \in \mathcal{Y}_0(q)(\bar{\mathbb{F}}_p), \iota \in I(\phi)} \frac{1}{\#\operatorname{Aut}(\phi)} i_p(\mathcal{CM}(K), \mathcal{T}_q, (\phi, \iota)) \log p. \tag{3.6}$$

Let $W$ be the Witt ring of $\bar{\mathbb{F}}_p$. Let $\mathbb{E}$ and $\mathbb{E}'$ be the universal deformations of $E$ and $E'$ to $W[[t]]$ and $W[[t']]$ respectively. Let $I$ be the minimal ideal of $W[[t, t']]$ such that

(1) $\phi$ can be lifted to an (unique) isogeny $\phi_I : E_I \to E'_I$, where $E_I = \mathbb{E} \mod I$ and $E'_I = \mathbb{E}' \mod I$.

(2) Let $(B_I, \iota_I, \lambda_I) \in \mathcal{M}(W[[t, t']]/I)$ be associated to $\phi_I$. The embedding $\iota$ can be lifted to an embedding $\iota_I : \mathcal{O}_K \hookrightarrow \operatorname{End}_{\mathcal{O}_F}(B_I)$.

By deformation theory, one can show that the local intersection index is equal to

$$i_p(\phi, \iota) := i_p(\mathcal{CM}(K), \mathcal{T}_q, (\phi, \iota)) = \operatorname{Length} W[[t, t']]/I. \tag{3.7}$$

To compute the local intersection index and to count the geometric intersection points, let $(\phi : E \to E') \in \mathcal{Y}_0(q)$ and let $(B, \iota, \lambda) = \Phi(\phi) \in \mathcal{M}$. Then

$$\operatorname{End}_{\mathcal{O}_F} B = \{g \in \operatorname{End}_S B :\ \iota(r)g = g\iota(r), r \in \mathcal{O}_F\}.$$

We first make the following identification

(3.8)

$$\pi^* : \operatorname{End}^0_{\mathcal{O}_F} B = \operatorname{End}_{\mathcal{O}_F} B \otimes \mathbb{Q} \cong \operatorname{End}^0(A) = \operatorname{End}^0(E) \otimes_{\mathbb{Z}} \mathcal{O}_F, g \mapsto \pi^{-1} \circ g \circ \pi = \frac{1}{q} \pi^\vee g \pi.$$

LEMMA 3.2. *Under the identification (3.8), we have*

$$\operatorname{End}(\phi) \otimes \mathcal{O}_F \subset \pi^* \operatorname{End}_{\mathcal{O}_F}(B) \subset \phi^{-1} \operatorname{Hom}(E, E') \otimes \mathcal{O}_F.$$

*Here*

$$\operatorname{End}(\phi) = \{f \in \operatorname{End}(E) :\ \phi f \phi^{-1} \in \operatorname{End}(E')\}.$$

*Proof.* For $f \in \mathrm{End}(\phi)$, and $x \in H$, let $f' = \phi f \phi^{-1} \in \mathrm{End}(E')$, one has

$$(\phi \otimes 1)((f \otimes 1)(x)) = (f' \otimes 1)(\phi \otimes 1)(x) = 0$$

and so $(f \otimes 1)(x) \in \ker(\phi \otimes 1) = \ker \phi \otimes \mathfrak{c}$. Clearly, $(f \otimes 1)(x) \in A[\mathfrak{q}]$. So $(f \otimes 1)(x) \in H$, and thus $f \otimes 1 = \pi^*(b)$ for some $b \in \mathrm{End}_{\mathcal{O}_F}(B)$.

On the other hand, if $b \in \mathrm{End}_{\mathcal{O}_F}(B)$, then

$$(\phi \otimes 1)\pi^*(b) = \pi_1 b \pi \in \mathrm{Hom}_{\mathcal{O}_F}(A, A') = \mathrm{Hom}(E, E') \otimes \mathcal{O}_F.$$

□

Since $\phi$ is an isomorphism away from $q$, one sees from the lemma

$$\mathrm{End}_{\mathcal{O}_F}(B) \otimes \mathbb{Z}_l \cong (\mathrm{End}(E) \otimes Z_l) \otimes_{\mathbb{Z}} \mathcal{O}_F$$

for all $l \neq q$ via $\pi^*$. We now study

$$\mathcal{O}_{B,q} = \mathrm{End}_{\mathcal{O}_F}(B) \otimes \mathbb{Z}_q = \mathrm{End}_{\mathcal{O}_F \otimes \mathbb{Z}_q} T_q(B), \tag{3.9}$$

where $T_q(B)$ is the Tate module of $B$ at $q$. We identify

$$F \hookrightarrow F_q = F_{\mathfrak{q}} \oplus F_{\mathfrak{q}'} \cong \mathbb{Q}_q \oplus \mathbb{Q}_q, \quad \sqrt{D} \mapsto (\sqrt{D}, -\sqrt{D}) \tag{3.10}$$

as fixed at the beginning of this section. Let $\{e, f\}$ be a *$\phi$-normal basis* of $T_q(E) \subset V_q(E) = T_q(E) \otimes \mathbb{Q}_q$ in the sense

$$T_q(E) = \mathbb{Z}_q e \oplus \mathbb{Z}_q f, \quad T_q(E') = \mathbb{Z}_q \phi(e) \oplus \mathbb{Z} q^{-1} \phi(f). \tag{3.11}$$

To clear up notation, we view both $T_q(E)$ and $T_q(E')$ as submodule of $V_q(E) = T_q(E) \otimes \mathbb{Q}_q$ so that $\phi(e) = e$ and $\phi(f) = f$. Let $\mathfrak{c}_q = \mathfrak{c} \otimes \mathbb{Z}_q = \mathbb{Z}_q(q^r, 0) + \mathbb{Z}_q(0, q^s)$. It is easy to see that

$$\begin{aligned} T_q(A) &= T_q(E) \otimes_{\mathbb{Z}_q} \mathfrak{c}_q, \\ T_q(A/A[\mathfrak{q}]) &= T_q(A) \otimes_{\mathcal{O}_q} \mathfrak{q}_q^{-1} = T_q(E) \otimes_{\mathbb{Z}_q} \mathfrak{c}_q \mathfrak{q}_q^{-1}, \\ T_q(A') &= T_q(E' \otimes \mathfrak{c}) = T_q(E') \otimes_{\mathbb{Z}_q} \mathfrak{c}_q. \end{aligned}$$

and

$$T_q(B) = T_q(A/A[\mathfrak{q}]) \cap T_q(A').$$

Now we use coordinates. Identify

$$\mathcal{O}_q = \mathcal{O}_{\mathfrak{q}} \oplus \mathcal{O}_{\mathfrak{q}'} = \mathbb{Z}_q \oplus \mathbb{Z}_q,$$

Then $\mathfrak{c}_q$ is generated by $(q^r, q^s)$ as an $\mathcal{O}_q$-module, and $\mathfrak{q}_q$ is generated by $(q, 1)$ as an $\mathcal{O}_q$-module. So

$$\begin{aligned} T_q(B) &= \big(\mathfrak{c}_q(q^{-1}, 1)e \oplus \mathfrak{c}_q(q^{-1}, 1)f\big) \cap \big(\mathfrak{c}_q e \oplus (q^{-1}, q^{-1})f\big) \\ &= \mathfrak{c}_q e \oplus \mathfrak{c}_q(q^{-1}, 1)f \\ &= (\mathbb{Z}_q q^r e + \mathbb{Z}_q q^{r-1} f) \oplus (\mathbb{Z}_q q^s e \oplus \mathbb{Z}_q q^s f), \end{aligned}$$

and $(x, y) \in \mathcal{O}_q = \mathbb{Z}_q \oplus \mathbb{Z}_q$ acts on $T_q(B)$ via

$$(x, y)(a_1 q^r e + b_1 q^{r-1} f, a_2 q^s e + b_2 q^s f) = (x a_1 q^r e + x b_1 q^{r-1} f, y a_2 q^s e + y b_2 q^s f).$$

So $\operatorname{End}_{\mathcal{O}_q} T_q(B)$ consists of $(\alpha,\beta) \in (\operatorname{End} V_q(E))^2$ satisfying

$$\alpha(\mathbb{Z}_q q^r e + \mathbb{Z}_q q^{r-1} f) \subset \mathbb{Z}_q q^r e + \mathbb{Z}_q q^{r-1} f, \quad \beta(\mathbb{Z}_q q^s e \oplus \mathbb{Z}_q q^s f) \subset \mathbb{Z}_q q^s e \oplus \mathbb{Z}_q q^s f. \tag{3.12}$$

Here $V_q(E) = T_q(E) \otimes \mathbb{Q}_q = \mathbb{Q}_q e \oplus \mathbb{Q}_q f$. This is the same as $\alpha \in \operatorname{End}(T_q(E'))$ and $\beta \in \operatorname{End}(T_q(E))$. So we have proved that

Proposition 3.3. *Under the identification $\mathcal{O}_q = \mathcal{O}_{\mathfrak{q}} \oplus \mathcal{O}_{\mathfrak{q}'} = \mathbb{Z}_q \oplus \mathbb{Z}_q$, one has*

$$\pi^* \operatorname{End}_{\mathcal{O}_q}(T_q(B)) = \{(\alpha,\beta) \in (\phi^{-1} \operatorname{Hom}(T_q(E), T_q(E')))^2 : \phi\alpha\phi^{-1} \in \operatorname{End} T_q(E'),$$

$$\beta \in \operatorname{End} T_q(E)\}.$$

*Equivalently, with respect to a $\phi$-normal basis $\{e, f\}$, the matrices of $\alpha$ and $\beta$, still denoted by $\alpha$ and $\beta$ respectively, have the properties*

$$\alpha \in \begin{pmatrix} \mathbb{Z}_q & \frac{1}{q}\mathbb{Z}_q \\ q\mathbb{Z}_q & \mathbb{Z}_q \end{pmatrix}, \quad \beta \in M_2(\mathbb{Z}_q), \tag{3.13}$$

*i.e.,*

$$\alpha \begin{pmatrix} e \\ f \end{pmatrix} = \begin{pmatrix} x_1 & \frac{1}{q}y_1 \\ qz_1 & w_1 \end{pmatrix} \begin{pmatrix} e \\ f \end{pmatrix}, \quad \beta \begin{pmatrix} e \\ f \end{pmatrix} = \begin{pmatrix} x_2 & y_2 \\ z_2 & w_2 \end{pmatrix} \begin{pmatrix} e \\ f \end{pmatrix},$$

*with $x_i, y_i, z_i, w_i \in \mathbb{Z}_q$.*

Corollary 3.4. *One has*

$$\pi^* \operatorname{End}_{\mathcal{O}_F}(B) = \{\alpha + \beta \otimes \frac{D+\sqrt{D}}{2} : \alpha, \beta \in \phi^{-1}\operatorname{Hom}(E, E')) \text{ satisfies } (*_q) \text{ below } \}. \tag{3.14}$$

*Here the matrices of $\alpha$ and $\beta$ with respect to a $\phi$-normal basis of $T_q(E)$, still denoted by $\alpha$ and $\beta$ respectively, have the following property $(*_q)$*

$$\alpha + \beta\frac{D+\sqrt{D}}{2} \in \begin{pmatrix} \mathbb{Z}_q & \frac{1}{q}\mathbb{Z}_q \\ q\mathbb{Z}_q & \mathbb{Z}_q \end{pmatrix}, \quad \alpha + \beta\frac{D-\sqrt{D}}{2} \in M_2(\mathbb{Z}_q). \tag{$*_q$}$$

*$(*_q)$ is equivalent to the condition*

$$\alpha + \beta\frac{D+\sqrt{D}}{2} \in \operatorname{End}(T_q(E')), \quad \alpha + \beta\frac{D-\sqrt{D}}{2} \in \operatorname{End}(T_q(E)). \tag{3.15}$$

**4. Local Intersection index.** Let the notation and assumption be as in Section 3. The purpose of this section is to compute the local intersection index $i_p(\phi, \iota)$ in (3.7). We need a little preparation. Replacing $\Delta$ by $m\Delta$ in [Ya4, Lemma 4.1], one has

Lemma 4.1. *Let $m \ge 1$ be an integer and let $0 < n < m\sqrt{\tilde{D}}$ be an integer with $\frac{m^2\tilde{D}-n^2}{D} \in \mathbb{Z}_{>0}$.*

*(1) When $D \nmid n$, there is a unique sign $\mu = \pm 1$ and a unique $2 \times 2$ positive definite matrix $T_m(\mu n) = \left(\begin{smallmatrix} a & b \\ b & c \end{smallmatrix}\right) \in \frac{1}{m}Sym_2(\mathbb{Z})$ such that*

$$\det T_m(\mu n) = ac - b^2 = \frac{m^2\tilde{D} - n^2}{Dm^2}, \tag{4.1}$$

$$\Delta = \frac{2\mu n_1 - Dc - (2b + Dc)\sqrt{D}}{2}, \tag{4.2}$$

$$-\mu n_1 = a + Db + \frac{D^2 - D}{4}c. \tag{4.3}$$

*Here $n_1 = n/m$.*

*(2) When $D|n$, for every sign $\mu = \pm 1$ there is a unique $2 \times 2$ integral positive definite matrix $T_m(\mu n) = \left(\begin{smallmatrix} a & b \\ b & c \end{smallmatrix}\right)$ satisfying the above conditions.*

REMARK 4.2. Throughout this paper, the sum $\sum_\mu$ means either $\sum_{\mu=\pm 1}$ when $D|n$ or the unique term $\mu$ satisfying the condition in Lemma 4.1 when $D \nmid n$.

Notice that (4.2) implies

$$2\mu n_1 - Dc, \quad 2b + Dc \in \mathbb{Z}. \tag{4.4}$$

Now let $p \neq q$ be a prime, and let $\phi : E \to E'$ be a cyclic isogeny of degree $q$ of supersingular elliptic curves over $\bar{\mathbb{F}}_p$, i.e., $(\phi : E \to E') \in \mathcal{Y}_0(q)(\bar{\mathbb{F}}_p)$. We consider the set $I(\phi)$ of $\mathcal{O}_K$-actions

$$\iota : \mathcal{O}_K \hookrightarrow \operatorname{End}_{\mathcal{O}_F}(B)$$

such that the Rosati involution associated to $\lambda$ gives the complex conjugation on $K$ (as in Section 3). Set

$$\pi^*\iota(\frac{w+\sqrt{\Delta}}{2}) = \alpha_0 + \beta_0\frac{D+\sqrt{D}}{2}, \quad \alpha_0, \beta_0 \in \phi^{-1}\operatorname{Hom}(E, E') \tag{4.5}$$

$$\pi^*\iota(\sqrt{\Delta}) = \alpha + \beta\frac{D+\sqrt{D}}{2} = x_1 + x_2\sqrt{D}, \tag{4.6}$$

with

$$\alpha = 2\alpha_0 - w_0, \quad \beta = 2\beta_0 - w_1, \tag{4.7}$$

and

$$x_1 = \alpha + \frac{D}{2}\beta, \quad x_2 = \frac{1}{2}\beta. \tag{4.8}$$

Let $\mathbb{O}_E = \operatorname{End}(E)$ and $\mathbb{B} = \mathbb{O}_E \otimes \mathbb{Q}$,

$$V = \{x \in \mathbb{B} : \operatorname{tr} x = 0\}, \quad Q(x) = -x^2 \tag{4.9}$$

and let

$$L(\phi) = (\mathbb{Z} + 2\phi^{-1}\operatorname{Hom}(E, E')) \cap V. \tag{4.10}$$

Then $\alpha, \beta \in L(\phi)$.

Notice that $(V, Q)$ is a quadratic subspace of the quadratic space $(\mathbb{B}, \det)$ where $\det(x)$ is the reduced norm of $x$. For $\vec{x} = (x_1, x_2, \cdots, x_n) \in \mathbb{B}^n$, we write

$$T(\vec{x}) = \frac{1}{2}(\vec{x}, \vec{x}) = \frac{1}{2}((x_i, x_j)). \tag{4.11}$$

Let $\mathbb{T}(\phi)$ be the set of pairs $(\alpha, \beta) \in L(\phi)^2$ which satisfies $(*_q)$ and $T(\alpha, \beta) = T_q(\mu n)$ for some integer (unique) $0 < n < q\sqrt{\tilde{D}}$ with $\frac{q^2\tilde{D}-n^2}{4D} \in p\mathbb{Z}_{>0}$ and some sign (unique) $\mu = \pm 1$.

Let $\tilde{\mathbb{T}}(\phi)$ be the set of pairs $(\alpha_0, \beta_0) \in (\phi^{-1}\operatorname{Hom}(E, E'))^2$ which satisfies $(*_q)$ and $T(1, \alpha_0, \beta_0) = \tilde{T}_q(\mu n)$ for some integer $0 < n < q\sqrt{\tilde{D}}$ with $\frac{q^2\tilde{D}-n^2}{4D} \in p\mathbb{Z}_{>0}$ and some sign $\mu = \pm 1$. Here
(4.12)

$$\tilde{T} = \begin{pmatrix} 1 & 0 & 0 \\ \frac{w_0}{2} & \frac{1}{2} & 0 \\ \frac{w_1}{2} & 0 & \frac{1}{2} \end{pmatrix} \operatorname{diag}(1, T) \begin{pmatrix} 1 & \frac{w_1}{2} & \frac{w_1}{2} \\ 0 & \frac{1}{2} & 0 \\ 0 & 0 & \frac{1}{2} \end{pmatrix} = \begin{pmatrix} 1 & \frac{w_1}{2} & \frac{w_1}{2} \\ \frac{w_0}{2} & \frac{1}{4}(a + w_0^2) & \frac{1}{4}(b + w_0 w_1) \\ \frac{w_1}{2} & \frac{1}{4}(b + w_0 w_1) & \frac{1}{4}(c + w_1^2) \end{pmatrix}$$

and $w = w_0 + w_1 \frac{D+\sqrt{D}}{2}$ is given in (1.5).

Proposition 4.3. *The correspondences*

$$\iota \in I(\phi) \leftrightarrow (\alpha, \beta) \in \mathbb{T}(\phi) \leftrightarrow (\alpha_0, \beta_0) \in \tilde{\mathbb{T}}(\phi)$$

*via (4.5)-(4.7) give bijections among $I(\phi)$, $\mathbb{T}(\phi)$, and $\tilde{\mathbb{T}}(\phi)$.*

*Proof.* Given $\iota \in I(\phi)$, and let $\alpha$ and $\beta$ be given via (4.6). Then $(\alpha, \beta) \in L(\phi)^2$ and satisfies $(*_q)$. Write $T(\alpha, \beta) = \left(\begin{smallmatrix} a & b \\ b & c \end{smallmatrix}\right)$ with $a = \frac{1}{2}(\alpha, \alpha) = -\alpha^2$, $b = \frac{1}{2}(\alpha, \beta)$, and $c = \frac{1}{2}(\beta, \beta) = -\beta^2$. First,

$$\begin{aligned} \Delta = (\pi^* \iota(\sqrt{\Delta}))^2 &= (\alpha + \frac{D}{2}\beta)^2 - (\alpha + \frac{D}{2}\beta, \frac{1}{2}\beta)\sqrt{D} \\ &= -a - Db - \frac{D^2 + D}{4}c - (b + \frac{1}{2}Dc)\sqrt{D}. \end{aligned}$$

We define $n = qn_1 > 0$ and $\mu = \pm 1$ by

$$-\mu n_1 = a + Db + \frac{D^2 - D}{4}c.$$

Then

$$\Delta = \frac{2\mu n_1 - Dc - (2b + Dc)\sqrt{D}}{2}$$

satisfying (4.2) in Lemma 4.1. Now a simple calculation using $\tilde{D} = \Delta\Delta'$ gives

$$\det T(\alpha, \beta) = ac - b^2 = \frac{q^2\tilde{D} - n^2}{q^2 D}$$

satisfying (4.1). So $T(\alpha, \beta) = T_q(\mu n)$ for a unique integer $n$ and a unique sign $\mu$ satisfying the conditions in Lemma 4.1. To show $p | q^2 \det T_q(\mu n) = \frac{q^2\tilde{D}-n^2}{D}$, we work over $\mathbb{Z}_p$ to avoid the denominator $q$ in $\det T_q(\mu n)$. Write $L_p = L(\phi) \otimes \mathbb{Z}_p$, and $\mathcal{O}_p = \mathbb{O}_E \otimes \mathbb{Z}_p$, then

$$L_p = (\mathbb{Z}_p + 2\mathcal{O}_p) \cap (V \otimes \mathbb{Q}_p)$$

has determinant $4p^2$. Let

$$\gamma = (\alpha, \beta) + 2\alpha\beta \in L_p.$$

Then

$$(\alpha, \gamma) = (\beta, \gamma) = 0, \quad (\gamma, \gamma) = 2(\alpha, \alpha)(\beta, \beta) - 2(\alpha, \beta)^2 = 8 \det T_q(\mu n).$$

So the determinant of $\{\alpha, \beta, \gamma\}$ is

$$\det T(\alpha,\beta,\gamma) = \det \operatorname{diag}(T_q(\mu n), 4\det T_q(\mu n)) = 4\det T_q(\mu n)^2.$$

So we have thus $p|\det T_q(\mu n)$ in $\mathbb{Z}_p$, i.e., $p|\frac{q^2\tilde{D}-n^2}{D}$. Similarly, to show $4|q^2\det T_q(\mu n)$, we work over $\mathbb{Z}_2$. It is easier to look at $\tilde{T}_q(\mu n) \in \operatorname{Sym}_3(\mathbb{Z}_2)^\vee$ (since $\alpha_0, \beta_0 \in \mathbb{O}_E \otimes \mathbb{Z}_2$). It implies that

$$a \equiv -w_0^2 \mod 4, \quad b \equiv -w_0 w_1 \mod 2, \quad c \equiv -w_1^2 \mod 4. \tag{4.13}$$

So $\det T_q(\mu n) = ac - b^2 \equiv 0 \mod 4$, and therefore $(\alpha,\beta) \in \mathbb{T}(\phi)$. A simple linear algebra calculation shows that $(\alpha_0, \beta_0) \in \tilde{\mathbb{T}}(\phi)$.

Next, we assume that $(\alpha,\beta) \in \mathbb{T}(\phi)$. Define $\iota$ and $(\alpha_0,\beta_0)$ by (4.6) and (4.7). The above calculation gives

$$(\alpha + \beta\frac{D+\sqrt{D}}{2})^2 = \Delta,$$

so $\iota$ gives an embedding from $K$ into $\operatorname{End}^0_{\mathcal{O}_F} B$ such that $\iota(\mathcal{O}_F[\sqrt{\Delta}]) \in \operatorname{End}_{\mathcal{O}_F} B$. To show that $\iota \in I(\phi)$, it suffices to show $\alpha_0, \beta_0 \in \phi^{-1}\operatorname{Hom}(E,E')$. Write by definition

$$\alpha = -u_0 + 2\alpha_1, \quad \beta = -u_1 + 2\beta_1, \quad u = u_0 + u_1\frac{D+\sqrt{D}}{2}$$

with $u_i \in \mathbb{Z}$, $\alpha_1, \beta_1 \in \phi^{-1}\operatorname{Hom}(E,E')$ . Then

$$\pi^*\iota(\frac{u+\sqrt{\Delta}}{2}) = \alpha_1 + \beta_1\frac{D+\sqrt{D}}{2}$$

and $(\alpha_1,\beta_1) \in (\phi^{-1}(E,E'))^2$ satisfies the condition $(*_q)$. So $\iota(\frac{u+\sqrt{\Delta}}{2}) \in \operatorname{End}_{\mathcal{O}_F} B$ and thus $\frac{u+\sqrt{\Delta}}{2} \in \mathcal{O}_K$. On the other hand, $\frac{w+\sqrt{\Delta}}{2} \in \mathcal{O}_K$. So $\frac{u-w}{2} \in \mathcal{O}_F$, i.e., $\frac{w_i-u_i}{2} \in \mathbb{Z}$, and

$$\alpha_0 = \alpha_1 + \frac{w_0-u_1}{2} \in \phi^{-1}(E,E'), \quad \beta_0 = \beta_1 + \frac{w_1-u_1}{2} \in \phi^{-1}(E,E')$$

as claimed. So $(\alpha_0,\beta_0) \in \tilde{\mathbb{T}}(\phi)$ and $\iota \in I(\phi)$. Finally, if $(\alpha_0,\beta_0) \in \tilde{\mathbb{T}}(\phi)$, let $(\alpha,\beta)$ be given by (4.7). Then it is easy to check that $(\alpha,\beta) \in \mathbb{T}(\phi)$. □

Now we are ready to compute local intersection indices.

PROPOSITION 4.4. *Let $\phi : E \to E'$ be an isogeny of supersingular elliptic curves over $\bar{\mathbb{F}}_p$ of degree $q$ $(p \neq q)$. Let $(\alpha,\beta) \in \mathbb{T}(\phi)$ be associated to $\iota \in I(\phi)$, and let $T_q(\mu n) = T(\alpha,\beta)$ be the associated matrix as in Proposition 4.3. Then*

$$i_p(\phi,\iota) = \frac{1}{2}\left(\operatorname{ord}_p \frac{q^2\tilde{D}-n^2}{4D} + 1\right)$$

*depends only on $n$.*

*Proof.* This is a local question at $p$. $\iota \in I(\phi)$ can be lifted to an embedding $\iota_I : \mathcal{O}_K \hookrightarrow \operatorname{End}_{\mathcal{O}_F}(B_I)$ if and only if $\alpha_0$ and $\beta_0$ can be lifted to $\alpha_{0,I}, \beta_{0,I} \in \phi_I^{-1}\operatorname{Hom}(E_I, E'_E)$, which is equivalent to that $\phi$, $\phi\alpha_0$ and $\phi\beta_0$ can be lifted to isogenies from $E_I$ to $E_I'$. So $\iota_p(\phi, \iota) = i_p(\phi, \phi\alpha_0, \phi\beta_0)$ is the local intersection index of $\phi, \phi\alpha_0, \phi\beta_0$ computed by Gross and Keating [GK]. It depends only on $T(\phi, \phi\alpha_0, \phi\beta_0) = qT_q(\mu n)$. The same calculation as in [Ya4, Theorem 3.1] (using Gross and Keating 's formula) gives (recall $n_1 = n/q, p \neq q$)

$$i_p(\phi, \iota) = \frac{1}{2}\left(\operatorname{ord}_p \frac{\tilde{D} - n_1^2}{4D} + 1\right) = \frac{1}{2}\left(\operatorname{ord}_p \frac{q^2\tilde{D} - n^2}{4D} + 1\right)$$

□

So we have by (3.6) and Proposition 4.4

Theorem 4.5. *For $p \neq q$, one has*

$$(\mathcal{T}_q.\mathcal{CM}(K))_p = \frac{1}{2} \sum_{\substack{0<n<q\sqrt{\tilde{D}} \\ \frac{q^2\tilde{D}-n^2}{4D} \in p\mathbb{Z}_{>0}}} \left(\operatorname{ord}_p \frac{q^2\tilde{D} - n^2}{4D} + 1\right) \sum_\mu \sum_\phi \frac{R(\phi, T_q(\mu n))}{\#Aut(\phi)}.$$

*Here $R(\phi, T_q(\mu n))$ is the number of pairs $(\alpha, \beta) \in L(\phi)^2$ such that $T(\alpha, \beta) = T_q(\mu n)$ and $(\alpha, \beta)$ satisfies the condition $(*_q)$, and $\sum_\phi$ is over all isogenies (up to equivalence) $\phi : E \to E'$ of supersingular elliptic curves over $\bar{\mathbb{F}}_p$ of degree $q$ up to equivalence. Two isogenies $\phi_i : E_i \to E_i'$ are equivalent if there isomorphisms $f : E_1 \cong E_2$ and $f' : E_1' \cong E_2'$ such $\phi_2 f = f'\phi_1$.*

**5. Local densities.** We write $[\phi : E \to E']$ for the equivalence class of $\phi$ and

$$\beta(p, \mu n) = \sum_{[\phi:E\to E']} \frac{R(\phi, T_q(\mu n))}{\#\mathrm{Aut}(\phi)}. \tag{5.1}$$

One can show that $\beta(p, \mu n)$ is the $T_q(\mu n)$-th Fourier coefficient of some Siegel-Eisenstein series of genus two and weight 3/2, and is thus product of local Whittaker functions, which are slight generalization of local densities computed in [Ya1] and [Ya2]. In principle, the idea in [Ya1] and [Ya2] can be extended to handle the general case. However, the actual computation is already complicated in [Ya1] and [Ya2]. In this section, we use a different way to write $\beta(p, \mu n)$ directly as product of local integrals over quaternions. In next section, we take advantage of known structure of quaternions to compute the involved local integrals.

Fix a cyclic isogeny $\phi_0 : E_0 \to E_0'$ of supersingular elliptic curves (over $\bar{\mathbb{F}}_p$) of degree $q$. and a $\phi_0$-normal basis $\{e_0, f_0\}$ of the Tate module $T_q(E_0)$. Let $\mathcal{O} = \mathrm{End}(E_0)$ and $\mathbb{B} = \mathcal{O} \otimes \mathbb{Q}$ be the unique quaternion algebra over $\mathbb{Q}$ ramified exactly at $p$ and $\infty$. Let $(B_0, \iota_0, \lambda_0) \in \mathcal{M}(\bar{\mathbb{F}}_p)$ be the abelian surface with real multiplication associated to $\phi_0$. Let $V$ and $L(\phi_0)$ be the ternary quadratic space and lattice defined in (4.9) and (4.10) with $\phi$ replaced by $\phi_0$. For $l \neq q$, let

$$L_l = L(\phi_0) \otimes \mathbb{Z}_l, \quad \Psi_l = \mathrm{char}(L_l^2). \tag{5.2}$$

For $l = q$, view $\mathbb{B}_q = \mathbb{B} \otimes \mathbb{Q}_q$ as the endomorphism ring of $V_q(E_0) = T_q(E_0) \otimes \mathbb{Q}_q$ and identify it with $M_2(\mathbb{Q}_q)$ using the $\phi$-normal basis $\{e_0, f_0\}$. Under this identification, $\mathcal{O}_q = M_2(\mathbb{Z}_q)$. Let

$$L_q' = \{X = \begin{pmatrix} x & \frac{1}{q}y \\ z & -x \end{pmatrix} \in V_q : x, y, z \in \mathbb{Z}_q\} \tag{5.3}$$

and

$$
\begin{aligned}
(5.4)\qquad \Omega_q =&\{\vec{x} = {}^t(X_1, X_2) \in (L'_q)^2 :\, z_1 + z_2 \frac{D+\sqrt{D}}{2} \equiv 0 \mod q,\\
& y_1 + y_2 \frac{D-\sqrt{D}}{2} \equiv 0 \mod q\}
\end{aligned}
$$

where $X_i = \left(\begin{smallmatrix} x_i & \frac{1}{q} y_i \\ z_i & -x_i \end{smallmatrix}\right) \in L'_q$. Let

$$
(5.5)\qquad \Psi_q = \mathrm{char}(\Omega_q), \quad \Psi = \otimes_{l<\infty} \Psi_l \in S(V(\mathbb{A}_f)^2).
$$

Next, let $\mathcal{K} = \prod_{l<\infty} \mathcal{K}_l \subset \mathbb{B}_f^*$ be the compact subgroup of $\mathbb{B}_f^*$ defined by

$$
(5.6)\qquad \mathcal{K}_l = \begin{cases} \mathcal{O}_l^* & \text{if } l \neq q, \\ K_0(q) = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in M_2(\mathbb{Z}_q) : c \equiv 0 \mod q\} & \text{if } l = q. \end{cases}
$$

Clearly, $\Psi$ is $\mathcal{K}$-invariant. The main purpose of this section is to prove

THEOREM 5.1. *Let the notation be as above. Then*

$$
(5.7)\qquad \beta(p, \mu n) = \frac{1}{2} \int_{\mathbb{Q}_f^* \backslash \mathbb{B}_f^* / \mathcal{K}} \Psi(g^{-1}.\vec{x}_0) dg
$$

*if there is $\vec{x}_0 = V(\mathbb{A}_f)^2$ with $T(\vec{x}_0) = T_q(\mu n)$. Otherwise, $\beta(p, \mu n) = 0$. Here*

$$
g.\vec{x} = (g.X_1, g.X_2) = (gX_1g^{-1}, gX_2g^{-1}), \quad \vec{x} = {}^t(X_1, X_2),
$$

*and $dg$ is the Tamagawa measure on $\mathbb{B}_f^*$.*

We first recall a close relation between $\mathbb{B}_f^*$ and cyclic isogenies $\phi : E \to E'$ of degree $q$. Let $T_l(E)$ be the $l$-Tate module of $E$ for $l \neq p$ and let $T_p(E)$ be the covariant Dieúdonne module of $E$ over the Witt ring $W = W(\bar{\mathbb{F}}_p)$, and let $\hat{T}(E) = \otimes T_l(E)$. A homomorphism from $T_p(E)$ to $T_p(E')$ means a $W$-linear map on the Dieudonné modules which commute with the Frobenius map. Then for $b \in \mathbb{B}_f^*$, there is an quasi-isogeny $f : E \to E_0$ such that $\hat{T}(f)\hat{T}(E) = b\hat{T}(E_0)$. Moreover, the equivalence class of $f : E \to E_0$ is determined by $b \mod \hat{\mathcal{O}}^*$ [Wel, Section 2.4]. Choose an integer $n > 0$ such that $nf$ is an isogeny. Let $E'$ be the fiber product as shown in the following diagram.

$$
(5.8)\qquad \begin{tikzcd}
E \arrow[r, dashed, "\phi"] \arrow[d, "nf"] & E' \arrow[r, "\phi_1"] \arrow[d, "nf'"] & E \arrow[d, "nf"] \\
E_0 \arrow[r, "\phi_0"] & E'_0 \arrow[r, "\phi'_0"] & E_0
\end{tikzcd}
$$

Then there is a unique $\phi : E \to E'$ making the above diagram commute. Let $\mathcal{S}_0(q)$ be the set of equivalence classes $[\phi : E \to E', f, f']$ of the diagrams:

$$
(5.9)\qquad \begin{tikzcd}
E \arrow[r, "\phi"] \arrow[d, squiggly, "f"] & E' \arrow[d, squiggly, "f'"] \\
E_0 \arrow[r, "\phi_0"] & E'_0
\end{tikzcd}
$$

where $E \rightsquigarrow E_0$ stands for quasi-isogeny. Here two such diagrams are equivalent if there are isomorphisms $g : E_1 \to E_2$ and $g' : E_1' \to E_2'$ such that the following diagram commutes:

(5.10)
$$\begin{tikzcd}
E_1 \arrow[rr, "\phi_1"] \arrow[dr, dashed, "g"] \arrow[dd, squiggly, "f_1"'] & & E_1' \arrow[dr, dashed, "g'"] \arrow[dd, squiggly, "f_1'" near start] & \\
& E_2 \arrow[rr, "\phi_2" near start] \arrow[dl, squiggly, "f_2"] & & E_2' \arrow[dl, squiggly, "f_2'"] \\
E_0 \arrow[rr, "\phi_0"] & & E_0' &
\end{tikzcd}.$$

Let $S_0(q)$ be the set of equivalence classes $[\phi : E \to E']$ of degree $q$ isogenies of supersingular curves over $\bar{\mathbb{F}}_p$. Then one has

Proposition 5.2. *The map $b \in \mathbb{B}_f^* \mapsto [\phi : E \to E', f, f']$ gives rise to a bijection between $\mathbb{B}_f^*/\mathcal{K}$ and $\mathcal{S}_0(q)$. The map $b \in \mathbb{B}_f^* \mapsto [\phi : E \to E']$ gives rise to a bijection between $\mathbb{B}^*\backslash\mathbb{B}_f^*/\mathcal{K}$ and the set $S_0(q)$. Moreover, for $\alpha_0, \beta_0 \in \mathbb{B} = \mathrm{End}(E_0) \otimes \mathbb{Q}$, let $\alpha = f^{-1}\alpha_0 f, \beta = f^{-1}\beta_0 f \in \mathrm{End}(E) \otimes \mathbb{Q}$. Then*

*(1) $\alpha \in \mathrm{End}(E)$ if and only if $b^{-1}\alpha_0 b \in \hat{\mathcal{O}} = \mathcal{O} \otimes \hat{\mathbb{Z}}$.*

*(2) $\phi\alpha\phi^{-1} \in \mathrm{End}(E')$ if and only if $\phi_0 b^{-1}\alpha_0 b\phi_0^{-1} \in \mathrm{End}(E_0') \otimes \hat{\mathbb{Z}}$.*

*(3) $\alpha \in \mathrm{End}(\phi)$ if and only if $b^{-1}\alpha_0 b \in \mathrm{End}(\phi_0) \otimes \hat{\mathbb{Z}}$.*

*(4) $\alpha + \beta\frac{D+\sqrt{D}}{2} \in \pi^* \mathrm{End}_{\mathcal{O}_F}(B)$ if and only if $b^{-1}(\alpha_0 + \beta_0\frac{D+\sqrt{D}}{2})b \in \pi_0^*(\mathrm{End}_{\mathcal{O}_F}(B_0) \otimes \hat{\mathbb{Z}})$.*

*Proof.* The same argument as in [We1, Section 2.4] gives the bijections.

(1) Clearly, $\alpha \in \mathrm{End}(E)$ if and only if $\hat{T}(\alpha)\hat{T}(E) \subset \hat{T}(E)$. If $b^{-1}\alpha_0 b \in \hat{\mathcal{O}}$, then

$$\begin{aligned}\hat{T}(\alpha)\hat{T}(E) &= \hat{T}(f)^{-1}\hat{T}(\alpha_0)\hat{T}(f)\hat{T}(E) = \hat{T}(f)^{-1}bb^{-1}\alpha_0 b\hat{T}(E_0)\\ &\subset \hat{T}(f)^{-1}b\hat{T}_0(E_0) = \hat{T}(f)^{-1}\hat{T}(f)\hat{T}(E) = \hat{T}(E),\end{aligned}$$

and thus $\alpha \in \mathrm{End}(E)$. Here we identify $\alpha_0$ with $\hat{T}(\alpha_0) \in \mathrm{End}^0(\hat{T}(E))$. Reversing the procedure with $\alpha_0 = f\alpha f^{-1}$, one sees that $b^{-1}\alpha_0 b \in \hat{\mathcal{O}}$ if $\alpha \in \mathrm{End}(E)$.

(2) Since

$$\hat{T}(\phi\alpha\phi^{-1}) = \hat{T}(\phi f^{-1})\hat{T}(\alpha_0)\hat{T}(f\phi^{-1}) = \hat{T}(f')^{-1}\hat{T}(\phi_0\alpha_0\phi_0^{-1})\hat{T}(f'),$$

the equivalence class of $E' \rightsquigarrow E_0'$ is associated to $b' = \phi_0 b\phi_0^{-1}$ when $E \rightsquigarrow E_0$ is associated to $b$. Now (2) follows from (1). (3) follows from (1) and (2) since $\alpha \in \mathrm{End}(\phi)$ if and only if $\alpha \in \mathrm{End}(E)$ and $\phi\alpha\phi^{-1} \in \mathrm{End}(E')$.

(4) Since

$$\hat{T}(\phi\alpha) = \hat{T}(f')(\phi_0 b\phi_0^{-1})\phi_0(b^{-1}\alpha_0 b),$$

$\alpha \in \phi^{-1}\mathrm{Hom}(E, E')$ if and only if $b^{-1}\alpha_0 b \in \phi_0^{-1}\mathrm{Hom}(\hat{T}(E), \hat{T}(E'))$. So by (1) and

(2) (more precisely their local analogue at $q$) and Corollary 3.4, one has

$$\begin{aligned}
&\alpha+\beta\frac{D+\sqrt{D}}{2} \in \pi^* \operatorname{End}_{\mathcal{O}_F}(B)\\
&\Leftrightarrow \alpha, \beta \in \phi^{-1}\operatorname{Hom}(E, E') \text{ and } (3.15)\\
&\Leftrightarrow b^{-1}\alpha_0 b, b^{-1}\beta_0 b \in \phi_0^{-1}\operatorname{Hom}(\hat{T}(E), \hat{T}(E')), \text{ and (3.15) for } (b^{-1}\alpha_0 b, b^{-1}\beta_0 b)\\
&\Leftrightarrow b^{-1}(\alpha_0+\beta_0\frac{D+\sqrt{D}}{2})b \in \pi_0^*(\operatorname{End}_{\mathcal{O}_F}(B_0)\otimes\hat{\mathbb{Z}})
\end{aligned}$$

as claimed. □

*Proof of Theorem 5.1.* Let

$$f_{\mu n}(g) = \sum_{\substack{\vec{x}\in V^2\\ T(\vec{x})=T_q(\mu n)}} \Psi(g^{-1}.\vec{x}). \tag{5.11}$$

Then $f_{\mu n}$ is left $\mathbb{B}^*$-invariant and right $\mathcal{K}$-invariant. We claim

$$\beta(p, \mu n) = \int_{\mathbb{B}^*\backslash\mathbb{B}_f^*/\mathcal{K}} f_{\mu n}(g)dg. \tag{5.12}$$

Indeed, write $\mathbb{B}_f^* = \bigsqcup_j \mathbb{B}^* b_j \mathcal{K}$ with $b_j \in \mathbb{B}_f^*$, and let $[\phi_i : E_i \to E_i'] \in S_0(q)$ be the associated equivalence class of cyclic isogenies as given in Proposition 5.2. Since the map

$$\mathbb{B}^*\times\mathcal{K} \to \mathbb{B}^* b_j\mathcal{K}, \quad (b, k)\mapsto bb_jk$$

has fiber $\mathbb{B}^*\cap b_j\mathcal{K}b_j^{-1}$ at $b_j$, one has

$$\int_{\mathbb{B}^*\backslash\mathbb{B}_f^*/\mathcal{K}} f_{\mu n}(g)dg = \sum_j f(b_j)\int_{\mathbb{B}\backslash\mathbb{B}b_j\mathcal{K}/\mathcal{K}} dg = \sum_j \frac{1}{\#\mathbb{B}^*\cap b_j\mathcal{K}b_j^{-1}} f_{\mu n}(b_j).$$

Let $[\phi_j : E_j \to E_j'] \in S_0(q)$ be associated to $b_j$, and choose $f_j : E_j \rightsquigarrow E_0$ and $f_j' \rightsquigarrow E_0'$ so that $[\phi_j : E_j \to E_j', f_j, f_j'] \in \mathcal{S}_0(q)$ is associated to $b_j$ by Proposition 5.2. For $\vec{x} = {}^t(\delta_0, \beta_0) \in V^2$ with $T(\vec{x}) = T_q(\mu n)$, one has by definition $\Psi(\vec{x}) = 1$ if and only if $\delta_0+\beta_0\frac{D+\sqrt{D}}{2} \in \pi_0^*(\operatorname{End}_{\mathcal{O}_F}(B_0))$, and for $\vec{x} = {}^t(\delta_0, \beta_0) \in V(\mathbb{A}_f)^2$, $\Psi(\vec{x}) = 1$ if and only if $\delta_0+\beta_0\frac{D+\sqrt{D}}{2} \in \pi_0^*(\operatorname{End}_{\mathcal{O}_F}(B_0)\otimes\hat{\mathbb{Z}})$. So one has by Proposition 5.2

$$\Psi(b_j^{-1}.\vec{x}) = 1 \Leftrightarrow \delta_j+\beta_j\frac{D+\sqrt{D}}{2} \in \pi^*\operatorname{End}_{\mathcal{O}_F}(B_j)$$

where $\delta_j = f^{-1}\delta_0 f_j$ and $\beta_j = f_j^{-1}\delta_0 f_j$. So

$$f_{\mu n}(b_j) = R(\phi_j, T_q(\mu n)).$$

Next for $\delta_0 \in \mathbb{B}^*$, one has by Proposition 5.2

$$\begin{aligned}
\delta_0 \in \mathbb{B}^*\cap b_j\mathcal{K}b_j^{-1} &\Leftrightarrow b_j^{-1}\delta_0 b_j \in \mathcal{K} = (\operatorname{End}(\phi_0)\otimes\hat{\mathbb{Z}})^*\\
&\Leftrightarrow \delta = f_j^{-1}\delta_0 f_j \in \operatorname{Aut}(\phi_j).
\end{aligned}$$

So $\#\mathbb{B}^* \cap b_j\mathcal{K}b_j^{-1} = \#\mathrm{Aut}(\phi_j)$, and thus

$$\begin{aligned}\int_{\mathbb{B}^*\backslash\mathbb{B}_f^*/\mathcal{K}} f_{\mu n}(g)dg &= \sum_j \frac{1}{\#\mathbb{B}^* \cap b_j\mathcal{K}b_j^{-1}} f_{\mu n}(b_j)\\ &= \sum_j \frac{1}{\#\mathrm{Aut}(\phi_j)} R(\phi_j, T_q(\mu n))\\ &= \beta(p, \mu n)\end{aligned}$$

by Proposition 5.2. This proves claim (5.12). If there is no $\vec{x} \in V^2$ such that $T(\vec{x}) = T_q(\mu n)$, one has clearly $\beta(p, \mu n) = 0$ by (5.12). At the same time, the Hasse principle asserts that there is no $\vec{x} \in V(\mathbb{A}_f)^2$ with $T(\vec{x}) = T_q(\mu n)$, and thus the right hand side of (5.7) is zero too, Theorem 5.1 holds trivially in this case. Now assume there is a $\vec{x} \in V^2$ such that $T(\vec{x}) = T_q(\mu n)$, and choose such a vector $\vec{x}_0$. By Witt's theorem, for any $\vec{x} \in V^2$ with $T(\vec{x}) = T_q(\mu n)$, there is $b \in \mathbb{B}^*$ such that $b^{-1}.\vec{x}_0 = \vec{x}$. It is easy to check that the stabilizer of $\vec{x}_0$ in $\mathbb{B}^*$ is $\mathbb{Q}^*$. So we have

$$\begin{aligned}\int_{\mathbb{B}^*\backslash\mathbb{B}_f^*/\mathcal{K}} f_{\mu n}(g)dg &= \int_{\mathbb{B}^*\backslash\mathbb{B}_f^*/\mathcal{K}} \sum_{b\in\mathbb{Q}^*\backslash\mathbb{B}^*} \Psi((bg)^{-1}.\vec{x}_0)dg\\ &= \int_{\mathbb{Q}^*\backslash\mathbb{B}_f^*/\mathcal{K}} \Psi(g^{-1}.\vec{x}_0)dg\\ &= \int_{\mathbb{Q}^*\backslash\mathbb{Q}_f^*} d^*x \cdot \int_{\mathbb{Q}_f^*\backslash\mathbb{B}_f^*/\mathcal{K}} \Psi(g^{-1}.\vec{x}_0)dg.\end{aligned}$$

Here $d^*x$ is the Haar measure on $\mathbb{Q}_f^* = \mathbb{A}_f^*$ such that $\hat{\mathbb{Z}}^*$ has Haar measure 1. Now Theorem 5.1 follows from the well-known fact

$$\int_{\mathbb{Q}^*\backslash\mathbb{Q}_f^*} d^*x = \frac{1}{2},$$

since $\mathbb{Q}_f^* = \mathbb{Q}^*\hat{\mathbb{Z}}^*$ and $\mathbb{Q}^* \cap \hat{\mathbb{Z}}^* = \{\pm 1\}$.

## 6. Local computation.

Let the notation be as in Section 5. The main purpose of this section is to compute the local integrals

$$\beta_l(T_q(\mu n), \Psi_l) = \int_{\mathbb{Q}_l^*\backslash\mathbb{B}_l^*/\mathcal{K}_l} \Psi_l(h^{-1}.\vec{x}_0)dh \tag{6.1}$$

where $\vec{x}_0 \in V_l^2$ with $T(\vec{x}_0) = T_q(\mu n)$, and $dh$ is a Haar measure on $\mathbb{B}_l^*$. It is a long calculation for $l = q$ and is quite technical. We summarize the result as two separate theorems for the convenience of the reader. Theorem 6.1 will be restated as Propositions 6.5 and 6.6, while Theorem 6.2 will be restated as Propositions 6.7, 6.11, and 6.12

THEOREM 6.1. *For $l \neq q$, $T_q(\mu n)$ is $\mathbb{Z}_l$-equivalent to $\mathrm{diag}(\alpha_l, \alpha_l^{-1}\det T_q(\mu n))$ with $\alpha_l \in \mathbb{Z}_l^*$. Let $t_l = \mathrm{ord}_l \frac{q^2\tilde{D}-n^2}{4Dq^2}$. Then*

$$\beta_l(T_q(\mu n), \Psi_l) = \begin{cases} 1 - (-\alpha_p, p)_p^{t_p} & \text{if } l = p,\\ \frac{1+(-1)^{t_l}}{2} & \text{if } l \neq p, (-\alpha_l, l)_l = -1,\\ t_l + 1 & \text{if } l \neq p, (-\alpha_l, l)_l = 1.\end{cases}$$

Theorem 6.2.

*(1)* *If $q \nmid n$, then $\beta_q(T_q(\mu n), \Psi_q) = 1$.*

*(2)* *If $q|n$ and $t_q = \operatorname{ord}_q \frac{q^2\tilde{D}-n^2}{4Dq^2} = 0$, then*

$$\beta_q(T_q(\mu n, \Psi_q) = \begin{cases} 4 & \textit{if } q \textit{ split completely in } \tilde{K}, \\ 2 & \textit{if } q \textit{ inert in } \tilde{F}, q\mathcal{O}_{\tilde{F}} \textit{ split in } \tilde{K}, \\ 0 & \textit{otherwise.} \end{cases}$$

*(3)* *If $q|n$ and $t_q = \operatorname{ord}_q \frac{q^2\tilde{D}-n^2}{4Dq^2} > 0$, then $T_q(\mu n)$ is $\mathbb{Z}_q$-equivalent to $\operatorname{diag}(\alpha_q, \alpha_q^{-1} \det T_q(\mu n))$ with $\alpha_q \in \mathbb{Z}_q^*$, and*

$$\beta_q(T_q(\mu n), \Psi_q) = \begin{cases} 0 & \textit{if } (-\alpha_q, q)_q = -1, \\ 2(t_q + 2) & \textit{if } (-\alpha_q, q)_q = 1. \end{cases}$$

For any locally constant function with compact support $f \in S(V_l^2)$ and a non-degenerate symmetric $2 \times 2$ matrix $T$ over $\mathbb{Q}_l$, let

$$\gamma_l(T, f) = \int_{\mathbb{Q}_l^* \backslash \mathbb{B}_l^*} f(h^{-1}.\vec{x}_0)dh \tag{6.2}$$

with $T(\vec{x}_0) = T$. Then

$$\beta_l(T_q(\mu n), \Psi_l) = \frac{1}{\operatorname{vol}(K_l)} \gamma_l(T_q(\mu n), \Psi_l). \tag{6.3}$$

Notice that $\beta_l$ is independent of the choice of the Haar measure while $\gamma_l$ gives freedom of the choice of $f \in S(V_l^2)$. We first give some general comments and lemmas.

When $l \neq p$, $\mathbb{B}_l^* = \mathrm{GL}_2(\mathbb{Q}_l)$ has two actions on $V_l^2$, the orthogonal action (by conjugation)

$$h.{}^t(X_1, X_2) = {}^t(hX_1h^{-1}, hX_2h^{-1})$$

and the natural linear action

$$\begin{pmatrix} g_1 & g_2 \\ g_3 & g_4 \end{pmatrix} \begin{pmatrix} X_1 \\ X_2 \end{pmatrix} = \begin{pmatrix} g_1X_1 + g_2X_2 \\ g_3X_1 + g_4X_2 \end{pmatrix}$$

To distinguish them, we write the orthogonal action as $h.x$. We also have the linear action of $\mathrm{GL}_2(\mathbb{Q}_p)$ on $V_p^2$ while $\mathbb{B}_p^*$ acts on $V_p^2$ orthogonally (by conjugation). These two actions commute. This commutativity implies the following lemma easily.

Lemma 6.3. *Let $T = g\tilde{T}\,{}^tg$ with $g \in \mathrm{GL}_2(\mathbb{Q}_l)$. Then for any $f \in S(V_l^2)$*

$$\gamma_l(T, f) = \gamma_l(\tilde{T}, f_{g^{-1}})$$

*where $f_g(\vec{x}) = f(g^{-1}\vec{x})$.*

The following lemma is well-known.

Lemma 6.4. *Write $h(r, u) = \left(\begin{smallmatrix} l^r & u \\ 0 & 1 \end{smallmatrix}\right)$ and $h'(r, u) = h(r, u)\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ for $r \in \mathbb{Z}$ and $u \in \mathbb{Q}_l$. Then*

$$\mathbb{Q}_l^* \backslash \operatorname{GL}_2(\mathbb{Q}_l) = \bigcup_{r \in \mathbb{Z}, u mod\ l^r} h(r,u) \operatorname{GL}_2(\mathbb{Z}_l),$$

$$\mathbb{Q}_q^* \backslash \operatorname{GL}_2(\mathbb{Q}_q) = \bigcup_{r \in \mathbb{Z}, u mod\ l^r} h(r,u) K_0(q) \bigcup ( \bigcup_{r \in \mathbb{Z}, u mod\ l^{r+1}} h'(r,u) K_0(q)),$$

*and*

$$\mathbb{Q}_p^* \backslash \mathbb{B}_p^* = \mathcal{O}_p^* \cup \pi \mathcal{O}_p^*$$

*where* $\pi \in \mathbb{B}_p^*$ *with* $\pi^2 = p$.

### 6.1. The case $l \nmid pq$.

Proposition 6.5. *For* $l \nmid pq$, $T_q(\mu n)$ *is* $\mathbb{Z}_l$*-equivalent to* $\operatorname{diag}(\alpha_l, \alpha_l^{-1} \det T_q(\mu n))$ *with* $\alpha_l \in \mathbb{Z}_l^*$. *Let* $t_l = \operatorname{ord}_l \det T_q(\mu n) = \operatorname{ord}_l \frac{q^2 \tilde{D} - n^2}{4Dq^2}$. *Then*

$$\beta_l(T_q(\mu n), \Psi_l) = \begin{cases} \frac{1+(-1)^{t_l}}{2} & \text{if } (-\alpha_l, l)_l = -1, \\ t_l + 1 & \text{if } (-\alpha_l, l)_l = 1. \end{cases}$$

*Proof.* Write $T_q(\mu n) = g \operatorname{diag}(\alpha_l, \alpha_l^{-1} \det T_q(\mu n)) {}^t g$ with some $g \in \operatorname{GL}_2(\mathbb{Z}_l)$. Since $\Psi_l$ is $\operatorname{GL}_2(\mathbb{Z}_l)$-invariant under the linear action, $(\Psi_l)_g = \Psi_l$. So Lemma 6.3 implies

$$\beta_l(T_q(\mu n), \Psi_l) = \beta_l(\operatorname{diag}(\alpha_l, \alpha_l^{-1} \det T_q(\mu n)), \Psi_l).$$

In general, for $T = \operatorname{diag}(\epsilon_1, \epsilon_2 l^t)$ with $\epsilon_i \in \mathbb{Z}_l^*$, $t \in \mathbb{Z}_{\geq 0}$, and $(-\epsilon_1, -\epsilon_2)_l = 1$ (it is only a condition for $l = 2$ and is true in our case $(\alpha_l, \alpha_l^{-1} \det T_q(\mu n))$ [Ya4, Lemma 4.1]), let

$$X_1 = \left( \begin{smallmatrix} 0 & 1 \\ -\epsilon_1 & 0 \end{smallmatrix} \right) \in L_l, \quad Q(X_1) = \epsilon_1, \tag{6.4}$$

Then

$$(\mathbb{Q}_l X_1)^\perp = \{ \left( \begin{smallmatrix} x & y \\ \epsilon_1 y & -x \end{smallmatrix} \right) \in V_l : x, y \in \mathbb{Q}_l \}. \tag{6.5}$$

So there is $\vec{x} = {}^t(X_1, X_2) \in V_l^2$ with $T(\vec{x}) = T$ if and only if there are $x, y \in \mathbb{Q}_l$ such that

$$x^2 + \epsilon_1 y^2 = -\epsilon_2 l^t, \tag{6.6}$$

which is equivalent to $(-\epsilon_1, -\epsilon_2 l^t)_l = 1$, i.e.,

$$(-\epsilon_1, l)_l^t = 1. \tag{6.7}$$

Assume (6.7) and $l \neq 2$. When $(-\epsilon_1, l)_l = -1$ and $t$ even, (6.6) has a solution $x_0, y_0 \in l^{\frac{t}{2}} \mathbb{Z}_l^*$. When $(-\epsilon_1, l)_l = 1$, (6.6) has a solution $x_0, y_0 \in \mathbb{Z}_l^*$. Fix such a solution, and let

$$X_2 = \left( \begin{smallmatrix} x_0 & y_0 \\ \epsilon_1 y_0 & -x_0 \end{smallmatrix} \right), \quad \vec{x}_0 = {}^t(X_1, X_2) \in L_l^2, \tag{6.8}$$

with $T(\vec{x}_0) = T$. A simple calculation gives

$$h(r,u)^{-1}.X_1 = \left(\begin{smallmatrix} \epsilon_1 u & l^{-r}(1+\epsilon_1 u^2) \\ -\epsilon_1 l^r & -\epsilon_1 u \end{smallmatrix}\right) \tag{6.9}$$

$$h(r,u)^{-1}.X_2 = \left(\begin{smallmatrix} x_0-\epsilon_1 y_0 u & l^{-r}(y_0+2x_0u-\epsilon_1 y_0 u^2) \\ \epsilon_1 y_0 l^r & -x_0+\epsilon_1 y_0 u \end{smallmatrix}\right) \tag{6.10}$$

So $h(r,u)^{-1}.\vec{x}_0 \in L_l^2$ if and only if

$$r \geq 0, u \in \mathbb{Z}_l, \quad 1+\epsilon_1 u^2 \equiv 0 \mod l^r, \quad y_0 + 2x_0 u - \epsilon_1 y_0 u^2 \equiv 0 \mod l^r,$$

or equivalently,

$$r \geq 0, b \in \mathbb{Z}_l, \quad x_0 u + y_0 \equiv 0 \mod l^r, \quad 1+\epsilon_1 u^2 \equiv 0 \mod l^r. \tag{6.11}$$

**Case 1**: First we assume $(-\epsilon_1, l)_l = -1$ and $t$ is even. In this case one has always $1+\epsilon_1 u^2 \in \mathbb{Z}_l^*$, and thus $r = 0$ and $u \in \mathbb{Z}_l$, i.e., $h(0,u) \in \mathcal{K}_l = \mathrm{GL}_2(\mathbb{Z}_l)$ is the only coset with $h(r,u)^{-1}.\vec{x}_0 \in L_l^2$, i.e., $\Psi_l(h(r,u).\vec{x}_0) \neq 0$. So $\beta_l(T, \Psi_l) = 1$ in this case.

**Case 2**: Now we assume $(\epsilon_1, l)_l = 1$. Using (6.11), one has

$$x_0^2(1+\epsilon_1 u^2) \equiv x_0^2 + \epsilon_1 y_0^2 = -\epsilon_2 l^t \mod l^r$$

and so $0 \leq r \leq t$. Moreover, for $0 \leq r \leq t$, the above condition also shows that $1+\epsilon_1 u^2 \equiv 0 \mod l^r$ follows from $u \equiv -\frac{y_0}{x_0} \mod l^r$. This implies

$$\begin{aligned}\beta_l(T, \Psi_l) &= \sum_{r \in \mathbb{Z}, u \bmod l^r} \Psi(h(r,u)^{-1}.\vec{x}_0) \\ &= \sum_{0 \leq r \leq t, u = -y_0/x_0 \bmod l^r} 1 = t+1.\end{aligned}$$

This proves the proposition for $l \neq 2$. This case $l = 2$ is similar with some modification, including

$$L_2 = \{A \in \mathbb{Z}_2 + 2M_2(\mathbb{Z}_2) : \mathrm{tr}\, A = 0\} = \{\left(\begin{smallmatrix} x & 2y \\ 2z & -x \end{smallmatrix}\right) : x, y, z \in \mathbb{Z}_2\}.$$

We leave the detail to the reader. □

**6.2. The case $l = p$.**

Proposition 6.6. *For $l = p$, $T_p(\mu n)$ is $\mathbb{Z}_p$-equivalent to* $\mathrm{diag}(\alpha_p, \alpha_p^{-1} \det T_q(\mu n))$ *with $\alpha_p \in \mathbb{Z}_p^*$, and*

$$\beta_p(T_q(\mu n), \Psi_p) = 1 - (-\alpha_p, p)_p^{t_p}.$$

*Proof.* We first assume that $p \neq 2$. Recall that $\mathcal{O}_p$ is the maximal order of $\mathbb{B}_p$ and is consisting of elements of integral reduced norm. So

$$L_p = (\mathbb{Z}_p + 2\mathcal{O}_p) \cap V_p = \{x \in V_p : Q(x) = -x^2 \in \mathbb{Z}_p\}$$

has a basis $\{e, \pi, \pi e\}$ with $e^2 = a \in \mathbb{Z}_p^*$, $\pi^2 = p$, and $\pi e = -e\pi$ with $(a,p)_p = -1$. Since $\Psi_p$ is $\mathrm{GL}_2(\mathbb{Z}_p)$-invariant (linearly), Lemma 6.3 implies that

$$\beta_p(T_q(\mu n), \Psi_p) = \beta_p(\mathrm{diag}(\alpha_p, \alpha_p^{-1} \det T_q(\mu n)), \Psi_p).$$

For $T = \operatorname{diag}(\epsilon_1, \epsilon_2 p^t)$ with $\epsilon_i \in \mathbb{Z}_p^*$ and $t \in \mathbb{Z}_{\geq 0}$ and $(-\epsilon_1, -\epsilon_2)_p = 1$, the above comment implies that if $T(\vec{x}) = T$ for some $\vec{x} \in V_p^2$, then $\vec{x} \in L_p^2$. If $X = x_1 e + x_2 \pi + x_3 \pi e$ satisfies

$$Q(X) = -ax_1^2 - px_2^2 + apx_3^2 = \epsilon_1,$$

then $(-\epsilon_1, p)_p = (a, p)_p = -1$. In this case, we choose $X_1 = x_1 e$ such that $Q(X_1) = -ax_1^2 = \epsilon_1$. Since $(\mathbb{Z}_p X_1)^\perp = \mathbb{Z}_p \pi + \mathbb{Z}_p \pi e$, finding $T(\vec{x}) = T$ with $\vec{x} = {}^t(X_1, X_2)$ is the same as finding $X_2 = y_2 \pi + y_3 \pi e$ with

$$Q(X_2) = -py_2^2 + pay_3^2 = \epsilon_2 p^t,$$

that is

$$y_2^2 - ay_3^2 = -\epsilon_2 p^{t-1}.$$

Since $(a, p)_p = (-\epsilon_1, p)_p = -1$ and $(a, -\epsilon_2)_p = (-\epsilon_1, -\epsilon_2)_p = 1$, it is equivalent to $t - 1$ being even. So there is $\vec{x} \in L_p^2$ such that $T(\vec{x}) = T$ if and only if

$$(-\epsilon_1, p)_p^t = -1.$$

Assuming this condition, choose one $\vec{x}_0 \in L_p^2$ with $T(\vec{x}_0) = T$. Notice that

$$\mathbb{Q}_p^* \backslash \mathbb{B}_p^* = \mathcal{O}_p^* \cup \pi \mathcal{O}_p^*$$

and $\pi . L_p^2 = L_p^2$. So in this case,

$$\beta_p(\operatorname{diag}(\epsilon_1, \epsilon_2 p^t, \Psi_p) = \int_{\mathbb{Q}_p^* \backslash \mathbb{B}_p^* / \mathcal{O}_p^*} \Psi_p(h^{-1}.\vec{x}_0) dh = 2.$$

In summary, we have

$$\beta_p(T_q(\mu n), \Psi_p) = 1 - (-\alpha_p, p)_p^{t_p}.$$

Now we assume $p = 2$. In this case,

$$\mathcal{O}_2 = \mathbb{Z}_2 + \mathbb{Z}_2 i + \mathbb{Z}_2 j + \mathbb{Z}_2 \frac{1 + i + j + k}{2}, \quad i^2 = j^2 = k^2 = -1, ij = -ji = k,$$

and so

$$L_2 = (\mathbb{Z}_2 + 2\mathcal{O}_2) \cap V_p = \mathbb{Z}_2 2i + \mathbb{Z}_2 2j + \mathbb{Z}_2(i + j + k)$$

is isomorphic to $\tilde{L} = \mathbb{Z}_2^3$ with quadratic form

$$Q(x, y, z) = 3x^2 + 8(y^2 + yz + z^2). \tag{6.12}$$

In order for it to represent $T = \operatorname{diag}(\epsilon_1, \epsilon_2 2^t)$ with $\epsilon_i \in \mathbb{Z}_2^*$ and $t \in \mathbb{Z}_{\geq 0}$, one has to have

$$\epsilon_1 = 3x^2 + 8(y^2 + yz + z^2) \equiv 3 \mod 8.$$

In such a case, we may choose $x_0 \in \mathbb{Z}_2^*$ such that $x_0^2 = \epsilon_1/3$. Let $e = (x_0, 0, 0) \in \tilde{L}$, then $Q(e) = \epsilon_1$. It is easy to see that $\tilde{L}$ represents $T$ if and only if $e^\perp$ represents $\epsilon_2 2^t$, i.e., $y^2+yz+z^2$ represents $\epsilon_2 2^{t-3}$, which is equivalent to that $t-3 \ge 0$ is even. Now the argument as above gives that

$$\beta_2(\mathrm{diag}(\epsilon_1, \epsilon_2 2^t), \Psi_2) = \begin{cases} 2 & \text{if } \epsilon_1 \equiv 3 \mod 8, t \ge 3 \text{ odd}, \\ 0 & \text{otherwise}. \end{cases}$$

For $T_q(\mu n) = \mathrm{diag}(\alpha_2, \alpha_2^{-1} \det T_q(\mu n))$ one has $\epsilon_1 = \alpha_2 \equiv 3 \mod 4$ and $t = t_2 + 2 = \mathrm{ord}_2 \det T_q(\mu n) = \mathrm{ord}_2 \frac{q^2\tilde{D}-n^2}{q^2 D} \ge 3$ since $\frac{q^2\tilde{D}-n^2}{q^2 D} \in 8\mathbb{Z}_2$. So we still have

$$\beta_2(T_q(\mu n), \Psi_2) = 1 - (-\alpha_2, 2)_2^{t_2}.$$

□

**6.3. The case $l = q$.** Now we come to the tricky case $l = q$. Recall

$$L'_q = \{X = \begin{pmatrix} x & \frac{1}{q}y \\ z & -x \end{pmatrix} : x, y, z \in \mathbb{Z}_q\}.$$

Let

$$\Omega'_q = \{x = {}^t(X_1, X_2) \in (L'_q)^2 : z_1 + z_2\sqrt{D} \equiv y_1 - y_2\sqrt{D} \equiv 0 \mod q\} \tag{6.13}$$

and $\Psi'_q = \mathrm{char}\Omega'_q$. Let

$$T'_q(\mu n) = \begin{pmatrix} 1 & \frac{D}{2} \\ 0 & \frac{1}{2} \end{pmatrix} T_q(\mu n) \begin{pmatrix} 1 & 0 \\ \frac{D}{2} & \frac{1}{2} \end{pmatrix} = \begin{pmatrix} a & b \\ b & c \end{pmatrix}.$$

Then

$$\begin{aligned} ac - b^2 = \det T'_q(\mu n) &= \frac{q^2\tilde{D} - n^2}{4Dq^2}, \\ \Delta &= -(a + Dc) - 2b\sqrt{D}, \\ a - Dc &= -\mu \frac{n}{D}. \end{aligned} \tag{6.14}$$

Lemma 6.3 implies that

$$\beta_q(T_q(\mu n), \Psi_q) = \beta_q(T'_q(\mu n), \Psi'_q). \tag{6.15}$$

Proposition 6.7. *When $q \nmid n$, one has*

$$\beta_q(T_q(\mu n), \Psi_q) = 1.$$

*Proof.* When $q \nmid n$, (6.14) implies that $a, c \in \frac{1}{q}\mathbb{Z}_q^*$, and so

$$T'_q(\mu n) = \begin{pmatrix} 1 & 0 \\ a^{-1}b & 1 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & \tilde{a} \end{pmatrix} \begin{pmatrix} 1 & a^{-1}b \\ 0 & 1 \end{pmatrix}$$

with $\tilde{a} = \frac{1}{q} \det T'_q(\mu n) \in \frac{1}{q}\mathbb{Z}_q^*$. Since $b \in \mathbb{Z}_q$, $\begin{pmatrix} 1 & 0 \\ a^{-1}b & 1 \end{pmatrix} \in K_0(q)$, and $\Psi'_q$ is $K_0(q)$-invariant (with respect to the linear action), one has

$$\beta_q(T'_q(\mu n), \Psi'_q) = \beta_q(\mathrm{diag}(a, \tilde{a}), \Psi'_q).$$

Since

$$-\frac{\tilde{a}}{a} = -\frac{\det T'_q(\mu n)}{a^2} = \frac{n^2 - q^2\tilde{D}}{4D(qa)^2} \equiv \frac{n^2}{4D(qa)^2} \mod q$$

there is $z_0 \in \mathbb{Z}_q^*$ with $z_0^2 = -\frac{\tilde{a}}{a}$. Set $\vec{x}_0 = {}^t(X_1, X_2) \in (L'_q)^2$ with

$$X_1 = \left(\begin{smallmatrix} 0 & -a \\ 1 & 0 \end{smallmatrix}\right), \quad X_2 = \left(\begin{smallmatrix} 0 & az_0 \\ z_0 & 0 \end{smallmatrix}\right).$$

Then $T(\vec{x}_0) = \operatorname{diag}(a, \tilde{a})$. It is easy to check that $h(r,u)^{-1}.\vec{x}_0 \in (L'_q)^2$ if and only if $r = 0$ and $u \in \mathbb{Z}_q$, i.e., $h(r,u) = 1 \mod K_0(q)$. In this case, $\vec{x}_0 \in \Omega'_q$ if and only if $1 + z_0\sqrt{D} = 0 \mod q$.

On the other hand, it is easy to check $h'(r,u)^{-1}.\vec{x}_0 \in (L'_q)^2$ if and only if $r = -1$ and $u \in \mathbb{Z}_q$, i.e., $h(r,u) = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) \mod K_0(q)$. In this case, $h'(-1,0)^{-1}.\vec{x}_0 \in \Omega'_q$ if and only if $1 - z_0\sqrt{D} \equiv 0 \mod q$.

Since

$$1 - z_0^2 D = 1 + \frac{\tilde{a}}{a}D = \frac{q(qa)(a + Dc) - q^2b^2}{(qa)^2} \equiv 0 \mod q,$$

exactly one of the following holds: $1 + z_0\sqrt{D} = 0 \mod q$ or $1 - z_0\sqrt{D} \equiv 0 \mod q$. So there is exactly one coset $\mathbb{Q}_q^* h K_0(q)$ such that $h^{-1}.\vec{x}_0 \in \Omega'_q$. This proves $\beta_q(\operatorname{diag}(a, \tilde{a}), \Psi'_q) = 1$, and thus the lemma. □

Next, we assume that $q|n$. In this case $T'_q(\mu n) \in \operatorname{Sym}_2(\mathbb{Z}_q)$. Actually, $T_q(\mu n) = T(\mu\frac{n}{q})$ in the notation of [Ya4]. So there is $g = \left(\begin{smallmatrix} g_1 & g_2 \\ g_3 & g_4 \end{smallmatrix}\right) \in \operatorname{SL}_2(\mathbb{Z}_q)$ such that

$$(6.16) \qquad T'_q(\mu n) = gT{}^tg, \quad T = \operatorname{diag}(\epsilon_1, \epsilon_2 q^t)$$

with $\epsilon_i \in \mathbb{Z}_q^*$, and $t = \operatorname{ord}_q \det T'_q(\mu n) = \operatorname{ord}_q \frac{q^2\tilde{D} - n^2}{4Dq^2}$.

For $v_1, v_2 \in \mathbb{Z}/q\mathbb{Z}$, we set

$$(6.17) \qquad \begin{aligned} \Omega_{v_1,v_2} &= \{\vec{x} = {}^t(X_1, X_2) \in L_q^2 : \ v_1z_1 + v_2z_2 = 0 \mod q\} \\ &= \{\vec{x} = {}^t(X_1, X_2) \in L_q^2 : \ v_1X_1 + v_2X_2 \in L_0(q)\} \end{aligned}$$

where $L_q = M_2(\mathbb{Z}_q)$ and

$$(6.18) \qquad L_0(q) = \{X = \{\left(\begin{smallmatrix} x & y \\ qz & -x \end{smallmatrix}\right) \in V_q : \ x, y, z \in \mathbb{Z}_q\}.$$

Let

$$(6.19) \qquad \Psi_{v_1,v_2} = \operatorname{char}(\Omega_{v_1,v_2}), \quad \Psi_0 = \operatorname{char}(L_0(q)^2).$$

Lemma 6.8. *Let $T'_q(\mu n) = gT{}^tg$ be as in (6.16), and let*

$$\left(\begin{smallmatrix} v_1 & v_2 \\ v_3 & v_4 \end{smallmatrix}\right) = \begin{pmatrix} g_1 + g_3\sqrt{D} & g_2 + g_4\sqrt{D} \\ g_1 - g_3\sqrt{D} & g_2 - g_4\sqrt{D} \end{pmatrix} = \begin{pmatrix} 1 & \sqrt{D} \\ 1 & -\sqrt{D} \end{pmatrix} \left(\begin{smallmatrix} g_1 & g_2 \\ g_3 & g_4 \end{smallmatrix}\right).$$

*Then*

$$\beta_q(T'_q(\mu n), \Psi'_q) = \beta_q(T, \Psi_{v_1,v_2}) + \beta_q(T, \Psi_{v_3,-v_4}) - \beta_q(T, \Psi_0).$$

*Proof.* Lemma 6.3 implies that

$$\beta_q(T'_q(\mu n), \Psi'_q) = \beta_q(T, f)$$

with $f(\vec{x}) = \Psi'_q(g\vec{x})$. So $f(\vec{x}) \neq 0$ if and only if $g\vec{x} \in \Omega'_q$, i.e., $\vec{x} = {}^t(X_1, X_2) \in (L'_q)^2$ with $X_i = \left(\begin{smallmatrix} x_i & \frac{1}{q}y_i \\ z_i & -x_i \end{smallmatrix}\right)$ and

$$v_1 z_1 + v_2 z_2 \equiv 0 \mod q, \tag{6.20}$$

$$v_3 y_1 - v_3 y_2 \equiv 0 \mod q. \tag{6.21}$$

Since $T \in \mathrm{Sym}_2(\mathbb{Z}_q)$, to have $T(\vec{x}) = T$ for $\vec{x} \in (L'_q)^2$, one has to have

$$y_1 z_1, y_2 z_2, y_1 z_2 + y_2 z_1 \in q\mathbb{Z}_q$$

and so either $y_1, y_2 \equiv 0 \mod q$, i.e., $\vec{x} \in L_q^2$, or $z_1, z_2 \equiv 0 \mod q$, i.e., $\left(\begin{smallmatrix} 0 & q^{-1} \\ 1 & 0 \end{smallmatrix}\right).\vec{x} \in L_q^2$.

When $y_1, y_2 \equiv 0 \mod q$, (6.20) is automatic and thus $g\vec{x} \in \Omega'_q$ if $\vec{x} \in \Omega_{v_1,v_2}$. When $z_1, z_2 \equiv 0 \mod q$, (6.21) is automatic, and $g\vec{x} \in \Omega'_q$ if and only if $\vec{x} \in \left(\begin{smallmatrix} 0 & 1 \\ q & 0 \end{smallmatrix}\right).\Omega_{v_3,-v_4}$. When $y_1, y_2, z_1, z_2 \equiv 0 \mod 4$, $g\vec{x} \in \Omega'_q$ automatically and $\vec{x} \in L_0(q)^2$. So we have

$$\begin{aligned}\beta_q(T'_q(\mu n), \Psi'_q) &= \beta_q(T, \Psi_{v_1,v_2}) + \beta_q(T, \mathrm{char}\left(\left(\begin{smallmatrix} 0 & 1 \\ q & 0 \end{smallmatrix}\right).\Omega_{v_3,-v_4}\right)) - \beta_q(T, \Psi_0) \\ &= \beta_q(T, \Psi_{v_1,v_2}) + \beta_q(T, \Psi_{v_3,-v_4}) - \beta_q(T, \Psi_0)\end{aligned}$$

as claimed. □

As in Section 5.2, there exists $\vec{x} = {}^t(X_1, X_2) \in V_q^2$ with $T(\vec{x}) = T$ if and only if $(-\epsilon_1, q)_q^t = 1$. Choose $\vec{x}_0 = {}^t(X_1, X_2)$ as in (6.8) (with $l$ replaced by $q$). The following lemma is contained in the proof of Proposition 6.5.

LEMMA 6.9. *(1) When $(-\epsilon_1, q)_q = -1$ and $t$ is even,*

$$h(r,u)^{-1}.\vec{x}_0 \in L_q^2 \Leftrightarrow h'(r,u)^{-1}.\vec{x}_0 \in L_q^2 \Leftrightarrow r = 0, u \in \mathbb{Z}_q.$$

*(2) When $(-\epsilon_1, q)_q = 1$,*

$$h(r,u)^{-1}.\vec{x}_0 \in L_q^2 \Leftrightarrow h'(r,u)^{-1}.\vec{x}_0 \in L_q^2 \Leftrightarrow 0 \le r \le t, u = -\frac{y_0}{x_0} \mod q^r.$$

We first consider a special case $t = 0$ which is different from the case $t > 0$.

LEMMA 6.10. *Let $v_1, v_2 \in \mathbb{Z}/q$ with at least one being nonzero. One has*

$$\beta_q(\mathrm{diag}(\epsilon_1, \epsilon_2), \Psi_{v_1,v_2}) = \begin{cases} 2 & \text{if } -(\epsilon_1 v_1^2 + \epsilon_2 v_2^2) \equiv \square \mod q, \\ 0 & \text{otherwise.} \end{cases}$$

*Proof.* By the above lemma, we only need to check whether $\vec{x}_0$ and $h'(0,u).\vec{x}_0$ belong to $\Omega_{v_1,v_2}$ with $u \in \mathbb{Z}/q$. $\vec{x}_0 \in \Omega_{v_1,v_2}$ if and only if $v_1 - v_2 y_0 \equiv 0 \mod q$. Since

$$h'(0,u)^{-1}.X_1 = \begin{pmatrix} -\epsilon_1 u & -\epsilon_1 \\ 1 + \epsilon_1 u^2 & \epsilon_1 u \end{pmatrix},$$

$$h'(0,u)^{-1}.X_2 = \begin{pmatrix} -x_0 + \epsilon_1 y_0 u & \epsilon_1 y_0 \\ y_0 + 2x_0 u - \epsilon_1 y_0 u^2 & x_0 - \epsilon_1 y_0 u \end{pmatrix},$$

$h'(0,u)^{-1}.\vec{x}_0 \in \Omega_{v_1,v_2}$ if and only if

$$\epsilon_1(v_1 - v_2y_0)u^2 + 2x_0v_2u + (v_1 + v_2y_0) \equiv 0 \mod q. \tag{6.22}$$

When $v_1 - v_2y_0 \equiv 0 \mod q$, $v_2 \not\equiv 0 \mod q$, and thus (6.22) has one solution $\mod q$. When $v_1 - v_2y_0 \not\equiv 0 \mod q$, (6.22) has either two or zero solutions mod $q$ depending on whether its discriminant

$$(2x_0v_2)^2 - 4\epsilon_0(v_1 - v_2y_0)(v_1 + v_2y_0) = -4(\epsilon_1v_1^2 + \epsilon_2v_2^2)$$

is a square or not mod $q$ (recall $x_0^2 + \epsilon_1y_0^2 = -\epsilon q^t$). Notice that when $v_1 - v_2y_0 \equiv 0$ mod $q$, $-(\epsilon_1v_1^2 + \epsilon_2v_2^2) = x_0^2v_2^2$ is a square. This proves the lemma. □

Proposition 6.11. *When $q|n$ and $\det T_q(\mu) = \frac{q^2\tilde{D}-n^2}{Dq^2} \in \mathbb{Z}_q^*$, one has*

$$\beta_q(T_q(\mu n), \Psi_q) = \begin{cases} 4 & \text{if } q \text{ split completely in } \tilde{K}, \\ 2 & \text{if } q \text{ inert in } \tilde{F}, q\mathcal{O}_{\tilde{F}} \text{ split in } \tilde{K}, \\ 0 & \text{otherwise.} \end{cases}$$

*Proof.* Write $T_q'(\mu n) = gT{}^tg$ with $g \in \mathrm{GL}_2(\mathbb{Z}_q)$ and $T = \mathrm{diag}(1, \epsilon)$, $\epsilon = \det T_q'(\mu n) = \frac{q^2\tilde{D}-n^2}{4Dq^2} \in \mathbb{Z}_q^*$ as above. Then

$$g_1^2 + g_2^2\epsilon = a, \quad g_1g_3 + g_2g_4\epsilon = b, \quad g_3^2 + g_4^2\epsilon = c.$$

So Lemmas 6.8 and (6.14) imply

$$v_1^2 + \epsilon v_2^2 = (g_1 + g_3\sqrt{D})^2 + \epsilon(g_2 + g_4\sqrt{D})^2 = a + Dc + 2b\sqrt{D} = -\Delta$$

and

$$v_3^2 + \epsilon v_4^2 = -\Delta'.$$

Now applying Lemma 6.10, one obtains

$$\beta_q(T, \Psi_{v_1,v_2}) = \begin{cases} 2 & \text{if } \Delta \in (\mathbb{Z}_q^*)^2, \\ 0 & \text{if } \Delta \notin (\mathbb{Z}_q^*)^2, \end{cases}$$

and

$$\beta_q(T, \Psi_{v_3,-v_4}) = \begin{cases} 2 & \text{if } \Delta' \in (\mathbb{Z}_q^*)^2, \\ 0 & \text{if } \Delta' \notin (\mathbb{Z}_q^*)^2, \end{cases}$$

Since $\epsilon_i \in \mathbb{Z}_q^*$, it is easy to see that $\beta_q(T, \Psi_0) = 0$. So Lemma 6.8 and (6.15) imply

$$\beta_q(T_q(\mu n), \Psi_q) = \begin{cases} 4 & \text{if } \Delta, \Delta' \in (\mathbb{Z}_q^*)^2, \\ 2 & \text{if exactly one of } \Delta \text{ or } \Delta' \in (\mathbb{Z}_q^*)^2, \\ 0 & \text{otherwise.} \end{cases}$$

Recall that $q = \mathfrak{q}\mathfrak{q}'$ is split in $F$, and under the identification $F \hookrightarrow F_{\mathfrak{q}} \cong \mathbb{Q}_q$, $\sqrt{D}$ goes to $\sqrt{D}$. So $\Delta \in (\mathbb{Z}_q^*)^2$ if and only if $\mathfrak{q}$ splits in $K$. $\Delta' \in (\mathbb{Z}_q^*)^2$ if and only if $\mathfrak{q}'$ splits in $K$.

Consider the diagram of fields:

$$\begin{tikzcd}[column sep=small]
 & & M \arrow[dll, dash] \arrow[drr, dash] & & \\
K \arrow[dr, dash] & & & & \tilde{K} \arrow[dl, dash] \\
 & F \arrow[dr, dash] & & \tilde{F} \arrow[dl, dash] & \\
 & & \mathbb{Q} & &
\end{tikzcd}$$

When $q = \tilde{\mathfrak{q}}\tilde{\mathfrak{q}}'$ is split in $\tilde{F}$, $(\Delta\Delta', q)_q = (\tilde{D}, q)_q = 1$. So either $q$ splits completely in $K$ and thus in $M = K\tilde{K}$ or both $\mathfrak{q}$ and $\mathfrak{q}'$ are inert in $K$. Similarly, since $q$ is split in $F$, either $q$ splits completely in $\tilde{K}$ and thus in $M$ or both $\tilde{\mathfrak{q}}$ and $\tilde{\mathfrak{q}}'$ are inert in $\tilde{K}$. Therefore, under the condition that $q$ is split in $\tilde{F}$, we have

$$\beta_q(T_q(\mu n), \Psi_q) = \begin{cases} 4 & \text{if } q \text{ split completely in } \tilde{K}, \\ 0 & \text{otherwise.} \end{cases}$$

When $q$ is inert in $\tilde{F}$, $(\Delta\Delta', q)_q = (\tilde{D}, q)_q = -1$, exactly one of $\Delta$ or $\Delta'$ is a square in $\mathbb{Z}_q^*$. This implies that there are at least three primes of $M$ above $q$, and thus that $q\mathcal{O}_{\tilde{F}}$ has to be split in $\tilde{K}$. This finishes the proof of the proposition. □

Finally we consider the case $t \geq 1$ and prove

Proposition 6.12. *Assume that $q|n$ and $t_q = \operatorname{ord}_q \frac{q^2\tilde{D}-n^2}{4Dq^2} > 0$, and let $T_q(\mu n)$ is $\mathbb{Z}_q$-equivalent to $\operatorname{diag}(\alpha_q, \alpha_q^{-1}\det T_q(\mu n))$ with $\alpha_q \in \mathbb{Z}_q^*$. Then*

$$\beta_q(T_q(\mu n), \Psi_q) = \begin{cases} 0 & \text{if } (-\alpha_q, q)_q = -1, \\ 2(t_q+2) & \text{if } (-\alpha_q, q)_q = 1. \end{cases}$$

*Proof.* Since $T_q'(\mu n)$ is $\mathbb{Z}_q$-equivalent to $T_q(\mu n)$, it is also $\mathbb{Z}_q$ equivalent to $\operatorname{diag}(\alpha_q, \alpha_q^{-1}\det T_q(\mu n))$, which we now shorten as $T = \operatorname{diag}(\epsilon_1, \epsilon_2 q^t)$ with $\epsilon_1 = \alpha_q, \epsilon_2 \in \mathbb{Z}_q^*$ and $t = t_q$. As in the proof of Proposition 6.11, we write $T_q'(\mu n) = gT^tg$ so that

$$\beta_q(T_q'(\mu n), \Psi_q') = \beta_q(T, \Psi_{v_1,v_2}) + \beta_q(T, \Psi_{v_3,-v_4}) - \beta_q(T, \Psi_0).$$

Here $v_i$ are given as in Lemma 6.9.

**Case 1:** We first assume that $(-\epsilon_1, q)_q = -1$, so $t = 2t_0$ is even. In this case $x_0, y_0 \in q^{t_0}\mathbb{Z}_q$ and thus $x_0, y_0 \equiv 0 \mod q$. In order to compute $\beta_q(T, \Psi_{v_1,v_2})$, we only need to consider whether $\vec{x}_0$ and $h'(0,u)^{-1}.\vec{x}_0$ belong to $\Omega_{v_1,v_2}$ by Lemma 6.8. It is easy to check as before that $\vec{x}_0 \in \Omega_{v_1,v_2}$ if and only if $v_1 - v_2 y_0 \equiv v_1 \equiv 0 \mod q$, and $h'(0,u)^{-1}.\vec{x}_0 \in \Omega_{v_1,v_2}$ if and only if

$$v_1(1+\epsilon_1 u^2) + v_2(y_0 + x_0 u - \epsilon_1 y_0 u^2) \equiv 0 \mod q$$

i.e., $v_1 \equiv 0 \mod q$. On the other hand, the same calculation as in the proof of Proposition 6.11 gives

$$-(\epsilon_1 v_1^2 + \epsilon_2 q^t v_2^2) = \Delta \not\equiv 0 \mod q$$

and thus $v_1 \not\equiv 0 \mod q$. So $\beta_q(T, \Psi_{v_1,v_2}) = 0$. For the same reason, $\beta_q(T, \Psi_{v_3,-v_4}) = 0$, and thus $\beta_q(T_q(\mu n), \Psi_q) = \beta_q(T_q'(\mu n), \Psi_q') = 0$.

**Case 2:** Now we assume $(-\epsilon_1, q)_q = 1$. By Lemma 6.8, we need to consider how many $h(r,u)^{-1}.\vec{x}_0$ and $h'(r,u)^{-1}.\vec{x}_0$ are in $\Omega_{v_1,v_2}$, with $0 \le r \le t$ and $u \equiv -\frac{y_0}{x_0} \mod q^r$. In the case $h(r,u)$ we count the number of $u \mod q^r$ classes, and in the case $h'(r,u)$ we count the number of $u \mod q^{r+1}$ classes.

When $r = 0$, the same argument as in the proof of Proposition 6.11 shows that there are two classes of $h$ among $h(0,u)$ and $h'(0,u)$ satisfying $h^{-1}.\vec{x}_0 \in L_{v_1,v_2}$, since $q$ splits completely in $\tilde{K}$. Indeed, let $n_1 = n/q \in \mathbb{Z}$. Then $t = t_q > 0$ means $q | \frac{\tilde{D}-n_1^2}{4D}$ and thus $q$ splits in $\tilde{F}$. Now [Ya4, Lemma 6.2] implies that one prime of $\tilde{F}$ above $q$ splits in $\tilde{K}$. Since $q$ is split in $F$, this implies that both primes of $\tilde{F}$ above $q$ split in $\tilde{K}$, i.e., $q$ splits completely in $\tilde{K}$.

When $r > 0$, $h(r,u)^{-1}.\vec{x}_0 \in \Omega_{v_1,v_2}$ automatically. On the other hand, the same calculation as in the proof of Lemma 6.10 shows that $h(r,u)^{-1}.\vec{x}_0 \in \Omega_{v_1,v_2}$ if and only if

$$\epsilon_1(v_1 - v_2y_0)u^2 + 2x_0v_2u + (v_1 + v_2y_0) \equiv 0 \mod q^{r+1}. \tag{6.23}$$

Since $u \equiv -\frac{y_0}{x_0} \mod q^r$, we write $u = -\frac{y_0}{x_0} + q^r\tilde{u}$. Now (6.23) becomes

$$\frac{2\epsilon_1 y_0 v_1}{x_0} q^r \tilde{u} + (v_1 - v_2y_0)\frac{-\epsilon_2 q^t}{x_0^2} \equiv 0 \mod q^{r+1}.$$

Since $\epsilon_1 v_1^2 + \epsilon_2 q^t \epsilon_2^2 = -\Delta \not\equiv 0 \mod q$, one has $v_1 \not\equiv 0 \mod q$. So the above equation has a unique solution $\tilde{u} \mod q$, and there is a unique $u \mod q^{r+1}$ for $1 \le r \le t$ such that $h'(r,u)^{-1}.\vec{x}_0 \in \Omega_{v_1,v_2}$. In summary, we have proved

$$\beta_q(T, \Psi_{v_1,v_2}) = 2t + 2.$$

For the same reason, $\beta_q(T, \Psi_{v_3,-v_4}) = 2t+2$. A similar argument gives $\beta_q(T, \Psi_0) = 2t$. Therefore,

$$\beta_q(T_q(\mu n), \Psi_q) = \beta_q(T, \Psi_{v_1,v_2}) + \beta_q(T, \Psi_{v_3,-v_4}) - \beta_q(T, \Psi_0) = 2t + 4.$$

□

## 7. Computing $b_m(p)$ and Proof of Theorem 1.8 .

In this section, we compute $b_m(p)$ assuming $(m, 2D\tilde{D}p) = 1$ and prove the following theorem. A little more work could remove the restriction. At the end of this section, we prove Theorem 1.8, which is clear after all these preparations.

THEOREM 7.1. *Assume (1.5) and that $\tilde{D} = \Delta\Delta' \equiv 1 \mod 4$ is square free, and that $m > 0$ is square-free with $(m, 2D\tilde{D}p) = 1$. Let $t_l = \mathrm{ord}_l \frac{m^2\tilde{D}-n^2}{4Dm^2}$. Then*

$$b_m(p) = \sum_{\substack{0<n<m\sqrt{\tilde{D}} \\ \frac{m^2\tilde{D}-n^2}{4D} \in p\mathbb{Z}_{>0}}} (\mathrm{ord}_p \frac{m^2\tilde{D}-n^2}{4D} + 1) \sum_{\mu} b(p, \mu n, m) \tag{7.1}$$

*where*

$$b(p, \mu n, m) = \prod_{l | \frac{m^2\tilde{D}-n^2}{4D}} b_l(p, \mu n, m) \tag{7.2}$$

*is given as follows.*

*(1) When $l \nmid m$ and $l | \frac{m^2\tilde{D}-n^2}{4D}$, $T_m(\mu n)$ is $\mathbb{Z}_l$-equivalent to* $\operatorname{diag}(\alpha_l, \alpha_l^{-1}\det T_m(\mu n))$ *with $\alpha_l \in \mathbb{Z}_l^*$, and*

$$b_l(p, \mu n, m) = \begin{cases} \frac{1-(-\alpha_p,p)_p^{t_p}}{2} & \text{if } l = p, \\ t_l + 1 & \text{if } l \nmid mp, (-\alpha_l, l)_l = 1, \\ \frac{1+(-1)^{t_l}}{2} & \text{if } l \nmid mp, (-\alpha_l, l)_l = -1. \end{cases} \tag{7.3}$$

*(2) When $l|m$, and $t_l = 0$, one has*

$$b_l(p, \mu n, m) = \begin{cases} 4 & \text{if } l \text{ split completely in } M, \\ 2 & \text{if } l \text{ inert in } \mathcal{O}_{\tilde{F}}, l\mathcal{O}_{\tilde{F}} \text{ split in } \tilde{K}, \\ 0 & \text{otherwise.} \end{cases} \tag{7.4}$$

*Here $M = K\tilde{K}$ is the Galois closure of $K$ (and $\tilde{K}$) over $\mathbb{Q}$.*

*(3) When $l|m$ is split in $F$ and $t_l > 0$, $T_m(\mu n)$ is $\mathbb{Z}_l$-equivalent to* $\operatorname{diag}(\alpha_l, \alpha_l^{-1}\det T_m(\mu n))$ *with $\alpha_l \in \mathbb{Z}_l^*$, and*

$$b_l(p, \mu n, m) = \begin{cases} 0 & \text{if } (-\alpha_l, l)_l = -1, \\ 2(t_l + 2) & \text{if } (-\alpha_l, l)_l = 1. \end{cases} \tag{7.5}$$

*(4) When $l|m$ is inert in $F$ and $t_l > 0$, $T_m(\mu n)$ is $\mathbb{Z}_l$-equivalent to* $\operatorname{diag}(\alpha_l, \alpha_l^{-1}\det T_m(\mu n))$ *with $\alpha_l \in \mathbb{Z}_l^*$, and*

$$b_l(p, \mu n, m) = \begin{cases} 1 - (-1)^{t_l} & \text{if } (-\alpha_l, l)_l = -1, \\ 0 & \text{if } (-\alpha_l, l)_l = 1. \end{cases} \tag{7.6}$$

*Proof.* Recall

$$b_m(p) = \sum_{\mathfrak{p}|p} \sum_{\substack{0<n<m\sqrt{\tilde{D}} \\ \frac{m^2\tilde{D}-n^2}{4D} \in p\mathbb{Z}_{>0}}} \sum_{\mu} \rho(t_n d_{\tilde{K}/\tilde{F}} \mathfrak{p}^{-1}), \tag{7.7}$$

with ($\mu = \pm 1$)

$$t_{\mu n} = \frac{\mu n + m\sqrt{\tilde{D}}}{2D} \in d_{\tilde{K}/\tilde{F}}^{-1}.$$

Clearly, $b_m(p) = 0$ unless there is an integer $0 < n < m\sqrt{\tilde{D}}$ such that $\frac{m^2\tilde{D}-n^2}{4D} \in p\mathbb{Z}_{>0}$. Fix such an integer $n$ and recall $T_m(\mu n)$ from Lemma 4.1.

The condition $\frac{m^2\tilde{D}-n^2}{4D} \in p\mathbb{Z}_{>0}$ implies that either $p$ is split in $\tilde{F}$ or $p|\gcd(D, n)$ is ramified in $\tilde{F}$. In the ramified case, we have $p\mathcal{O}_{\tilde{F}} = \mathfrak{p}^2$. In the split case, we choose the splitting $p\mathcal{O}_{\tilde{F}} = \mathfrak{p}\mathfrak{p}'$ so that

$$t_{\mu n} = \frac{\mu n + m\sqrt{\tilde{D}}}{2D} \in \mathfrak{p} d_{\tilde{K}/\tilde{F}}^{-1} \tag{7.8}$$

satisfies

$$\operatorname{ord}_{\mathfrak{p}} t_{\mu n} = \operatorname{ord}_p \frac{m^2\tilde{D} - n^2}{4D}, \quad \operatorname{ord}_{\mathfrak{p}'}(t_{\mu n}) = 0 \text{ or } -1. \tag{7.9}$$

With this notation, we have by definition

$$b_m(p) = \sum_{\substack{0<n<m\sqrt{\tilde{D}} \\ \frac{m^2\tilde{D}-n^2}{4D} \in p\mathbb{Z}_{>0}}} (\mathrm{ord}_p \frac{m^2\tilde{D}-n^2}{4D} + 1) \sum_{\mu} b(p, \mu n, m) \tag{7.10}$$

where

$$b(p, \mu n, m) = \begin{cases} 0 & \text{if } \mathfrak{p} \text{ is split in } \tilde{K}, \\ \rho(t_{\mu n} d_{\tilde{K}/\tilde{F}} \mathfrak{p}^{-1}) & \text{if } \mathfrak{p} \text{ is not split in } \tilde{K}. \end{cases} \tag{7.11}$$

Assume now that $\mathfrak{p}$ is not split in $\tilde{K}$. Notice that

$$\rho(t_{\mu n} d_{\tilde{K}/\tilde{F}} \mathfrak{p}^{-1}) = \prod_{\mathfrak{l}} \rho_{\mathfrak{l}}(t_{\mu n} d_{\tilde{K}/\tilde{F}} \mathfrak{p}^{-1})$$

where the product runs over all prime ideals $\mathfrak{l}$ of $\tilde{F}$, and

$$\rho_{\mathfrak{l}}(t_{\mu n} d_{\tilde{K}/\tilde{F}} \mathfrak{p}^{-1}) = \begin{cases} 1 & \text{if } \mathfrak{l} \text{ is ramified in } \tilde{K}, \\ \frac{1+(-1)^{\mathrm{ord}_{\mathfrak{l}}(t_{\mu n} d_{\tilde{K}/\tilde{F}} \mathfrak{p}^{-1})}}{2} & \text{if } \mathfrak{l} \text{ is inert in } \tilde{K}, \\ 1 + \mathrm{ord}_{\mathfrak{l}}(t_{\mu n} d_{\tilde{K}/\tilde{F}} \mathfrak{p}^{-1}) & \text{if } \mathfrak{l} \text{ is split in } \tilde{K}. \end{cases} \tag{7.12}$$

We write (assuming that $\mathfrak{p}$ is not split in $\tilde{F}$)

$$b(p, \mu n, m) = \prod_{l} b_l(p, \mu n, m) \tag{7.13}$$

with

$$b_l(b, \mu n, m) = \prod_{\mathfrak{l}|l} \rho_{\mathfrak{l}}(t_{\mu n} d_{\tilde{K}/\tilde{F}} \mathfrak{p}^{-1}). \tag{7.14}$$

Clearly $b_l(b, \mu n, m) = 1$ if $l \nmid \frac{m^2\tilde{D}-n^2}{4Dp}$. When $l | \frac{m^2\tilde{D}-n^2}{4Dp}$, there are three cases:

(a) $l|m$,

(b) $l \nmid m$ and $l|\gcd(\tilde{D}, n)$ is ramified in $\tilde{F}$, or

(c) $l \nmid m$, and $l\mathcal{O}_{\tilde{F}} = \mathfrak{l}\mathfrak{l}'$ is split in $\tilde{F}$.

In case (c), we choose the ideal $\mathfrak{l}$ so that

$$\begin{aligned} \mathrm{ord}_{\mathfrak{l}}(t_{\mu n} d_{\tilde{K}/\tilde{F}} \mathfrak{p}^{-1}) = \mathrm{ord}_l \frac{m^2\tilde{D}-n^2}{4Dp} &= \mathrm{ord}_l \, \mathrm{ord}_l \frac{m^2\tilde{D}-n^2}{4Dpm^2}, \\ \mathrm{ord}_{\mathfrak{l}'}(t_{\mu n} d_{\tilde{K}/\tilde{F}} \mathfrak{p}^{-1}) &= 0. \end{aligned} \tag{7.15}$$

Since $m$ does not affect local calculation in cases (b) and (c), the same proof as in [Ya4, Lemma 6.2] gives

Lemma 7.2. *Let the notation be as above. Assume $l|\frac{m^2\tilde{D}-n^2}{4D}$, $l \nmid m$ and $\mathfrak{l} \neq d_{\tilde{K}/\tilde{F}}$. Then $T_m(\mu n)$ is $\mathrm{GL}_2(\mathbb{Z}_l)$-equivalent to $\mathrm{diag}(\alpha_l, \alpha_l^{-1} T_m(\mu n))$ with $\alpha_l \in \mathbb{Z}_l^*$. Moreover, $\tilde{K}/\tilde{F}$ is split (inert) at $\mathfrak{l}$ if and only if $(-\alpha_l, l)_l = 1$ (resp. $-1$).*

Proposition 7.3. *One has always*

$$b(p,\mu n,m)=\prod_{l\mid\frac{m^2\tilde{D}-n^2}{4D}} b_l(p,\mu n,m)$$

*with*

$$b_l(p,\mu n,m)=\begin{cases}\frac{1-(-\alpha_p,p)_p^{t_p}}{2} & \text{if } l=p,\\ t_l+1 & \text{if } l\nmid mp, (-\alpha_l,l)_l=1,\\ \frac{1+(-1)^{t_l}}{2} & \text{if } l\nmid mp, (-\alpha_l,l)_l=-1.\end{cases}$$

*Here $T_m(\mu n)$ is $\mathrm{GL}_2(\mathbb{Z}_l)$-equivalent to $\mathrm{diag}(\alpha_l,\alpha_l^{-1}\det T_m(\mu n))$ with $\alpha_l\in\mathbb{Z}_l^*$, and $t_l=\mathrm{ord}_l\,T_m(\mu n)=\mathrm{ord}_l\,\frac{m^2\tilde{D}-n^2}{4Dm^2}$.*

*Proof.* First notice that the formula is true even when $\mathfrak{p}$ is split in $\tilde{K}$. Indeed,

$$b_p(p,\mu n,m)=\frac{1-(-\alpha_p,p)_p^{t_p}}{2}=0$$

since $(-\alpha_p,p)_p=1$ by Lemma 7.2. When $\mathfrak{p}$ is non-split in $\tilde{K}$, the formulae follows from Lemma 7.2 and (7.12)-(7.15). □

*Proof of Theorem 7.1 (cont.).* Proposition 7.3 settles Formulae (7.1), (7.2) and Case (1) in the theorem. Now we assume $l|m$ and $l|\frac{m^2\tilde{D}-n^2}{4D}$. This implies $l|n$. In this case we have

$$T_m(\mu n)=lT_{\frac{m}{l}}(\mu\frac{n}{l}). \tag{7.16}$$

Write $m_1=\frac{m}{l}$ and $n_1=\frac{n}{l}$.

(2) Now we deal with case (2): i.e., $l|m$ and $t_l=\frac{m^2\tilde{D}-n^2}{4Dm^2}=\mathrm{ord}_l\,\frac{m_1^2\tilde{D}-n_1^2}{4D}=0$.

**Case 1:** If $l$ is inert in $\tilde{F}$, then $\mathrm{ord}_l\,t_{\mu n}=1$. So

$$b_l(p,\mu n,m)=\begin{cases}2 & \text{if } l\mathcal{O}_{\tilde{F}} \text{ is split in } \tilde{K},\\ 0 & \text{if } l\mathcal{O}_{\tilde{F}} \text{ is inert in } \tilde{K}.\end{cases}$$

**Case 2:** If $l=\mathfrak{l}\mathfrak{l}'$ is split in $\tilde{F}$, then $\mathrm{ord}_{\mathfrak{l}}\,t_{\mu n}=\mathrm{ord}_{\mathfrak{l}'}\,t_{\mu n}=1$, and so

$$b_l(p,\mu n,m)=\begin{cases}4 & \text{if } l \text{ split completely in } \tilde{K},\\ 0 & \text{otherwise.}\end{cases}$$

On the other hand, $\Delta\Delta'=Dv^2$ for some integer $v\neq0$. So $l$ is split completely in $\tilde{K}$ implies that $(D,l)_l=1$, i.e., $l$ is split in $F$ too, and thus $l$ is split completely in $M$. This proves (2)

(3) Now we assume $l|m$, $t_l>0$ and that $l$ is split in $F$. in this case, $l|\frac{m_1^2\tilde{D}-n_1^2}{4D}$. Since $(m,2D\tilde{D}p)=1$, $l=\mathfrak{l}\mathfrak{l}'$ is split in $\tilde{F}$. Choose the splitting in $\tilde{F}$ so that

$$\mathrm{ord}_{\mathfrak{l}}\,t_{\mu n}=t_l+1,\quad \mathrm{ord}_{\mathfrak{l}'}\,t_{\mu n}=1. \tag{7.17}$$

Since $l$ is split in $F$, $(D,l)_l = 1$. So $\tilde{\Delta}\tilde{\Delta}' = Dv^2$ implies that either both $\mathfrak{l}$ and $\mathfrak{l}'$ are inert in $\tilde{K}$ or both are split in $\tilde{K}$. So

$$b_l(p,\mu n,m) = \begin{cases} 2(t_l+2) & \text{if } l \text{ split completely in } \tilde{K}, \\ 0 & \text{otherwise.} \end{cases} \tag{7.18}$$

Since $t_l > 0$, applying Lemma 7.2 to the pair $(m_1, n_1)$, we see that $\tilde{K}/\tilde{F}$ is split at $\mathfrak{l}$ if and only if $(-\alpha_l, l)_l = 1$. So we have

$$b_l(p,\mu n,m) = \begin{cases} 0 & \text{if } (-\alpha_l,l)_l = -1, \\ 2(t_l+2) & \text{if } (-\alpha_l,l)_l = 1 \end{cases} \tag{7.19}$$

as claimed.

(4) Finally, we assume $l|m$, $t_l > 0$, and $l$ is inert in $F$. Just as in (3), $l = \mathfrak{l}\mathfrak{l}'$ is split in $\tilde{F}$ and we can again choose the splitting as in (7.17). Since $(D,l)_l = -1$, $\tilde{\Delta}\tilde{\Delta}' = Dv^2$ implies that exactly one of $\mathfrak{l}$ and $\mathfrak{l}'$ is split in $\tilde{K}$, and the other one is inert in $\tilde{K}$. So

$$b_l(p,\mu n,m) = \begin{cases} 0 & \text{if } \mathfrak{l} \text{ is split in } \tilde{K}, \\ 1-(-1)^{t_l} & \text{if } \mathfrak{l} \text{ is inert in } \tilde{K}. \end{cases} \tag{7.20}$$

Applying Lemma 7.2 to $(m_1, n_1)$ again, we obtain (4). This finishes the proof of Theorem 7.1. □

*Proof of Theorem 1.8.* By Theorems 4.5 and 5.1, one has for $p \neq q$

$$(\mathcal{T}_q.\mathcal{CM}(K))_p = \frac{1}{2} \sum_{\substack{0<n<q\sqrt{\tilde{D}} \\ \frac{q^2\tilde{D}-n^2}{4D} \in p\mathbb{Z}_{>0}}} \left( \operatorname{ord}_p \frac{q^2\tilde{D}-n^2}{4D} + 1 \right) \sum_{\mu} \beta(p,\mu n)$$

where

$$\beta(p,\mu n) = \frac{1}{2} \prod_l \beta_l(T_q(\mu n), \Psi_l)$$

is computed in Section 6. By Theorems 6.1 and 6.2, one has $\beta_l(T_q(\mu n), \Psi_l) = 1$ for $l \nmid \frac{q^2\tilde{D}-n^2}{4D}$, and so

$$\beta(p,\mu n) = \frac{1}{2} \prod_{l | \frac{q^2\tilde{D}-n^2}{4D}} \beta_l(T_q(\mu n), \Psi_l)$$

Now comparing Theorems 6.1 and 6.2 with Theorem 7.1, one sees that for $l|\frac{q^2\tilde{D}-n^2}{4D}$ (recall $q$ is a prime split in $F$)

$$\beta_l(T_q(\mu n), \Psi_l) = \begin{cases} 2b_p(p,\mu n, q) & \text{if } l = p, \\ b_l(p,\mu n,q) & \text{if } l \neq p. \end{cases}$$

and thus

$$\beta(p,\mu n) = b(p,\mu n,q).$$

Now applying Theorem 7.1, one sees

$$(\mathcal{T}_q.\mathcal{CM}(K))_p = \frac{1}{2} b_q(p)$$

as claimed in Theorem 1.8.

**8. Faltings height and Proofs of Theorems 1.2, 1.3 and 1.4 .** Let $\tilde{\mathcal{M}}$ be a toroidal compactification of $\mathcal{M}$ and let $C = \tilde{\mathcal{M}} - \mathcal{M}$ be the boundary. We need the Faltings height pairing in a slightly more general setting as written in literature, i.e., on DM-stacks where Green functions have pre-log-log growth along the boundary $C$ in the sense of [BKK]. We restrict to our special case to avoid introducing more complicated concept 'pre-log-log Green object', and refer to [BKK] for detailed study in this subject, and to [BBK, Section 1] for a brief summary.

Let $N \ge 3$, and let $X$ be the moduli scheme over $\mathbb{C}$ of abelian surfaces with real multiplication by $\mathcal{O}_F$ and with full $N$-level structure [Pa], and let $\tilde{X}$ be a toroidal compactification of $X$. Then $M = \mathcal{M}(\mathbb{C}) = [\Gamma\backslash X]$ and $\tilde{M} = \tilde{\mathcal{M}}(\mathbb{C}) = [\Gamma\backslash\tilde{X}]$ are quotient stacks, where $\Gamma = \Gamma(N)\backslash \mathrm{SL}_2(\mathcal{O}_F)$. Let $\pi$ be the natural map from $\tilde{X}$ to $\tilde{M}$. Let $Z$ be a divisor of $\tilde{M}$, and let $Z_N = \pi^{-1}(Z)$ be its preimage in $\tilde{X}$. Following [KRY2, Chapter 2], the Dirac current $\delta_Z$ on $\tilde{M}$ is given by

$$\langle \delta_Z, f\rangle_{\tilde{M}} = \frac{1}{\#\Gamma}\langle \delta_{Z_N}, f\rangle_{\tilde{X}}$$

for every $C^\infty$ function on $\tilde{M}$ with compact support, which is defined as a $\Gamma$-invariant $C^\infty$ functions on $X$ with compact support. A pre-log-log Green function for $Z$ is defined to be a $\Gamma$-invariant pre-log-log Green function $g$ for $Z_N$, i.e., $g$ is $\Gamma$-invariant, has log singularity along $Z_N$ and pre-log-log growth along $C$ in the sense of [BKK], see also [BBK, Section 1] such that

$$dd^c g + \delta_{Z_N} = [\omega]_{\tilde{X}}$$

as currents for a $\Gamma$-invariant $C^\infty$ (log-log growth along with $C$ and $C^\infty$ everywhere else) $(1,1)$-form $\omega$. When viewed as currents on $\tilde{M}$, one has also

$$dd^c g + \delta_Z = [\omega]_{\tilde{M}}.$$

Let $\widehat{\mathrm{Z}}^1(\tilde{\mathcal{M}}, \mathcal{D}_{\mathrm{pre}})$ be the abelian group of the pairs $(\mathcal{Z}, g)$ where $\mathcal{Z}$ is a divisor of $\tilde{\mathcal{M}}$ and $g$ is a pre-log-log Green function for $Z = \mathcal{Z}(\mathbb{C})$. For a rational function $f$ on $\mathcal{M}$,

$$\widehat{\mathrm{div}}(f) = (\mathrm{div}\, f, -\log|f|^2) \in \widehat{\mathrm{Z}}^1(\tilde{\mathcal{M}}, \mathcal{D}_{\mathrm{pre}})$$

and let $\widehat{\mathrm{CH}}^1(\tilde{\mathcal{M}}, \mathcal{D}_{\mathrm{pre}})$ be the quotient group of $\widehat{\mathrm{Z}}^1(\tilde{\mathcal{M}}, \mathcal{D}_{\mathrm{pre}})$ by the subgroup generated by all $\widehat{\mathrm{div}}(f)$. Let $\mathcal{Z}$ be a prime cycle in $\mathcal{M}$ (not intersecting with the boundary $C$) of dimension 1, and let $j : \mathcal{Z} \to \tilde{\mathcal{M}}$ be the natural embedding. Then $j$ induces a natural map

$$j^* : \widehat{\mathrm{CH}}^1(\tilde{\mathcal{M}}, \mathcal{D}_{\mathrm{pre}})_{\mathbb{Q}} \to \widehat{\mathrm{CH}}^1(\mathcal{Z})_{\mathbb{Q}}, \tag{8.1}$$

which is given by

$$j^*(\mathcal{T}, g) = (j^*\mathcal{T}, j^*g), \quad j^*(g)(z) = g(j(z))$$

when $\mathcal{T}$ and $\mathcal{Z}$ intersect properly. Here for an abelian group $A$, we write $A_{\mathbb{Q}}$ for the $\mathbb{Q}$-vector space $A \otimes \mathbb{Q}$. Since $\mathcal{Z}(\mathbb{C})$ does not intersect with the boundary $C$, $j^*g$ well-defined over $\mathcal{Z}(\mathbb{C})$. Here arithmetic Chow group $\widehat{\mathrm{CH}}^1(\mathcal{Z})$ is defined the same way as above except that the Green function $g$ is $C^\infty$ (actually in special case, just constants at points of $\mathcal{Z}(\mathbb{C})$). In [KRY2, Chapter 2], it is shown that there is a linear map—the arithmetic degree

$$\widehat{\deg} : \widehat{\mathrm{CH}}^1(\mathcal{Z})_{\mathbb{Q}} \to \mathbb{R}, \quad \widehat{\deg}(\mathcal{T}, g) = \sum_p \sum_{z \in \mathcal{T}(\bar{\mathbb{F}}_p)} \frac{1}{\#\mathrm{Aut} z} i_p(\mathcal{T}, z) \log p + \frac{1}{2} \sum_{z \in \mathcal{Z}(\mathbb{C})} \frac{1}{\#\mathrm{Aut}(z)} g(z). \tag{8.2}$$

Here $i_p(\mathcal{T}) = \mathrm{Length}(\hat{\mathcal{O}}_{\mathcal{T},z})$ and $\hat{\mathcal{O}}_{\mathcal{T},z}$ is the strictly local henselian ring of $\mathcal{T}$ at $z$. This way, we obtain a bilinear map—the Faltings height function

$$h : \widehat{\mathrm{CH}}^1(\tilde{\mathcal{M}}, \mathcal{D}_{\mathrm{pre}})_{\mathbb{Q}} \times Z^2(\mathcal{M})_{\mathbb{Q}} \to \mathbb{R}, \quad (\hat{\mathcal{T}}, \mathcal{Z}) \mapsto h_{\hat{\mathcal{T}}}(\mathcal{Z}) = \widehat{\deg}(j^* \hat{\mathcal{T}}), \tag{8.3}$$

which is given by

$$h_{\hat{\mathcal{T}}}(\mathcal{Z}) = \mathcal{Z}.\mathcal{T} + \frac{1}{2} \sum_{z \in \mathcal{Z}(\mathbb{C})} \frac{1}{\#\mathrm{Aut}(z)} g(z) \tag{8.4}$$

when $\mathcal{Z}$ and $\mathcal{T}$ intersect properly.

Finally, if $\hat{\mathcal{L}} = (\mathcal{L}, \| \, \|)$ is a metrized line bundle on $\tilde{\mathcal{M}}$ with a pre-log growth metric along the boundary in the sense of [BBK, Section 1], let $s$ be a rational section of $\mathcal{L}$, and $\widehat{\mathrm{div}} s = (\mathrm{div}\, s, -\log \|s\|^2) \in \widehat{\mathrm{CH}}^1(\tilde{\mathcal{M}}, \mathcal{D}_{\mathrm{pre}})$ is independent of the choice of $s$, and is denoted by $\hat{c}_1(\hat{\mathcal{L}})$. Actually, it only depends on the equivalence class of $\hat{\mathcal{L}}$. We define the Faltings height of $\mathcal{Z}$ with respect to $\hat{\mathcal{L}}$ by

$$h_{\hat{\mathcal{L}}}(\mathcal{Z}) = h_{\widehat{\mathrm{div}} s}(\mathcal{Z}) \tag{8.5}$$

which depends only on the equivalence class of $\hat{\mathcal{L}}$.

Let $\tilde{\mathcal{T}}_m$ be the closure of the arithmetic Hirzebruch-Zagier divisor $\mathcal{T}_m$ in $\tilde{\mathcal{M}}$. It is also the flat closure of $\tilde{T}_m$ where $\tilde{T}_m$ is the closure of the classical Hirzebruch-Zagier divisor $T_m$ in $\tilde{\mathcal{M}}(\mathbb{C})$. Bruinier, Burgos-Gil, and Kühn defined in [BBK] a pre-log-log Green function $G_m$ for $\tilde{T}_m$ so that $\hat{\mathcal{T}}_m = (\tilde{\mathcal{T}}_m, G_m) \in \widehat{\mathrm{CH}}^1(\tilde{\mathcal{M}}, \mathcal{D}_{\mathrm{pre}})$.

Let $\omega$ be the Hodge bundle on $\tilde{\mathcal{M}}$. Then the rational sections of $\omega^k$ can be identified with meromorphic Hilbert modular forms for $\mathrm{SL}_2(\mathcal{O}_F)$ of weight $k$. We give it the following Petersson metric

$$\|F(z_1, z_2)\|_{\mathrm{Pet}} = |F(z_1, z_2)| \big(16\pi^2 y_1 y_2\big)^{k/2} \tag{8.6}$$

for a Hilbert modular form $F(z)$ of weight $k$. This gives a metrized Hodge bundle $\hat{\omega} = (\omega, \| \, \|_{\mathrm{Pet}})$. This metric is shown in [BBK, Section 2] to have pre-log growth along the boundary, and so $\hat{c}_1(\hat{\omega}) \in \widehat{\mathrm{CH}}^1(\tilde{\mathcal{M}}, \mathcal{D}_{\mathrm{pre}})$. It is proved in [Ya3, Corollary 2.4] that

$$h_{\hat{\omega}}(\mathcal{CM}(K)) = \frac{2\#\,\mathrm{CM}(K)}{W_K} h_{\mathrm{Fal}}(A) \tag{8.7}$$

for any CM abelian surface $(A, \iota, \lambda) \in \mathcal{CM}(K)(\mathbb{C})$. The following theorem is proved in [BBK].

THEOREM 8.1. *(1) The generating function*

$$\hat{\phi}(\tau) = -\frac{1}{2}\hat{c}_1(\hat{\omega}) + \sum_{m>0} \hat{\mathcal{T}}_m e(m\tau)$$

*is a modular form of weight* 2*, level* $D$*, and Nebentypus character* $(\frac{D}{})$ *with values in* $\widehat{\mathrm{CH}}^1(\tilde{\mathcal{M}}, \mathcal{D}_{\mathrm{pre}})_{\mathbb{Q}}$.

*(2) Let* $\mathcal{HZ}$ *be the subspace of* $\widehat{\mathrm{CH}}^1(\tilde{\mathcal{M}}, \mathcal{D}_{\mathrm{pre}})_{\mathbb{Q}}$ *generated by* $\hat{\mathcal{T}}_m$*. Then* $\mathcal{HZ}$ *is a finite dimensional vector space over* $\mathbb{Q}$.

*(3) Let* $S$ *be the set of primes split in* $F$*, and let* $S_0$ *be a finite subset of* $S$*. Then* $\mathcal{HZ}$ *is generated by* $\hat{\mathcal{T}}_q$ *with* $q \in S - S_0$.

*Proof of Theorem 1.2.* Now we are ready to prove the main result of this paper. We first show that Theorem 1.2 holds for a prime $q$ split in $F$, strengthening Theorem 1.8. By Theorem 8.1, there are non-zero integers $c, c_i$ and primes $q_i$ $(\neq q)$ split in $F$ such that

$$c\hat{\mathcal{T}}_q = \sum c_i \hat{\mathcal{T}}_{q_i}.$$

This means that there is a (normalized integral in the sense of [BY, Page 3]) meromorphic function $\Psi$ such that

$$\operatorname{div}\Psi = c\tilde{\mathcal{T}}_q - \sum c_i \tilde{\mathcal{T}}_{q_i}.$$

So one has by (8.4) and Lemma 3.1

$$\begin{aligned} 0 &= h_{\widehat{\operatorname{div}}(\Psi)}(\mathcal{CM}(K)) \\ &= c\mathcal{CM}(K).\tilde{\mathcal{T}}_q - \sum c_i \mathcal{CM}(K).\tilde{\mathcal{T}}_{q_i} - \frac{2}{W_K}\sum_{z\in \mathrm{CM}(K)} \log|\Psi(z)| \\ &= c\mathcal{CM}(K).\mathcal{T}_q - \sum c_i \mathcal{CM}(K).\mathcal{T}_{q_i} - \frac{2}{W_K}\sum_{z\in \mathrm{CM}(K)} \log|\Psi(z)|. \end{aligned}$$

Here we used the fact that $\mathcal{CM}(K)$ never meets with the boundary of $\tilde{\mathcal{M}}$ and thus $\mathcal{CM}(K).\tilde{\mathcal{T}}_m = \mathcal{CM}(K).\mathcal{T}_m$. By [BY, Theorem 1.1] (this is the place we need the condition that $\tilde{D}$ is prime), and the fact

$$W_K = W_{\tilde{K}} = \begin{cases} 10 & \text{if } K = \mathbb{Q}(\zeta_5), \\ 2 & \text{otherwise,} \end{cases} \tag{8.8}$$

one has

$$\frac{2}{W_K}\sum_{z\in \mathrm{CM}(K)} \log|\Psi(z)| = \frac{1}{2}cb_q - \frac{1}{2}\sum c_i b_{q_i}.$$

Now applying Theorem 1.8, one has

$$0 = c(\mathcal{T}_q.\mathcal{CM}(K) - \frac{1}{2}b_q) - \sum c_i(\mathcal{T}_{q_i}.\mathcal{CM}(K) - \frac{1}{2}b_{q_i}) = cc_q\log q - \sum c_i c_{q_i}\log q_i$$

for some rational numbers $c_q, c_i \in \mathbb{Q}$. Since $\log q$ and $\log q_i$ are $\mathbb{Q}$-linearly independent, we have $c_q = c_{q_i} = 0$, and thus

$$\mathcal{T}_q.\mathcal{CM}(K) = \frac{1}{2}b_q. \tag{8.9}$$

Now we turn to the general case. Using again Theorem 8.1, there are non-zero integers $c$ and $c_i$ and primes $q_i$ split in $F$ such that

$$c\hat{\mathcal{T}}_m = \sum c_i \hat{\mathcal{T}}_{q_i}.$$

So there is a (normalized integral) Hilbert meromorphic function $\Psi$ such that

$$\operatorname{div}(\Psi) = c\tilde{\mathcal{T}}_m - \sum c_i \tilde{\mathcal{T}}_{q_i}.$$

So one has by (8.4), (8.9) and [BY, Theorem 1.1]

$$\begin{aligned} 0 &= h_{\widehat{\operatorname{div}(\Psi)}}(\mathcal{CM}(K)) \\ &= c\mathcal{CM}(K).\mathcal{T}_m - \sum c_i \mathcal{CM}(K).\mathcal{T}_{q_i} - \frac{2}{W_K} \sum_{z \in \mathrm{CM}(K)} \log|\Psi(z)| \\ &= c\mathcal{CM}(K).\mathcal{T}_m - \frac{1}{2} c b_m. \end{aligned}$$

Therefore $\mathcal{T}_m.\mathcal{CM}(K) = \frac{1}{2} b_m$. This proves Theorem 1.2.

*Proof of Theorem 1.3.* By [BBK, Theorems 4.15, 5.7], there is a normalized integral meromorphic Hilbert modular form $\Psi$ of weight $c(0) > 0$ such that

$$\operatorname{div}\Psi = \sum_{m>0} c_m \tilde{\mathcal{T}}_m.$$

Now the same argument as in the proof of [Ya4, Theorem 1.5] gives

$$h_{\hat{\omega}}(\mathcal{CM}(K)) = \frac{\#\,\mathrm{CM}(K)}{W_K} \beta(K/F). \tag{8.10}$$

Combining this with (8.7), one proves the theorem.

To state Theorem 1.4 more precisely and prove it, we need some preparation. Let

$$E_2^+(\tau) = 1 + \sum_{m>0} C(m,0) e(n\tau), \quad C(m,0) = \frac{2\sum_{d|m} d}{L(-1, (\frac{D}{}))} \tag{8.11}$$

be the Eisenstein series of weight 2, level $D$, and Nebentypus character $(\frac{D}{})$ given in [BY, Corollary 2.3].

Let $\chi_{\tilde{K}/\tilde{F}}$ be the quadratic Hecke character of $\tilde{F}$ associated to $\tilde{K}/\tilde{F}$, and let $I(s, \chi_{\tilde{K}/\tilde{F}})$ be the induced representation of $\mathrm{SL}_2(\mathbb{A}_{\tilde{F}})$. In [BY, Section 6], we choose a specific section $\Phi \in I(s, \chi_{\tilde{K}/\tilde{F}})$ and constructed an (incoherent) Eisenstein series of weight 1

$$E^*(\tau_1, \tau_2, s, \Phi) = (v_1 v_2)^{-\frac{1}{2}} E(g_{\tau_1} g_{\tau_2}, s, \Phi) \Lambda(s+1, \chi_{\tilde{K}/\tilde{F}}).$$

Here $\tau_j = u_j + iv_j \in \mathbb{H}$. The Eisenstein series is automatically zero at $s = 0$. So its diagonal restriction of $\mathbb{H}$ is a modular form of weight 2, level $D$, Nebentypus character $(\frac{D}{})$ which is zero at $s = 0$. Let

$$\tilde{f}(\tau) = \frac{1}{\sqrt{D}} E^{*,\prime}(\tau, \tau, 0, \Phi)|_2 W_D$$

be the modular form defined in [BY, (7.2)]) (with $K$ in [BY, Sections 7 and 8] replaced by $\tilde{K}$). Here $W_D = \left(\begin{smallmatrix} 0 & -1 \\ D & 0 \end{smallmatrix}\right)$. Finally let $f$ be the holomorphic projection of $\tilde{f}$. According to [BY, Theorem 8.1], one has the Fourier expansion

$$f(\tau) = -4 \sum_{m>0} (b_m + c_m + d_m) e(m\tau) \tag{8.12}$$

where $b_m$ is the number in Conjecture 1.1,

$$d_m = \frac{1}{2} C(m, 0) \Lambda(0, \chi_{\tilde{K}/\tilde{F}}) \beta(\tilde{K}/\tilde{F}) \tag{8.13}$$

and $c_m$ is some complicated constant defined in [BY, Theorem 8.1]. Notice that the Green function $G_m$ in $\hat{\mathcal{T}}_m$ is also the Green function used in [BY]. So [BY, (9.3)] gives ($\mathcal{CM}(K)$ in [BY] is our $\mathrm{CM}(K)$)

$$c_m = \frac{4}{W_{\tilde{K}}} G_m(\mathrm{CM}(K)) = \frac{4}{W_K} G_m(\mathrm{CM}(K)). \tag{8.14}$$

As explained in the proof of [Ya4, Theorem 1.5], one has

$$\Lambda(s, \chi_{\tilde{K}/\tilde{F}}) = \Lambda(s, \chi_{K/F}).$$

So $\beta(\tilde{K}/\tilde{F}) = \beta(K/F)$. One has also by [BY, (9.2)] and (8.8)

$$\Lambda(0, \chi_{\tilde{K}/\tilde{F}}) = \frac{2\# \,\mathrm{CM}(K)}{W_K}. \tag{8.15}$$

So (8.10) implies

$$d_m = h_{\hat{\omega}}(\mathcal{CM}(K)) C(m, 0). \tag{8.16}$$

So we have

$$f(\tau) = -4 \sum_{m>0} (b_m + \frac{4}{W_K} G_m(\mathrm{CM}(K))) e(m\tau) - 4 h_{\hat{\omega}}(\mathcal{CM}(K)) \sum_{m>0} C(m, 0) e(m\tau). \tag{8.17}$$

Now we can restate Theorem 1.4 more precisely:

Theorem 8.2. *Let the notation be as above. Assuming (1.5) and that* $\tilde{D} = \Delta\Delta' \equiv 1 \mod 4$ *is a prime. Then*

$$h_{\hat{\phi}}(\mathcal{CM}(K)) + \frac{1}{2} h_{\hat{\omega}}(\mathcal{CM}(K)) E_2^+(\tau) = -\frac{1}{8} f(\tau).$$

*Proof.* By Theorem 1.2, (8.4), and (8.10), we have

$$\begin{aligned} h_{\hat{\phi}}(\mathcal{CM}(K)) &= -\frac{1}{2} h_{\hat{\omega}}(\mathcal{CM}(K)) + \sum_{m>0} h_{\hat{\mathcal{T}}}(\mathcal{CM}(K)) e(m\tau) \\ &= -\frac{1}{2} h_{\hat{\omega}}(\mathcal{CM}(K)) + \sum_{m>0} (\mathcal{CM}(K).\mathcal{T}_m + \frac{2}{W_K} G_m(\mathrm{CM}(K))) e(m\tau) \\ &= -\frac{1}{2} h_{\hat{\omega}}(\mathcal{CM}(K)) + \frac{1}{2} \sum_{m>0} (b_m + \frac{4}{W_K} G_m(\mathrm{CM}(K))) e(m\tau). \end{aligned}$$

Combining this with (8.11) and (8.17), one proves the theorem. □

**9. Siegel modular variety of genus 2 and Lauter's conjecture.** Following [CF], let $\mathcal{A}_2$ be the moduli stack over $\mathbb{Z}$ representing the principally polarized abelian surfaces $(A, \lambda)$. Then $\mathcal{A}_2(\mathbb{C}) = \mathrm{Sp}_2(\mathbb{Z})\backslash\mathbb{H}_2$ is the Siegel modular surface of genus 2. Here $\mathbb{H}_2 = \{Z \in \mathrm{Mat}_2(\mathbb{C});\ Z = {}^tZ, \mathrm{Im}(Z) > 0\}$ is the Siegel upper half plane of genus two. Let $\epsilon$ be a fixed fundamental unit if $F = \mathbb{Q}(\sqrt{D})$ with $\epsilon > 0$ and $\epsilon' < 0$. Then

$$\phi_D : \mathcal{M} \to \mathcal{A}_2, \quad (A, \iota, \lambda) \mapsto (A, \lambda(\frac{\epsilon}{\sqrt{D}})) \tag{9.1}$$

is a natural map from $\mathcal{M}$ to $\mathcal{A}_2$, which is proper and generically 2 to 1. For an integer $m \geq 1$, let $G_m$ be the Humbert surface in $\mathcal{A}_2(\mathbb{Q})$ [Ge, Chapter IX], defined as follows (over $\mathbb{C}$). Let $L = \mathbb{Z}^5$ be the lattice with the quadratic form

$$Q(a, b, c, d, e) = b^2 - 4ac - 4de.$$

We remark that there is an isomorphism between $\mathrm{Sp}_2(\mathbb{Q})/\{\pm 1\}$ and $\mathrm{SO}(L \otimes \mathbb{Q})$. For $x \in L$ with $Q(x) > 0$, we define

$$H_x = \{\tau = \left(\begin{smallmatrix} \tau_1 & \tau_2 \\ \tau_2 & \tau_3 \end{smallmatrix}\right) \in \mathbb{H}_2 :\ a\tau_1 + b\tau_2 + c\tau_3 + d(\tau_2^2 - \tau_1\tau_3) + e = 0\}.$$

Then $H_x$ is a copy of $\mathbb{H}^2$ embedded into $\mathbb{H}_2$. The Humbert surface $G_m$ is then defined by

$$G_m = \mathrm{Sp}_2(\mathbb{Z})\backslash\{H_x :\ x \in L, Q(x) = m\}. \tag{9.2}$$

Let $\mathcal{G}_m$ be the flat closure of $G_m$ in $\mathcal{A}_2$. Then $(\phi_D)_*\mathcal{M} = 2\mathcal{G}_D$, and

$$\phi_D^*\mathcal{G}_m = \sum_{n>0,\, \frac{Dm-n^2}{4} \in \mathbb{Z}_{>0}} \mathcal{T}_{\frac{Dm-n^2}{4}} \tag{9.3}$$

when $mD$ is a not a square. Indeed, it is known [Fr, Theorem 3.3.5], [Ge, Proposition IX 2.8] that

$$\phi_D^* G_m = \sum_{n>0,\, \frac{Dm-n^2}{4} \in \mathbb{Z}_{>0}} T_{\frac{Dm-n^2}{4}}.$$

So their flat closures in $\mathcal{M}$ are equal too, which is (9.4).

Let $K$ be a quartic CM number field with real quadratic subfield $F$, and let $\mathcal{CM}_S(K)$ be the moduli stack over $\mathbb{Z}$ representing the moduli problem which assigns a scheme $S$ the set of triples $(A, \iota, \lambda)$ where $(A, \lambda) \in \mathcal{A}_2(S)$ and $\iota$ is an $\mathcal{O}_K$-action on $A$ such that the Rosati involution associated to $\lambda$ gives complex conjugation on $K$. Notice that the map

$$\mathcal{CM}(K) \to \mathcal{CM}_S(K), \quad (A, \iota, \lambda) \mapsto (A, \iota, \lambda(\frac{\epsilon}{\sqrt{D}})) \tag{9.4}$$

is an isomorphism of stacks. We also denote $\mathcal{CM}_S(K)$ for the direct image of $\mathcal{CM}_S(K)$ in $\mathcal{A}_2$ under the forgetful map (forgetting the $\mathcal{O}_K$ action). Then the above isomorphism implies that $(\phi_D)_*(\mathcal{CM}(K)) = \mathcal{CM}_S(K)$. Now the proof of Theorem 1.5 is easy.

*Proof of Theorem 1.5.* By the projection formula, Theorem 1.2, and remarks above, one has

$$\begin{aligned}\mathcal{CM}_S(K).\mathcal{G}_m &= (\phi_D)_*(\mathcal{CM}(K)).\mathcal{G}_m\\ &= \mathcal{CM}(K).\phi_D^*(\mathcal{G}_m)\\ &= \sum_{n>0,\,\frac{Dm-n^2}{4}\in\mathbb{Z}_{>0}} \mathcal{CM}(K).\mathcal{T}_{\frac{Dm-n^2}{4}}\\ &= \frac{1}{2}\sum_{n>0,\,\frac{Dm-n^2}{4}\in\mathbb{Z}_{>0}} b_{\frac{Dm-n^2}{4}}\end{aligned}$$

as claimed.

To describe and prove Lauter's conjecture on Igusa invariants, we need more notation. Let

$$\theta_{a,b}(\tau,z) = \sum_{n\in\mathbb{Z}^2} e^{\pi i\,{}^t(n+\frac{1}{2}a)\tau(n+\frac{1}{2}a)+2\,{}^t(n+\frac{1}{2}a)(z+\frac{1}{2}b)} \tag{9.5}$$

be the theta functions on $\mathbb{H}_2\times\mathbb{C}^2$ with characters $a, b \in (\mathbb{Z}/2)^2$. It is zero at $z = 0$ unless ${}^tab \equiv 0 \mod 2$. In such a case, we call $\theta_{a,b}(\tau, 0)$ an even theta constants. There are exactly ten of them, we renumber them as $\theta_i$, $1 \le i \le 10$. They are Siegel modular forms of weight 1/2 and some level.

$$h_{10} = \prod_i \theta_i^2$$

is a cusp form of weight 10 and level 1 and is the famous Igusa cusp form $\chi_{10}$. Igusa also defines in [Ig1] three other Siegel modular forms $h_4 = \sum_i \theta_i^8$, $h_{12}$, and $h_{16}$ for $\mathrm{Sp}_2(\mathbb{Z})$ of weight 4, 12, and 16 respectively as polynomials of these even theta constants. We refer to [Wen] for the precise definition of $h_{12}$ and $h_{16}$ since they are complicated and not essential to us. The so-called 3 Igusa invariants are defined as ([Wen, Section 5]

$$j_1 = \frac{h_{12}^5}{h_{10}^6},\quad j_2 = \frac{h_4h_{12}^3}{h_{10}^4},\quad j_3 = \frac{h_{16}h_{12}^2}{h_{10}^4}. \tag{9.6}$$

It is known that $h_i$ have integral Fourier coefficients. Since four of ten theta constants have constant term 1 and the other six are multiples of 2, one can check ([GN])

$$h_{10} = 2^{12}\Psi_{1,S}$$

where $\Psi_{1,S}$ is an integral Siegel modular form for $\mathrm{Sp}_2(\mathbb{Z})$ with constant term 1 and $\operatorname{div}\Psi_{1,S} = 2\mathcal{G}_1$. One can also check

$$h_4 = 2^4\tilde{h}_4,\quad h_{12} = 2^{15}\tilde{h}_{12},\quad h_{16} = 2^{15}\tilde{h}_{16}$$

with $\tilde{h}_4, \tilde{h}_{12}$, and $\tilde{h}_{16}$ still having integral coefficients. So

$$j_1 = 2^3\frac{\tilde{h}_{12}^5}{\Psi_{1,S}^6},\quad j_2 = 2\frac{\tilde{h}_4\tilde{h}_{12}}{\Psi_{1,S}^4},\quad j_3 = 2^{-3}\frac{\tilde{h}_{12}\tilde{h}_{16}}{\Psi_{1,S}^4}. \tag{9.7}$$

We renormalize

$$j_1 = 2^3 B_1 j_1', \quad j_2 = 2B_2 j_2', \quad j_3 = 2^{-3} B_3 j_3' \tag{9.8}$$

for some positive integers $B_i$ so that $j_i'$ can be written as

$$j_i' = \frac{f_i}{\Psi_{1,S}^{n_i}}$$

with $n_1 = 6, n_2 = n_3 = 4$ such that $f_i$ are integral Siegel modular forms whose Fourier coefficients have greatest common divisor 1.

Let $K$ be a quartic non-biquadratic CM number field with real quadratic subfield $F = \mathbb{Q}(\sqrt{D})$. For a CM type $\Phi$ of $K$, let $\mathrm{CM}_S(K, \Phi)$ be the formal sum of principally polarized abelian surfaces over $\mathbb{C}$ of CM type $(\mathcal{O}_K, \Phi)$ (up to isomorphism). It is the image of $\mathrm{CM}(K, \Phi)$ under $\phi_D$. So $\mathrm{CM}_S(K) = \mathrm{CM}_S(K, \Phi_1) + \mathrm{CM}_S(K, \Phi_2)$ is defined over $\mathbb{Q}$ and

$$\mathcal{CM}_S(K)(\mathbb{C}) = 2\,\mathrm{CM}_S(K).$$

Here $\Phi_1$ and $\Phi_2$ are two CM types of $K$ such that $\Phi_i$ and $\rho\Phi_i$ give all CM types of $K$ ($\rho$ is the complex conjugation). By the theory of complex multiplication [Sh, Main Theorem 1, page 112],

$$j_i'(\mathrm{CM}_S(K)) := \prod_{z \in \mathrm{CM}_S(K)} j_i'(z)$$

is a power of $\mathrm{N}(j_i'(z))$ for any CM point $z \in \mathrm{CM}_S(K)$.

*Proof of Theorem 1.7.* We prove the theorem for $j_1'$. The proof for $j_2'$ and $j_3'$ is the same. We first prove $A_1\,\mathrm{N}(j_1'(\tau)) \in \mathbb{Z}$. By the theory of complex multiplication [Sh, Main Theorem 1, page 112],

$$j_i'(\mathrm{CM}_S(K)) := \prod_{\tau \in \mathrm{CM}_S(K)} j_i'(\tau)$$

is a power of $\mathrm{N}(j_i'(\tau))$ for any CM point $\tau \in \mathrm{CM}_S(K)$. Since $\mathcal{CL}_0(K) \cong \mathcal{CL}_0(\tilde{K})$ in our case by [BY, Lemma 5.3], we have actually $j_i'(\mathrm{CM}_S(K)) = \mathrm{N}(j_1'(\tau))$.

Notice that

$$\operatorname{div} j_1' = \operatorname{div} f_1 - 12\mathcal{G}_1.$$

If $\mathcal{CM}(K)$ and $\operatorname{div} f_1$ intersect improperly, they have a common point over $\mathbb{C}$ (since both are horizontal). So $f_1(\mathrm{CM}(K) = 0$ and $j_1'(\mathrm{CM}_S(K)) = 0$, there is nothing to prove. So we may assume $\mathcal{CM}(K)$ and $\operatorname{div} f_1$ intersect properly. Since both are effective cycles, one has

$$\mathcal{CM}(K).\operatorname{div} f_1 = a \log C$$

for some positive integer $C > 0$ and a rational number $a > 0$. Now

$$\begin{aligned} 0 &= h_{\widehat{\operatorname{div} j_1'}}(\mathcal{CM}(K)) \\ &= \mathcal{CM}(K).\operatorname{div} f_1 - 12\mathcal{CM}(K).\mathcal{G}_1 - \frac{2}{W_K}\log|j_1'(\mathrm{CM}_S(K))| \\ &= \mathcal{CM}(K).\operatorname{div} f_1 - 6\sum_{0<n<\sqrt{D}, odd} b_{\frac{D-n^2}{4}} - \frac{2}{W_K}\log|j_1'(\mathrm{CM}_S(K)|. \end{aligned}$$

Write $\mathrm{N}(j_1'(\tau)) = M_1/N_1$ with $(M_1, N_1) = 1$. Then

$$\log|M_1| - \log N_1 = \log|j_1'(\mathrm{CM}_S(K)| = \frac{aW_K}{2}\log C - 3W_K \sum_{0<n<\sqrt{D}, odd} b_{\frac{D-n^2}{4}},$$

and so

$$\begin{aligned}\log N_1 &= 3W_K \sum_{0<n<\sqrt{D}, odd} b_{\frac{D-n^2}{4}} + \log|M_1| - \frac{aW_k}{2}\log C \\ &= \log A_1 + \log|M_1| - \frac{aW_k}{2}\log C.\end{aligned}$$

So $N_1 C^{\frac{aW_K}{2}} = A_1|M_1|$, and thus $N_1|A_1$. $A_1\,\mathrm{N}(j_1'(\tau)) \in \mathbb{Z}$.

We now derive $A_1 H_1(x) \in \mathbb{Z}$. The $k$-th coefficient of $H_1(x)$ is

$$a_k = \sum_{i_1 \le i_2 \le \cdots \le i_k} j_1'(\tau_{i_1}) \cdots j_1'(\tau_{i_k})$$

where $\tau_j \in \mathcal{CM}_S(K)$. Write

$$j_1'(\tau_j)\mathcal{O}_L = \frac{\mathfrak{a}_j}{\mathfrak{b}_j}$$

uniquely with $\mathfrak{a}_j, \mathfrak{b}_j$ being integral ideals of $\mathcal{O}_L$, where $L$ is a Galois extension of $\mathbb{Q}$ containing all $j_1'(\tau_j)$. Then $N_1\mathbb{Z} = \prod \mathfrak{b}_j$. So

$$a_k\mathbb{Z} = \mathfrak{c}/N_1$$

where

$$\mathfrak{c} = \sum \prod_{l=1}^{k} \mathfrak{a}_{i_l} \prod_{j \ne i_l} \mathfrak{b}_j$$

is an integral ideal of $L$. So $\mathfrak{c} = c\mathbb{Z}$ for some integer $c$, and thus $a_k = \pm c/N_1$. That is $Aa_k \in \mathbb{Z}$. This proves Theorem 1.7

**Update.** After the paper was first written in 2007, there were quite a few developments. Here are a couple that I know of. Ben Howard and the author looked at the problem again in 2009 and developed a direct approach using Kudla and Rapoport's moduli interpretation of the arithmetic Hirzeburch-Zagier divisors. Actually we discovered a finer moduli problem and proved a new arithmetic Siegel-Weil formula under some technical local condition [HY]. The result is more general and works for more general real quadratic fields. Bruinier, Kudla, and the author [BKY] generalized the work in [BY] to more general CM number fields too. Both are a little more complicated than the statement we have here and [BY]. It seems very reasonable to prove Colmez's conjecture for a general CM quartic field now using results in [HY] and [BKY]. I hope to get back to it in the near future. The computational work of [GJLLSVW] confirms the main theorem in this paper in cases we dealt with and the abnormality they pointed out should be explainable by the new work in [BKY] and [HY].

## REFERENCES

[An] G. Anderson, *Logarithmic derivatives of Dirichlet L-functions and the periods of abelian varieties*, Compositio Math., 45 (1982), pp. 315–332.

[BBK] J. Bruinier, J. Burgos Gil, and U. Kühn, *Borcherds products and arithmetic intersection theory on Hilbert modular surfaces*, Duke Math. J., 139 (2007), pp. 1–88.

[BKK] J. Burgos Gil, J. Kramer, and U. Kühm , *Cohomological arithmetic Chow rings*, J. Inst. Math. Jussieu, 6 (2007), pp. 1–172.

[BKY] J. Bruinier, S. Kudla, and T. H. Yang, *Big CM values of automorphic greens functions*, IMRN (2012), no. 9, pp. 1917–1967.

[BY] J. H. Bruinier and T. H. Yang, *CM values of Hilbert modular functions*, Invent. Math., 163 (2006), pp. 229–288.

[CF] G. Faltings and C. L. Chai, *Degeneration of abelian varieties*, Springer-Verlag, 1990.

[CS] C. Chowla and A. Selberg, *On Epstein's zeta-function*, J. Reine Angew. Math., 227 (1967), pp. 86–110.

[CL] H. Cohn and K. Lauter, *Generating genus two curves with complext multiplication*, Microsoft Internal Techincal Report, January, 2001.

[Co] P. Colmez, *Périods des variétés abéliennes à multiplication complex*, Ann. Math., 138 (1993), pp. 625–683.

[Co2] P. Colmez, *Périodes de variétés abéliennes à multiplication complexe et dérivées de fonctions L d'Artin en s* = 0, C. R. Acad. Sci. Paris Sér. I Math., 309 (1989), pp. 139–142.

[Fa] G. Faltings, *Finiteness theorems for abelian varieties over number fields*, Translated from the German original [Invent. Math., 73:3 (1983), pp. 349–366; ibid. 75:2 (1984), 381; MR 85g:11026ab] by Edward Shipz. Arithmetic geometry (Storrs, Conn., 1984), pp. 9–27, Springer, New York, 1986.

[Fr] H.-G. Franke, *Kurven in Hilbertschen Modulflächen und Humbertsche Flächen im Siegelraum*, Bonner Math. Schriften, 104 (1978).

[Ge] G. van der Geer, *Hilbert Modular Surfaces*, Springer-Verlag (1988).

[Gi] H. Gillet, *Intersection theory on algebraic stacks and Q-varieties*, in Proceedings of the Luminy conference on algebraic K-theory (Luminy, 1983), volume 34, pp. 193–240, 1984.

[Go] E. Goren, *Lectures on Hilbert modular varieties and modular forms*, CRM monograph series 14, 2001.

[GL] E. Goren and K. Lauter, *Class invariants for quartic CM fields*, Ann. Inst. Fourier (Grenoble), 57 (2007), pp. 457–480.

[GN] V. A. Gritsentko and V. V. Nikulin, *Siegel automorphic form corrections of some Lorentzian Kac-Moody Lie algebras*, Amer. J. Math., 119 (1997), pp. 181–224.

[Gr] B. Gross, *On the periods of abelian integrals and a formula of Chowla and Selberg*, with an appendix by David E. Rohrlich, Invent. Math., 45 (1978), pp. 193–211.

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

[GZ1] B. Gross and D. Zagier, *Heegner points and derivatives of L-series*, Invent. Math., 84 (1986), pp. 225–320.

[GZ2] B. Gross and D. Zagier, *On singular moduli*, J. Reine Angew. Math., 355 (1985), pp. 191–220.

[GJLLSVW] H. Grundman, J. Johnson-Leung, K. Lauter, A. Aalerno, B. Viray, and E. Wittenborn, *Igusa class polynomials, embeddings of quartic cm fields, and arithmetic intersection theory*, in WIN–Women in Numbers: Research Directions in Number Theory, Fields Institute Communications Series, Volume 60 (2011).

[HZ] F. Hirzebruch and D. Zagier, *Intersection Numbers of Curves on Hilbert Modular Surfaces and Modular Forms of Nebentypus*, Invent. Math., 36 (1976), pp. 57–113.

[Ho] B. Howard, *Complex nultiplication cycles and Kudla-Rapoport divisors*, Ann. Math., 176 (2012), pp. 1097–1171.

[HY] B. Howard and T. H. Yang, *Intersection of Hirzebruch-Zagier divisors and CM cycles*, Lecture Notes in Mathematics, 2041 (2012), Springer, New York, pp145.

[Ig1] J.-I. Igusa, *Arithmetic Variety of Moduli for Genus Two*, Ann. Math., 72 (1960), pp. 612–649

[Ig2] J.-I. Igusa, *Modular Forms and Projective Invariants*, American Journal of Mathematics, 89 (1967), pp. 817–855.

[La] K. Lauter, *Primes in the denominators of Igusa Class Polynomials*, preprint, pp3, http://www.arxiv.org/math.NT/0301240/

[KRo] K. Köhler and D. Roessler, *Afixed point formula of Lefschetz type in Arakelov geometry. IV. The modular height of C.M. abelian varieties*, J. Reine Angew. Math., 556 (2003), pp. 127–148.

[KZ] M. Kontsevich and D. Zagier, *Periods*, Mathematics unlimited—2001 and beyond, pp. 771–808, Springer, Berlin, 2001.

[Ku1] S. Kudla, *Central derivatives of Eisenstein series and height pairings*, Ann. of Math. (2), 146 (1997), pp. 545–646.

[Ku2] S. Kudla, *Derivatives of Eisentein series and arithmetic geometry*, Publ. ICM, Vol II (Beijing 2002), pp. 173–183, Higher Education Press, Beijing, 2002.

[Ku3] S. Kudla, *Special cycles and derivatives of Eisenstein series*, in Heegner points and Rankin L-series, 243-270, Math. Sci. Res. Inst. Publ., 49, Cambridge Univ. Press, Cambridge, 2004.

[KR1] S. Kudla and M. Rapoport, *Arithmetic Hirzebruch Zagier cycles*, J. reine angew. Math., 515 (1999), pp. 155–244.

[KR2] S. Kudla and M. Rapoport, *Cycles on Siegel 3-folds and derivatives of Eisenstein series*, Annales Ecole. Norm. Sup., 33 (2000), pp. 695–756.

[KRY1] S. Kudla, M. Rapoport, and T. H. Yang, *Derivatives of Eisenstein Series and Faltings heights*, Comp. Math., 140 (2004), pp. 887–951.

[KRY2] S. Kudla, M. Rapoport, and T. H. Yang, *Modular forms and special cycles on Shimura curves*, Annals of Math. Studies series, vol. 161, Princeton Univ. Publ., 2006.

[KRY3] S. Kudla, M. Rapoport, and T. H. Yang, *On the derivative of Eisenstein Series of weight one*, IMRN (1999), pp. 347–385.

[MR] V. Maillot and D. Roessler, *On the periods of motives with complex multiplication and a conjecture of Gross-Deligne*, Ann. of Math. (2), 160 (2004), pp. 727–754.

[Pa] G. Pappas, *Arithmetic models for Hilbert modular varieties*, Compos. Math., 98 (1995), pp. 43–76.

[Ru] B. Runge, *Endomorphism rings of abelian surfaces and projective models of their moduli spaces*, Tohoku Math. J., 51 (1999), pp. 283–303.

[Se] J.-P. Serre, *A course in Arithmetic*, GTM 7, Springer-Verlag, New York, 1973.

[Sh] G. Shimura, *Abelian varieties with complex multiplication and modular functions*, Princeton Math. Series, vol. 46, Princeton Univ. Press, 1997.

[Vi] A. Vistoli, *Intersection theory on algebraic stacks and on their moduli spaces*, Invent. Math., 97 (1989), pp. 613–670.

[Vo] I. Vollaard, *On the Hilbert-Blumenthal moduli problem*, J. Inst. Math. Jussieu, 4 (2005), pp. 653–683.

[We1] T. Wedhorn, *The genus of the endomorphisms of a supersingular elliptic curve*, Chapter 5 in ARGOS seminar on Intersections of Modular Correspondences, pp. 37–58; Astérisque, 312 (2007), pp. 25–47.

[We2] T. Wedhorn, *Caculation of representation densities*, Chapter 15 in ARGOS seminar on Intersections of Modular Correspondences, pp. 185–196; Astérisque, 312 (2007), pp. 179–190.

[Wen] A. Weng, *Constructing hyperelliptic curves of genus two suitable for cryptography*, Math. Comp., 72 (2002), pp. 435–458.

[Ya1] T. H. Yang, *An explicit formula for local densities of quadratic forms*, J. Number Theory, 72 (1998), pp. 309–356.

[Ya2] T. H. Yang, *Local densities of* 2*-adic quadratic forms*, J. Number Theory, 108 (2004), pp. 287–345.

[Ya3] T. H. Yang, *Chowla-Selberg Formula and Colmez's Conjecture*, accepted to appear in Canada J. Math., pp17.

[Ya4] T. H. Yang, *An arithmetic intersection formula on Hilbert modular surfaces*, accepted to appear in Amer. J. Math., pp30.

[Ya5] T. H. Yang, *Hilbert modular functions and their CM values*, Proc. of the 3rd ICCM, AMS/IP Studies in Adv. Math., 42 (2008), pp. 135–154.

[Yo] H. Yoshida, *Absolute CM-periods. Mathematical Surveys and Monographs*, 106, American Mathematical Society, Providence, RI, 2003.

[Yu] C. F. Yu, *The isomorphism classes of abelian varieties of CM types*, Jour. pure and Appl. Algebra, 187 (2004), pp. 305–319.

[Zh1] S. W. Zhang, *Heights of Heegner cycles and derivatives of L-series*, Invent. Math., 130:1 (1997), pp. 99–152.

[Zh2] S. W. Zhang, *Heights of Heegner points on Shimura curves*, Ann. of Math. (2), 153:1 (2001), pp. 27–147.

[Zh3] S. W. Zhang, *Gross-Zagier formula for GL(2)*, Asian. J. Math., 5:2 (2001), pp. 183–290; II, Heegner points and Rankin L-series, pp. 191–214, Math. Sci. Res. Inst. Publ., 49, Cambridge Univ. Press, Cambridge, 2004.