Notes on Howard-Yang's singular moduli

Avi Zeff

Note: this is my attempt to understand section 2 of Howard-Yang's paper [3] essentially by rewriting it, up to leaving out a few lemmas. There is nothing original in this document, and the reader will probably be better served by reading the original paper (which also includes the missing lemmas) except insofar as having multiple expositions of the same ideas might be helpful.

Fix imaginary quadratic fields K_1 and K_2, with rings of integers $\mathcal{O}_{K_1}$ and $\mathcal{O}_{K_2}$ and coprime discriminants d_1 and d_2 respectively, and set $K = K_1 \otimes K_2$ and let F be the totally real quadratic subfield of K, with corresponding rings of integers $\mathcal{O}_K$ and $\mathcal{O}_F$. Let $\mathcal{X}$ be the stack classifying pairs of elliptic curves (E_1, E_2) over a base scheme S where E_i has complex multiplication by $\mathcal{O}_{K_i}$, and set $V(E_1, E_2) = \mathrm{Hom}(E_1, E_2) \otimes_{\mathbb{Z}} \mathbb{Q}$. Let $\kappa_i : \mathcal{O}_{K_i} \hookrightarrow \mathrm{End}(E_i)$ be the action morphisms. For $t_1 \otimes t_2 \in \mathcal{O}_K = \mathcal{O}_{K_1} \otimes \mathcal{O}_{K_2}$ and $j \in \mathrm{Hom}(E_1, E_2)$, we can define

$$(t_1 \otimes t_2) \bullet j = \kappa_2(t_2) \circ j \circ \kappa_1(t_1)^{-1},$$

which extends to an action of $\mathcal{O}_K$ on V. There is a quadratic form $\deg_{\mathrm{CM}}$ on V defined over F which lifts the usual degree form, i.e.

$$\deg_{\mathrm{CM}} = \mathrm{Tr}_{F/\mathbb{Q}} \circ \deg .$$

For any integer $m \geq 1$, define $\mathcal{T}_m$ to be the stack classifying triples (E_1, E_2, j) where E_1 and E_2 are elliptic curves over a base scheme S with respective actions by $\mathcal{O}_{K_1}$ and $\mathcal{O}_{K_2}$ as above and $j \in \mathrm{Hom}(E_1, E_2)$ satisfies $\deg j = m$. Using $\deg_{\mathrm{CM}}$, we can refine this further: for any $\alpha \in F^\times$, let $\mathcal{X}_\alpha$ be the stack classifying triples (E_1, E_2, j) such that $(E_1, E_2) \in \mathcal{X}(S)$ is pair of elliptic curves with complex multiplication as above and $j \in \mathrm{Hom}(E_1, E_2)$ satisfies $\deg_{\mathrm{CM}}(j) = \alpha$. Then we have

$$\mathcal{T}_m = \bigsqcup_{\substack{\alpha \in F^\times \\ \mathrm{Tr}_{F/\mathbb{Q}}(\alpha) = m}} \mathcal{X}_\alpha.$$

For any scheme S and stack X, write $[X(S)]$ for the set of isomorphism classes in $X(S)$. Our goal is to compute the Arakelov degree of $\mathcal{X}_\alpha$, defined as

$$\deg \mathcal{X}_\alpha = \sum_p \log(p) \sum_{x \in [\mathcal{X}_\alpha(\overline{\mathbb{F}_p})]} \frac{\mathrm{length}\, \mathcal{O}^{\mathrm{sh}}_{\mathcal{X}_\alpha, x}}{\mathrm{Aut}(x)}$$

where $\mathcal{O}^{\mathrm{sh}}_{\mathcal{X}_\alpha, x}$ is the strictly Henselian local ring of $\mathcal{X}_\alpha$ at x, a modification of the usual local ring to be defined in the following section. Using this computation and the above decomposition, we can recover the main result of [2] in the form of a computation of the Arakelov degree of $\mathcal{T}_1$.

The method is as follows. First, we study the term $\mathrm{length}\, \mathcal{O}^{\mathrm{sh}}_{\mathcal{X}_\alpha, x}$ using the deformation theory of the one-dimensional height 2 p-divisible group over $\overline{\mathbb{F}_p}$; this is isomorphic to the p-divisible group of any supersingular elliptic curve, and we'll see that we can assume that our curves are in fact supersingular and so we can apply this to the deformation theory of

a tuple (E_1, E_2, j). We will find that in fact length $\mathcal{O}^{\mathrm{sh}}_{\mathcal{X}_\alpha, x}$ is independent of x, and can be computed explicitly. It remains then to compute

$$\sum_{x \in [\mathcal{X}_\alpha(\overline{\mathbb{F}_p})]} \frac{1}{\mathrm{Aut}(x)}$$

for each p, which we do by rewriting adelically and decomposing the sum into a product of orbital integrals, which we then compute. (In fact $\mathrm{Aut}(x)$ also turns out to be independent of x, so this is really just counting points (up to isomorphism) on $\mathcal{X}_\alpha(\overline{\mathbb{F}_p})$.)

1. Deformation theory

Fix a point $(E_1, E_2, j) \in \mathcal{X}_\alpha$ over $\overline{\mathbb{F}_p}$. Since E_1 and E_2 are isogenous via j, they are either both supersingular or both ordinary; if they are both ordinary, then the injections $\kappa_i : \mathcal{O}_{K_i} \hookrightarrow \mathrm{End}(E_i)$ extend to injections $K_i \hookrightarrow \mathrm{End}(E_i) \otimes_{\mathbb{Z}} \mathbb{Q}$, both sides of which are 2-dimensional vector spaces over $\mathbb{Q}$, so this is in fact an isomorphism. But isogenous elliptic curves have isomorphic endomorphism rings, so we conclude $K_1 \simeq K_2$, contrary to our assumptions. Therefore E_1 and E_2 must both be supersingular, and so the κ_i extend to embeddings $K_i \hookrightarrow B$ into the unique quaternion algebra ramified at p and ∞. In particular it follows that p is nonsplit in both K_1 and K_2.

Let $W = W(\overline{\mathbb{F}_p})$ be the Witt vectors of $\overline{\mathbb{F}_p}$, i.e. the ring of integers in the completion of the maximal unramified extension of $\mathbb{Q}_p$. Let $\mathcal{CLN}$ be the category of complete local Noetherian W-algebras with residue field $\overline{\mathbb{F}_p}$, and let $\mathrm{Def}(E_1, E_2, j) : \mathcal{CLN} \to \mathbf{Set}$ be the functor sending $R \in \mathcal{CLN}$ to the set of isomorphism classes of deformations of (E_1, E_2, j) to R, i.e. elliptic curves $\tilde{E}_i$ over R with complex multiplication by $\mathcal{O}_{K_i}$ whose reduction to $\overline{\mathbb{F}_p}$ is E_i and an isogeny $\tilde{\jmath} \in \mathrm{Hom}(\tilde{E}_1, \tilde{E}_2)$ whose reduction to $\overline{\mathbb{F}_p}$ is j.

We first want to reduce the computation of length $\mathcal{O}^{\mathrm{sh}}_{\mathcal{X}_\alpha, x}$ to a deformation-theoretic computation. In order to do so we first need to say what this object even is. For any algebraic stack $\mathcal{C}$ over $\mathrm{Spec}\,\mathbb{Z}$ and a geometric point $x \in \mathcal{C}(\overline{\mathbb{F}_p})$, define an étale neighborhood of x to be a commutative diagram of algebraic stacks

$$\begin{array}{ccc} & & U \\ & \overset{\tilde{x}}{\nearrow} & \downarrow \\ \mathrm{Spec}(\overline{\mathbb{F}_p}) & \xrightarrow{x} & \mathcal{C} \end{array}$$

where U is a scheme and the vertical arrow is étale. We define

$$\mathcal{O}^{\mathrm{sh}}_{\mathcal{C}, x} = \varinjlim_{(U, \tilde{x})} \mathcal{O}_{U, \tilde{x}}$$

where $(U, \tilde{x})$ ranges over all étale neighborhoods of x and $\mathcal{O}_{U,\tilde{x}}$ is the usual local ring of U at x. This is strictly Henselian and has residue field $\overline{\mathbb{F}_p}$, and its completion $\widehat{\mathcal{O}}^{\mathrm{sh}}_{\mathcal{C}, x}$ is naturally a W-algebra.

Proposition 1.1. *Fix $x = (E_1, E_2, j) \in \mathcal{X}_\alpha(\overline{\mathbb{F}_p})$. The deformation functor $\mathrm{Def}(E_1, E_2, j)$ is represented by $\widehat{\mathcal{O}}^{\mathrm{sh}}_{\mathcal{X}_\alpha, x}$.*

Thus in order to find the length of $\mathcal{O}^{\mathrm{sh}}_{\mathcal{X}_\alpha,x}$ (or equivalently its completion) it suffices to study the deformation functor $\mathrm{Def}(E_1, E_2, j)$.

Proof. Fix $R \in \mathcal{CLN}$, and $z \in \mathrm{Def}(E_1, E_2, j)(R)$. By definition this means that we have a point $z = (\tilde{E}_1, \tilde{E}_2, \tilde{\jmath}) \in \mathcal{X}_\alpha(R)$ such that the diagram

$$\begin{array}{ccc} \mathrm{Spec}(R) & & \\ \uparrow & \overset{z}{\searrow} & \\ \mathrm{Spec}(\overline{\mathbb{F}_p}) & \xrightarrow{x} & \mathcal{X}_\alpha \end{array}$$

commutes. Given an étale neighborhood

$$\begin{array}{ccc} & & U \\ & \overset{\tilde{x}}{\nearrow} & \downarrow \\ \mathrm{Spec}(\overline{\mathbb{F}_p}) & \xrightarrow{x} & \mathcal{X}_\alpha \end{array}$$

of x, since the morphism $U \to \mathcal{X}_\alpha$ is étale it is formally étale and so there exists a lifting $\tilde{z}$ of $z : \mathrm{Spec}(R) \to \mathcal{X}_\alpha$ to U, i.e. a morphism $\tilde{z} : \mathrm{Spec}(R) \to U$ making the diagram

$$\begin{array}{ccc} \mathrm{Spec}(R) & \xrightarrow{\tilde{z}} & U \\ \uparrow & \nearrow & \downarrow \\ \mathrm{Spec}(\overline{\mathbb{F}_p}) & \xrightarrow{x} & \mathcal{X}_\alpha \end{array}$$

commute. By abuse of notation we also write $\tilde{z}$ for the induced morphism $\mathcal{O}_{U,\tilde{x}} \to R$. Letting the étale neighborhood $(U, \tilde{x})$ vary, we get a morphism $\tilde{z} : \mathcal{O}^{\mathrm{sh}}_{\mathcal{X}_\alpha,x} \to R$, whose specialization to any $(U, \tilde{x})$ gives a diagram as above. In particular $\tilde{z}$ commutes with the reduction maps to $\overline{\mathbb{F}_p}$, i.e. it induces the identity map on residue fields, and so extends uniquely to a map $\widehat{\mathcal{O}}^{\mathrm{sh}}_{\mathcal{X}_\alpha,x} \to R$. Thus fixing $z \in \mathrm{Def}(E_1, E_2, j)(R)$ yields a ring homomorphism $\widehat{\mathcal{O}}^{\mathrm{sh}}_{\mathcal{X}_\alpha,x} \to R$, and so we get a map $\mathrm{Def}(E_1, E_2, j)(R) \to \mathrm{Hom}_{\mathcal{CLN}}(\widehat{\mathcal{O}}^{\mathrm{sh}}_{\mathcal{X}_\alpha,x}, R)$. On the other hand, given $\tilde{z} \in \mathrm{Hom}_{\mathcal{CLN}}(\widehat{\mathcal{O}}^{\mathrm{sh}}_{\mathcal{X}_\alpha,x}, R)$, composing with the natural map $\mathrm{Spec}\, \widehat{\mathcal{O}}^{\mathrm{sh}}_{\mathcal{X}_\alpha,x} \to \mathcal{X}_\alpha$ recovers z, giving an inverse to the map above. Therefore this is a bijection, and so $\widehat{\mathcal{O}}^{\mathrm{sh}}_{\mathcal{X}_\alpha,x}$ represents $\mathrm{Def}(E_1, E_2, j)$. □

It remains to analyze $\mathrm{Def}(E_1, E_2, j)$. We first need to introduce some more notation.

Thinking of E_1 and E_2 as algebraic groups over $\overline{\mathbb{F}_p}$, the action $t : E_i \to E_i$ of an element t of $\mathcal{O}_{K_i}$ on E_i yields an action $t : \mathrm{Lie}(E_i) \to \mathrm{Lie}(E_i)$ on the Lie algebra of E_i, which we write as $\kappa_i^{\mathrm{Lie}} : \mathcal{O}_{K_i} \to \mathrm{End}_{\overline{\mathbb{F}_p}}(\mathrm{Lie}(E_i))$. Since E_i is one-dimensional, $\mathrm{End}_{\overline{\mathbb{F}_p}}(\mathrm{Lie}(E_i)) \simeq \overline{\mathbb{F}_p}$, so the κ_i^{Lie} combine to a homomorphism $\kappa_K^{\mathrm{Lie}} : \mathcal{O}_K \simeq \mathcal{O}_{K_1} \otimes \mathcal{O}_{K_2} \to \overline{\mathbb{F}_p}$ sending $t_1 \otimes t_2 \mapsto \kappa_1^{\mathrm{Lie}}(t_1) \cdot \kappa_2^{\mathrm{Lie}}(t_2)$. The kernel of κ_K^{Lie} is a prime ideal of $\mathcal{O}_K$, which lies over some prime ideal $\mathfrak{p}$ of its real subfield F over p. Call this prime $\mathfrak{p}$ the *reflex prime* of the pair (E_1, E_2).

Let $\mathfrak{g}$ be the unique (up to isomorphism) one-dimensional p-divisible group of height 2 over $\overline{\mathbb{F}_p}$. Since E_1 and E_2 are supersingular, we can choose isomorphisms $E_1[p^\infty] \simeq \mathfrak{g} \simeq E_2[p^\infty]$.

Letting $\Delta = \mathrm{End}(\mathfrak{g})$, we conclude that Δ is the maximal order in the unique non-split quaternion algebra over $\mathbb{Q}_p$. Let $\mathfrak{m}_\Delta$ be the maximal ideal of Δ, and define a valuation ord_Δ by setting $\mathrm{ord}_\Delta(j) = k$ for a nonnegative integer k if and only if j is in $\mathfrak{m}_\Delta^k$ but not $\mathfrak{m}_\Delta^{k+1}$.

For any $\mathbb{Z}_p$-subalgebra $\mathcal{O}$ of Δ, we get an induced action $\mathcal{O} \hookrightarrow \Delta = \mathrm{End}(\mathfrak{g})$ of $\mathcal{O}$ on $\mathfrak{g}$. Let $\mathrm{Def}(\mathfrak{g}, \mathcal{O}) : \mathcal{CLN} \to \mathbf{Set}$ be the functor sending $R \in \mathcal{CLN}$ to the set of isomorphism classes of deformations of $\mathfrak{g}$ to R, with the action of $\mathcal{O}$. If L is a quadratic extension of $\mathbb{Q}_p$ with ring of integers $\mathcal{O}_L$ injecting into Δ, let $\mathcal{W}_L$ be the ring of integers in the completion of the maximal unramified extension of L, and fix a continuous ring homomorphism $W \to \mathcal{W}_L$. By Lubin-Tate theory $\mathcal{W}_L$ represents $\mathrm{Def}(\mathfrak{g}, \mathcal{O}_L)$.

Let $\mathfrak{G}$ be the universal deformation of $\mathfrak{g}$ to $\mathcal{W}_L$, equipped with an action of $\mathcal{O}_L$. For each positive integer k write $\mathfrak{G}_k$ for the reduction of $\mathfrak{G}$ to $\mathcal{W}_L/\pi_L^k\mathcal{W}_L$, where π_L is a uniformizer for L. It is a result of Gross [1, Proposition 3.3] that

$$\mathrm{End}(\mathfrak{G}_k) \simeq \mathcal{O}_L + p^{k-1}\Delta;$$

note that for $k = 1$, so that $\mathfrak{G}_k$ is just $\mathfrak{g}$, this gives Δ as desired (since $\mathcal{O}_L \subset \Delta$) and for $k = \infty$, so that $\mathfrak{G}_k = \mathfrak{G}$, this gives $\mathcal{O}_L$, i.e. the only endomorphisms which lift all the way to $\mathfrak{G}$ are those coming from the action of $\mathcal{O}_L$. In particular if $j \in \Delta$ is not in $\mathcal{O}_L$, there exists some integer k such that j lifts to an endomorphism of $\mathfrak{G}_k$, but not of $\mathfrak{G}_{k+1}$. Then $\mathrm{Def}(\mathfrak{g}, \mathcal{O}_L[j])$ is represented by $\mathcal{W}_L/\pi_L^k\mathcal{W}_L$, with universal deformation $\mathfrak{G}_k$.

Write $K_{i,p}$ for the completion of K_i at p. Let $\mathcal{O}_{L_i}$ be the image of $\mathcal{O}_{K_{i,p}}$ in Δ via the action of K_i on E_i and thus on $\mathfrak{g}$ via the chosen isomorphism $E_i[p^\infty] \simeq \mathfrak{g}$ (completed at p), and analogously write L_i for the fraction field of $\mathcal{O}_{L_i}$, so that $L_i \simeq K_{i,p}$.

Let $\mathrm{Def}(E_1, E_2) : \mathcal{CLN} \to \mathbf{Set}$ be the functor taking R to the set of isomorphism classes of deformations of (E_1, E_2) to R, i.e. deformations of elliptic curves to R equipped with the action of $\mathcal{O}_{K_1}$ and $\mathcal{O}_{K_2}$ respectively. Since there is no relation imposed between E_1 and E_2 and each has p-divisible group isomorphic to $\mathfrak{g}$, with the action of $\mathcal{O}_{K_i}$ corresponding to the action of $\mathcal{O}_{L_i}$ on $\mathfrak{g}$, by the Serre-Tate theorem we have

$$\mathrm{Def}(E_1, E_2) \simeq \mathrm{Def}(\mathfrak{g}, \mathcal{O}_{L_1}) \times \mathrm{Def}(\mathfrak{g}, \mathcal{O}_{L_2}),$$

which as above is represented by the (derived) tensor product $\mathcal{W}_{L_1} \widehat{\otimes}_W \mathcal{W}_{L_2}$.

Suppose first for simplicity that p is unramified in both K_1 and K_2. Recall that $\deg_{\mathrm{CM}}$ is an F-quadratic form on $V = \mathrm{Hom}(E_1, E_2) \otimes \mathbb{Q}$, and that the reflex prime $\mathfrak{p}$ is a prime ideal of F.

Proposition 1.2. *If p is unramified in K_1 and K_2, the deformation functor $\mathrm{Def}(E_1, E_2, j)$ is represented by a local Artinian W-algebra of length*

$$\frac{\mathrm{ord}_\mathfrak{p}(\deg_{\mathrm{CM}}(j)) + 1}{2}.$$

Proof. Since p is unramified in both K_1 and K_2, both fields $K_{i,p}$ are unramified quadratic extensions of $\mathbb{Q}_p$ and therefore isomorphic to $\mathbb{Q}_{p^2}$, and in particular we can choose the isomorphisms $E_i[p^\infty] \simeq \mathfrak{g}$ such that the images of $\mathcal{O}_{K_{i,p}}$ in Δ are the same; this image is the ring of integers of $\mathbb{Q}_{p^2}$, which we denote $\mathbb{Z}_{p^2}$. Thus in this case $L = \mathbb{Q}_{p^2}$ and $\mathcal{O}_L = \mathbb{Z}_{p^2}$. Note that therefore the maximal unramified extension of L is the same as that of $\mathbb{Q}_p$, and so

$\mathcal{W}_L = W$. Therefore W represents the functor $\mathrm{Def}(\mathfrak{g}, \mathbb{Z}_{p^2})$, and so $\mathrm{Def}(E_1, E_2)$ is represented by $W \widehat{\otimes}_W W = W$. The universal deformation of (E_1, E_2) therefore has p-divisible group $(\mathfrak{G}, \mathfrak{G})$, and the universal deformation of (E_1, E_2, j) corresponds to $(\mathfrak{G}_k, \mathfrak{G}_k, \tilde{j})$ for the largest k such that j lifts to an endomorphism $\tilde{j}$ of $\mathfrak{G}_k$, and so $\mathrm{Def}(E_1, E_2, j)$ is represented by $W/p^k W$. This is a local Artinian W-algebra of length k; thus it remains only to compute this maximal k.

Writing ι for the canonical involution on Δ, we can choose a uniformizer Π such that $u\Pi = \Pi\iota(u)$ for every $u \in \mathbb{Z}_{p^2}$. In fact Δ is a free left $\mathbb{Z}_{p^2}$-module via left multiplication, and since it is rank 4 over $\mathbb{Z}_p$ it is rank 2 over $\mathbb{Z}_{p^2}$; therefore we can write

$$\Delta = \Delta_+ \oplus \Delta_-$$

where $\Delta_+ = \mathbb{Z}_{p^2}$ and $\Delta_- = \mathbb{Z}_{p^2}\Pi$. Let $\mathcal{O}_{K,p}$ be the ring of integers of the completion K_p of K at p, and define two functions $f_\pm : \mathcal{O}_{K,p} \to \mathbb{Z}_{p^2}$ by

$$f_+(t_1 \otimes t_2) = \kappa_1(\overline{t_1})\kappa_2(t_2),$$

$$f_-(t_1 \otimes t_2) = \kappa_1(t_1)\kappa_2(t_2),$$

where $t_1 \mapsto \overline{t_1}$ is the involution on K_1 given by complex conjugation. Their product $\Psi := f_+ \times f_-$ gives an isomorphism $\mathcal{O}_{K,p} \simeq \mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2}$.

Since F is a quadratic extension of $\mathbb{Q}$, there are two primes of F over p, one of which is the reflex prime $\mathfrak{p}$; set $\mathfrak{p}_- = \mathfrak{p}$ and call the other prime $\mathfrak{p}_+$. Then $f_\pm$ factors through completion at $\mathfrak{p}_\pm$. Via the inclusion of $\mathcal{O}_K$ into its completions, we get an action of $\mathcal{O}_K$ on Δ via $t \bullet j = f_+(t)j_+ + f_-(t)j_-$ where $j = j_+ + j_-$ is the decomposition of j via $\Delta = \Delta_+ \oplus \Delta_-$ as above. In fact after unwinding the definitions and various isomorphisms this is the same action as that defined in the introduction on $V(E_1, E_2)$. In this form, we can write $\deg_{\mathrm{CM}}$ (now completed at p) explicitly as

$$\deg_{\mathrm{CM}}(j) = \Psi^{-1}(\deg(j_+), \deg(j_-))$$

since taking the trace down to $\mathbb{Q}$ on the right-hand side gives $\deg(j_+ + j_-) = \deg(j)$.

Taking ord_p of both sides gives

$$\mathrm{ord}_p(\deg_{\mathrm{CM}}(j)) = \mathrm{ord}_p(\deg(j_+)) + \mathrm{ord}_p(\deg(j_-)),$$

and the left-hand side decomposes into $\mathrm{ord}_{\mathfrak{p}_+}(\deg_{\mathrm{CM}}(j)) + \mathrm{ord}_{\mathfrak{p}_-}(\deg_{\mathrm{CM}}(j))$. Since $f_\pm$ factors through completion at $\mathfrak{p}_\pm$, we can further identify terms

$$\mathrm{ord}_{\mathfrak{p}_+}(\deg_{\mathrm{CM}}(j)) = \mathrm{ord}_p(\deg(j_+)),$$

$$\mathrm{ord}_{\mathfrak{p}_-}(\deg_{\mathrm{CM}}(j)) = \mathrm{ord}_p(\deg(j_-)).$$

As above, we know in this case that $j \in \Delta$ lifts to an endomorphism of $\mathfrak{G}_k$ if and only if it is in $\mathbb{Z}_{p^2} + p^{k-1}\Delta$. Since we decompose Δ into $\mathbb{Z}_{p^2} \oplus \mathbb{Z}_{p^2}\Pi$, writing $j = j_+ + j_-$ for this decomposition we have $j \in \mathbb{Z}_{p^2} + p^{k-1}\Delta$ if and only if $j_- \in p^{k-1}\mathbb{Z}_{p^2}\Pi$. Taking degrees, since multiplication by p has degree p^2 and Π has degree p this is equivalent to $\mathrm{ord}_p(\deg(j_-)) \geq 2k - 1$, which by the above is equivalent to

$$\frac{\mathrm{ord}_{\mathfrak{p}}(\deg_{\mathrm{CM}}(j)) + 1}{2} \geq k,$$

where $\mathfrak{p} = \mathfrak{p}_-$ is the reflex prime. Therefore the greatest k such that j lifts to an endomorphism of $\mathfrak{G}_k$ is given by the left-hand side of this inequality. Combined with the observations above, this yields the result. □

In the ramified case, we get a slightly more complicated formula. Recall that since the discriminants of K_1 and K_2 are coprime, p is ramified in at most one of K_1 and K_2. Let $\mathfrak{D}$ be the different ideal of $F/\mathbb{Q}$, which is generated by the square root of the discriminant $\sqrt{D} = \sqrt{d_1 d_2}$.

Proposition 1.3. *If p is ramified in one of K_1 and K_2, the deformation functor $\mathrm{Def}(E_1, E_2, j)$ is represented by a local Artinian W-algebra of length*

$$\frac{\mathrm{ord}_{\mathfrak{p}}(\deg_{\mathrm{CM}}(j)) + \mathrm{ord}_{\mathfrak{p}}(\mathfrak{D}) + 1}{2}.$$

The proof is not totally analogous, but we'll skip it for now anyway (I may add it later).

Combining Propositions 1.2 and 1.3 with Proposition 1.1, we immediately get an expression for length $\mathcal{O}^{\mathrm{sh}}_{\mathcal{X}_\alpha, x}$ as desired.

Corollary 1.4. *Let $x = (E_1, E_2, j) \in \mathcal{X}_\alpha(\overline{\mathbb{F}_p})$, and let $\mathfrak{p}$ be the reflex prime of (E_1, E_2). Then we have*

$$\text{length } \mathcal{O}^{\mathrm{sh}}_{\mathcal{X}_\alpha, x} = \frac{\mathrm{ord}_{\mathfrak{p}}(\alpha\mathfrak{D}) + 1}{2}.$$

Proof. This follows immediately from the propositions above upon observing that in the unramified case $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{D}) = 0$ and since by assumption $x \in \mathcal{X}_\alpha(\overline{\mathbb{F}_p})$ we have $\deg_{\mathrm{CM}}(j) = \alpha$. □

We claimed in the introduction that we would get a formula for length $\mathcal{O}^{\mathrm{sh}}_{\mathcal{X}_\alpha, x}$ which does not depend on x. Corollary 1.4 almost satisfies this requirement: there is no dependence on j, but there is an implicit dependence on the pair (E_1, E_2) in that the formula depends on the reflex prime $\mathfrak{p}$ of this pair. But in fact for each p every element of $\mathcal{X}_\alpha(\overline{\mathbb{F}_p})$ has the same reflex prime $\mathfrak{p}$, which is the unique prime of F such that $\chi_{\mathfrak{p}}(\alpha\mathfrak{D}) = -1$ where χ is the Hecke character associated to the quadratic extension K/F and $\chi_{\mathfrak{p}}$ is its local factor at $\mathfrak{p}$. In fact there is only one prime p such that $\mathcal{X}_\alpha(\overline{\mathbb{F}_p})$ is nonempty. We will not prove either assertion, though, at least for now.

We'll need one final lemma for the final formula, which we include in this section as its proof is deformation-theoretic. Let $\Gamma = \mathrm{Cl}(K_1) \times \mathrm{Cl}(K_2)$ be the product of the class groups of K_1 and K_2.

Lemma 1.5. *Fix a prime $\mathfrak{p}$ of F over p. There are $2 \cdot |\Gamma|$ isomorphism classes of pairs (E_1, E_2) of elliptic curves over $\overline{\mathbb{F}_p}$ with respective actions by $\mathcal{O}_{K_i}$ such that the reflex prime of (E_1, E_2) is $\mathfrak{p}$.*

Proof. First assume p is unramified in both K_1 and K_2. Then $\mathrm{Def}(E_1, E_2)$ is represented by $W \widehat{\otimes}_W W = W$, and so for any W-algebra $R \in \mathcal{CLN}$ the only map $W \to R$ in $\mathcal{CLN}$ is the structure map and therefore $\mathrm{Hom}_{\mathcal{CLN}}(W, R) \simeq \mathrm{Def}(E_1, E_2)(R)$ consists of a single element, i.e. (E_1, E_2) lifts uniquely to R. In particular taking $R = \mathbb{C}_p := \widehat{\overline{\mathbb{Q}_p}}$ we get a bijection between isomorphism classes of pairs (E_1, E_2) over $\mathbb{C}_p$ and over $\overline{\mathbb{F}_p}$. By the theory of

complex multiplication, for each embedding of K_i into $\mathbb{C}_p$ there are $\mathrm{Cl}(K_i)$ elliptic curves over $\mathbb{C}_p$ with complex multiplication by $\mathcal{O}_{K_i}$, and so in total there are $4\cdot|\mathrm{Cl}(K_1)|\cdot|\mathrm{Cl}(K_2)| = 4\cdot|\Gamma|$ isomorphism classes of pairs over $\mathbb{C}_p$, and thus over $\overline{\mathbb{F}_p}$. Exactly half of these will have reflex prime $\mathfrak{p}$, as can be seen for example by the following involution: if $\kappa_2 : \mathcal{O}_{K_2} \hookrightarrow \mathrm{End}(E_2)$ is the action morphism, define κ_2' by precomposing with the involution on $\mathcal{O}_{K_2}$ given by complex conjugation. Then writing E_2' for the elliptic curve E_2 with this new action κ_2', the pair (E_1, E_2') has the opposite reflex prime from (E_1, E_2). This completes the proof in the unramified case.

If p is ramified in one of K_1 and K_2 (say K_1), then similarly $\mathrm{Def}(E_1, E_2)$ is represented by $\mathcal{W}_{L_1}\widehat{\otimes}_W W = \mathcal{W}_{L_1}$ where L_1 is the fraction field of the image of $\mathcal{O}_{K_{1,p}}$, so as above L_1 is isomorphic to $K_{1,p}$. This time $\mathrm{Hom}_{\mathcal{CLN}}(\mathcal{W}_{L_1}, R)$ consists of two elements (for R sufficiently large), corresponding to the two elements of $\mathrm{Aut}(\mathcal{W}_{L_1}/W)$. Therefore there are exactly two deformations of (E_1, E_2) to $\mathbb{C}_p$, and so there is a two-to-one map from isomorphism classes of pairs over $\mathbb{C}_p$ to pairs over $\overline{\mathbb{F}_p}$ given by reduction. Since there are still $4\cdot|\Gamma|$ classes over $\mathbb{C}_p$, it follows that there are $2\cdot|\Gamma|$ pairs over $\overline{\mathbb{F}_p}$. Since p is ramified in K_1, it is ramified in F, and so $p\mathcal{O}_F = \mathfrak{p}^2$; thus the only prime of F over p is $\mathfrak{p}$, so all pairs (E_1, E_2) have reflex primes $\mathfrak{p}$, which combined with the above gives the result. □

2. Decomposition into orbital integrals

Recall that our goal is to compute the degree

$$\deg \mathcal{X}_\alpha = \sum_p \log(p) \sum_{x\in[\mathcal{X}_\alpha(\overline{\mathbb{F}_p})]} \frac{\mathrm{length}\,\mathcal{O}^{\mathrm{sh}}_{\mathcal{X}_\alpha,x}}{\mathrm{Aut}(x)}.$$

In the previous section we found a formula for $\mathrm{length}\,\mathcal{O}^{\mathrm{sh}}_{\mathcal{X}_\alpha,x}$, independent of x; thus it remains only to compute

$$\sum_{x\in[\mathcal{X}_\alpha(\overline{\mathbb{F}_p})]} \frac{1}{\mathrm{Aut}(x)}.$$

Let $w_i = |\mathcal{O}_{K_i}^\times|$, which since K_i is imaginary quadratic is just the number of roots of unity of K_i.

Proposition 2.1. *For each $x \in \mathcal{X}_\alpha(\overline{\mathbb{F}_p})$, we have $|\mathrm{Aut}(x)| = w_1w_2$.*

Proof. Write $x = (E_1, E_2, j)$. Since each E_i is supersingular, its endomorphism ring is the maximal order of a quaternion algebra and contains an order isomorphic to $\mathcal{O}_{K_i}$. However, automorphisms of x must preserve the $\mathcal{O}_{K_i}$ action on E_i, and so we can restrict to the $\mathcal{O}_{K_i}$-linear endomorphisms of E_i, which are just $\mathcal{O}_{K_i}$; therefore the automorphisms are $\mathcal{O}_{K_i}^\times$. Therefore the set of automorphisms of the pair (E_1, E_2) preserving the complex multiplication on each has order w_1w_2.

Every automorphism of x must induce one of these w_1w_2 automorphisms of (E_1, E_2). The only automorphism of j is the identity; the result follows immediately. □

Thus in order to compute $\deg \mathcal{X}_\alpha$ it suffices to count the isomorphism classes of $\mathcal{X}_\alpha(\overline{\mathbb{F}_p})$. We can do this as follows. We have

$$|[\mathcal{X}_\alpha(\overline{\mathbb{F}_p})]| = \sum_{(E_1,E_2)} \sum_{\substack{j\in \mathrm{Hom}(E_1,E_2)\\ \deg_{\mathrm{CM}}(j)=\alpha}} 1$$

where the first sum is over isomorphism classes of pairs (E_1, E_2) over $\overline{\mathbb{F}_p}$. Write $L(\alpha, E_1, E_2)$ for the set of isogenies $j : E_1 \to E_2$ with $\deg_{\mathrm{CM}}(j) = \alpha$. Recall that we have an action of $\Gamma = \mathrm{Cl}(K_1) \times \mathrm{Cl}(K_2)$ on the set of isomorphism classes of pairs (E_1, E_2); write $\Gamma \cdot L(\alpha, E_1, E_2)$ for the union of $L(\alpha, \gamma_1 \cdot E_1, \gamma_2 \cdot E_2)$ for $(\gamma_1, \gamma_2) \in \Gamma$. Since there are exactly two orbits of this action and there is a bijection between them preserving the number of isogenies, as per Lemma 1.5 and its proof, we have

$$|[\mathcal{X}_\alpha(\overline{\mathbb{F}_p})]| = 2|\Gamma \cdot L(\alpha, E_1, E_2)|$$

for any pair (E_1, E_2). The key observation is that we can write Γ as an adelic quotient, and this will allow us to factor $|\Gamma \cdot L(\alpha, E_1, E_2)|$ as a product of orbital integrals.

We need a lot of notation. For any $\mathbb{Q}$-algebra A, set $T_i(A) = (K_i \otimes_{\mathbb{Q}} A)^\times$. This inherits an action of complex conjugation from K_i and thus a norm $\nu_i : T_i(A) \to A^\times$ by $\nu_i(t) = t\bar{t}$. We define $T(A)$ to be the product of the $T_i(A)$ along these maps, i.e. $T(A) \subset T_1(A) \times T_2(A)$ consists of pairs (t_1, t_2) such that $\nu_1(t_1) = \nu_2(t_2)$. Since ν_1 and ν_2 agree on $T(A)$, we can define a single norm $\nu : T(A) \to A^\times$ by $\nu(t_1, t_2) = \nu_1(t_1) = \nu_2(t_2)$. We similarly define $S(A)$ to be the subgroup of $(K \otimes_{\mathbb{Q}} A)^\times$ consisting of elements z such that $\mathrm{Nm}_{K/F}(z) = 1$. This gives a map $\eta : T(A) \to S(A)$ by $(t_1, t_2) \mapsto \frac{1}{\nu(t_1,t_2)} t_1 \otimes_A t_2$, since $\mathrm{Nm}(t_1 \otimes_A t_2) = \nu(t_1, t_2)$.

Specializing to the case of the finite adeles $\mathbb{A}_f$ over $\mathbb{Q}$, for each number field L write $\widehat{\mathcal{O}}_L = \prod_w \mathcal{O}_{L_w}$ for the ring of integers of the finite adeles $\mathbb{A}_{L,f}$ over L and set

$$U = T(\mathbb{A}_f) \cap (\widehat{\mathcal{O}}_{K_1} \times \widehat{\mathcal{O}}_{K_2}),$$

so U consists of pairs (t_1, t_2) with $t_i \in K_i \otimes_{\mathbb{Q}} \mathbb{A}_f \cap \widehat{\mathcal{O}}_{K_i}$ such that $\nu_1(t_1) = \nu_2(t_2)$. Let V be the image of U under $\eta : T(\mathbb{A}_f) \to S(\mathbb{A}_f)$. Observe that

$$U = \prod_\ell U_\ell, \qquad V = \prod_\ell V_\ell$$

for U_ℓ compact open subgroups of $T(\mathbb{Q}_\ell)$ and similarly for V_ℓ.

We have a short exact sequence

$$1 \to \mathbb{A}_f^\times \to T(\mathbb{A}_f) \xrightarrow{\eta} S(\mathbb{A}_f) \to 1,$$

essentially by Hilbert's Theorem 90, and the same holds upon replacing $\mathbb{A}_f$ by $\mathbb{Q}_\ell$ for any prime ℓ. Thus we can think of $S(\mathbb{A}_f)$ as $T(\mathbb{A}_f)/\mathbb{A}_f^\times$. Via the inclusion $\mathbb{A}_f^\times \hookrightarrow T(\mathbb{Q})U$, it follows that $T(\mathbb{Q})\backslash T(\mathbb{A}_f)/U$ is isomorphic to $S(\mathbb{Q})\backslash S(\mathbb{A}_f)/V$.

We have a homomorphism $T(\mathbb{A}_f) \to \Gamma$ sending (t_1, t_2) to their images in $K_i^\times \backslash \mathbb{A}_{K_i,f}^\times / \mathcal{O}_{K_i}$, which is just the adelic form of the class group. Since $K_i^\times = (K_i \otimes_{\mathbb{Q}} \mathbb{Q})^\times = T_i(\mathbb{Q})$, this descends to a map $T(\mathbb{Q})\backslash T(\mathbb{A}_f)/U \to \Gamma$; in fact this induced map is an isomorphism, though we'll again skip the proof.

Recall that $L(\alpha, E_1, E_2)$ is the set of isogenies $j : E_1 \to E_2$ with $\deg_{\mathrm{CM}}(j) = \alpha$. We can extend $\deg_{\mathrm{CM}}$ to $V(E_1, E_2) := \mathrm{Hom}(E_1, E_2) \otimes \mathbb{Q}$, $L_\ell(E_1, E_2) = \mathrm{Hom}(E_1, E_2) \otimes \mathbb{Z}_\ell$, and $V_\ell(E_1, E_2) = \mathrm{Hom}(E_1, E_2) \otimes \mathbb{Q}_\ell$ for each prime ℓ, and we set $V(\alpha, E_1, E_2)$ to be the set of quasi-isogenies j in $\mathrm{Hom}(E_1, E_2) \otimes \mathbb{Q}$ with $\deg_{\mathrm{CM}}(j) = \alpha$ and similarly for $L_\ell(\alpha, E_1, E_2)$ and $V_\ell(\alpha, E_1, E_2)$. Then $T(\mathbb{Q})$ acts on $L(\alpha, E_1, E_2)$ by $(t_1, t_2) \bullet j = \kappa_2(t_2) \circ j \circ \kappa_1(t_1)^{-1}$, and this action extends to $V(\alpha, E_1, E_2)$. Similarly we get an action of $T(\mathbb{Q}_\ell)$ on $V_\ell(\alpha, E_1, E_2)$, which is transitive for each ℓ.

We can now define orbital integrals. For each prime ℓ, if $V_\ell(\alpha, E_1, E_2)$ is nonempty then choose an element j and set

$$\mathrm{O}_\ell(\alpha, E_1, E_2) = \sum_{t \in \mathbb{Q}_\ell^\times \backslash T(\mathbb{Q}_\ell)/U_\ell} \mathbf{1}_{L_\ell(E_1, E_2)}(t^{-1} \bullet j),$$

and set $\mathrm{O}_\ell(\alpha, E_1, E_2) = 0$ if $V_\ell(\alpha, E_1, E_2)$ is empty. Here $\mathbf{1}_{L_\ell(\alpha, E_1, E_2)}$ is the indicator function as usual. Note that since $T(\mathbb{Q}_\ell)$ acts transitively on $V_\ell(\alpha, E_1, E_2)$ the orbital integral does not depend on the choice of j.

The main utility of orbital integrals in this case is given by the following proposition.

Proposition 2.2. *We have*

$$|\Gamma \cdot L(\alpha, E_1, E_2)| = \frac{w_1 w_2}{2} \prod_\ell \mathrm{O}_\ell(\alpha, E_1, E_2).$$

Combined with the discussion above, it follows that $|[\mathcal{X}_\alpha(\overline{\mathbb{F}_p})]| = w_1 w_2 \prod_\ell \mathrm{O}_\ell(\alpha, E_1, E_2)$ for any fixed pair (E_1, E_2).

A first observation is that the left-hand side depends only on the Γ-orbit of (E_1, E_2) and not on the particular choice, whereas this is not obvious for the right-hand side. However recalling the isomorphism $T(\mathbb{Q})\backslash T(\mathbb{A}_f)/U \to \Gamma$ we can think of the action of Γ on (E_1, E_2) as a shift by an element of $T(\mathbb{A}_f)$, which does not affect the result.

Proof of Proposition 2.2. We have

$$|\Gamma \cdot L(\alpha, E_1, E_2)| = \sum_{(\gamma_1, \gamma_2) \in \Gamma} |L(\alpha, \gamma_1 \cdot E_1, \gamma_2 \cdot E_2)| = \sum_{(\gamma_1, \gamma_2) \in \Gamma} \sum_{j \in V(\alpha, \gamma_1 \cdot E_1, \gamma_2 \cdot E_2)} \mathbf{1}_{L(E_1, E_2)}(j).$$

If $V(\alpha, E_1, E_2)$ is empty, then this will be 0, and indeed in this case at least one $V_\ell(\alpha, E_1, E_2)$ will be empty and so both sides are 0. Therefore we can assume that there exists some $j \in V(\alpha, E_1, E_2)$. Recalling the isomorphisms $\Gamma \simeq T(\mathbb{Q})\backslash T(\mathbb{A}_f)/U \simeq S(\mathbb{Q})\backslash S(\mathbb{A}_f)/V$ and

the fact that $S(\mathbb{Q}) = K^\times = (K_1 \otimes_{\mathbb{Q}} K_2)^\times$ acts transitively on $V(\alpha, E_1, E_2)$, fixing j we have

$$\begin{aligned}
|\Gamma \cdot L(\alpha, E_1, E_2)| &= \sum_{s \in S(\mathbb{Q})\backslash S(\mathbb{A}_f)/V} \sum_{t \in S(\mathbb{Q})} \mathbf{1}_{s \bullet L(E_1,E_2)}(t^{-1} \bullet j) \\
&= |S(\mathbb{Q}) \cap V| \sum_{s \in S(\mathbb{A}_f)/V} \mathbf{1}_{s \bullet L(E_1,E_2)}(j) \\
&= |S(\mathbb{Q}) \cap V| \prod_\ell \sum_{s \in S(\mathbb{Q}_\ell)/V_\ell} \mathbf{1}_{s \bullet L_\ell(E_1,E_2)}(j) \\
&= |S(\mathbb{Q}) \cap V| \prod_\ell \sum_{t \in \mathbb{Q}_\ell^\times \backslash T(\mathbb{Q}_\ell)/U_\ell} \mathbf{1}_{L_\ell(E_1,E_2)}(t^{-1} \bullet j) \\
&= |S(\mathbb{Q}) \cap V| \prod_\ell \mathrm{O}_\ell(\alpha, E_1, E_2)
\end{aligned}$$

where $s \bullet L(E_1, E_2) = L(E_1', E_2')$ where $(E_1', E_2') = s \cdot (E_1, E_2)$ via the isomorphism

$$S(\mathbb{Q})\backslash S(\mathbb{A}_f)/V \simeq \Gamma,$$

which factors at each ℓ to the inverse action of $S(\mathbb{Q}_\ell)$ on $V_\ell(E_1, E_2)$. The second-to-last equality is via the identification of $S(\mathbb{Q}_\ell)$ with $\mathbb{Q}_\ell^\times \backslash T(\mathbb{Q}_\ell)$. Finally we have a map $T(\mathbb{Q}) \cap U \to S(\mathbb{Q}) \cap V$ given by restricting η, and we know that the kernel of this map is $\mathbb{Q}^\times \cap U = \mathbb{Z}^\times = \{\pm 1\}$, so $|S(\mathbb{Q}) \cap V| \geq \frac{1}{2}|T(\mathbb{Q}) \cap U|$ (since we don't know that this map is surjective). By definition $T(\mathbb{Q}) \cap U = \mathcal{O}_{K_1}^\times \times \mathcal{O}_{K_2}^\times$ and so it has $w_1 w_2$ elements, i.e. $|S(\mathbb{Q}) \cap V| \geq \frac{1}{2} w_1 w_2$; on the other hand $S(\mathbb{Q}) \cap V \subset S(\mathbb{Q}) \cap \widehat{\mathcal{O}}_K^\times$ is bounded by the roots of unity of K, of which there are $\frac{1}{2} w_1 w_2$. Together with the above this completes the proof. □

Combining this with the previous section and the discussion opening this section, we have the formula

$$\deg \mathcal{X}_\alpha = \frac{1}{2} \sum_p \log(p) \operatorname{ord}_{\mathfrak{p}}(\alpha \mathfrak{p} \mathfrak{D}) \prod_\ell \mathrm{O}_\ell(\alpha, E_1, E_2)$$

where (E_1, E_2) is a fixed pair of elliptic curves over $\overline{\mathbb{F}_p}$ with respective complex multiplication by $\mathcal{O}_{K_1}$ and $\mathcal{O}_{K_2}$ and reflex prime $\mathfrak{p}$. (Here we've contracted $\operatorname{ord}_{\mathfrak{p}}(\alpha\mathfrak{D}) + 1$ to $\operatorname{ord}_{\mathfrak{p}}(\alpha\mathfrak{p}\mathfrak{D})$ purely for notational convenience.) It remains only to compute the orbital integrals.

3. Computation of orbital integrals

With notation as above, fix a pair (E_1, E_2) over $\overline{\mathbb{F}_p}$ with reflex prime $\mathfrak{p}$ and $\alpha \in F^\times$. For each prime ℓ, let $\mathfrak{D}_\ell$ be the local different ideal of $F_\ell/\mathbb{Q}$ and for each fractional ideal $\mathfrak{b}$ of F_ℓ define $\rho_\ell(\mathfrak{b})$ to be the number of ideals $\mathfrak{B}$ of K_ℓ such that $\mathrm{Nm}_{K/F}(\mathfrak{B}) = \mathfrak{b}$.

Proposition 3.1. *For every $\ell \neq p$, we have*

$$\mathrm{O}_\ell(\alpha, E_1, E_2) = \rho_\ell(\alpha \mathfrak{D}_\ell).$$

Proof. Since $V(E_1, E_2)$ has dimension 4 as a $\mathbb{Q}$-module, it has dimension 1 as a K-module and so is isomorphic to K, and analogously $V_\ell(E_1, E_2) \simeq K_\ell$. We will not prove this, but it is true that there exists some $\beta \in \mathbb{A}_{F,f}^\times$ such that $\beta\widehat{\mathcal{O}}_F = \mathfrak{p}\mathfrak{D}^{-1}\widehat{\mathcal{O}}_F$ and the degree F-form $\deg_{\mathrm{CM}}$ on $V_\ell(E_1, E_2)$ corresponds to $\mathrm{Nm}_{K_\ell/F_\ell}$ times the local component β_ℓ on K_ℓ. Thus if $j \in V_\ell(E_1, E_2)$ corresponds to $\phi \in K_\ell$, the condition $\deg_{\mathrm{CM}}(j) = \alpha$ is equivalent to $\beta_\ell \cdot \mathrm{Nm}_{K_\ell/F_\ell}(\phi) = \alpha$. Thus $V_\ell(\alpha, E_1, E_2)$ is nonempty if and only if there exists some $\phi \in K_\ell$ with $\mathrm{Nm}_{K_\ell/F_\ell}(\phi) = \alpha\beta_\ell^{-1}$, and thus if and only if $\rho_\ell(\alpha\mathfrak{D}_\ell^{-1}) > 0$ since the ℓ-component of $\mathfrak{p}\mathfrak{D}^{-1}\widehat{\mathcal{O}}_F$ is just $\mathfrak{D}_\ell^{-1}$ at $\ell \neq p$. Therefore we can assume that both sides are nonzero.

As in the proof of Proposition 1.5, we can rewrite $\mathrm{O}_\ell(\alpha, E_1, E_2)$ as

$$\sum_{s \in S(\mathbb{Q}_\ell)/V_\ell} \mathbf{1}_{L_\ell(E_1,E_2)}(s^{-1} \bullet j)$$

for some representative $j \in V_\ell(\alpha, E_1, E_2)$. If j corresponds to ϕ, then this can be rewritten as

$$\sum_{s \in S(\mathbb{Q}_\ell)/V_\ell} \mathbf{1}_{\mathcal{O}_{K_\ell}}(s^{-1}\phi)$$

where the action of $S(\mathbb{Q}_\ell) = (K \otimes_{\mathbb{Q}} \mathbb{Q}_\ell)^\times = K_\ell^\times$ on K_ℓ is by multiplication.

We then need to examine the various cases depending on whether ℓ is inert, split, or ramified in each of K_1 and K_2. We will not do this in full, but just the simplest case where ℓ is inert in both K_1 and K_2; in this case $\mathcal{O}_{K_\ell} \simeq \mathbb{Z}_{\ell^2} \times \mathbb{Z}_{\ell^2}$, so in particular $S(\mathbb{Q}_\ell)/V_\ell \simeq \mathbb{Q}_\ell^\times \backslash T(\mathbb{Q}_\ell)/U_\ell$ is trivial. Therefore $\mathrm{O}_\ell(\alpha, E_1, E_2)$ is 1 if there exists some $\phi \in K_\ell$ with norm $\alpha\beta_\ell^{-1}$, i.e. $\rho_\ell(\alpha\mathfrak{D}_\ell^{-1}) \geq 1$; on the other hand since ℓ is inert in K_1 and K_2 there is at most one ideal of K with norm $\alpha\mathfrak{D}_\ell^{-1}$, so both sides are 1 in this case and 0 otherwise.

The remaining, more complicated cases are left to the reader (and are covered in [3]). In particular the case where ℓ is inert in one of the K_i and ramified in the other is essentially identical. □

Proposition 3.2. *At $\ell = p$, we have*

$$\mathrm{O}_p(\alpha, E_1, E_2) = \rho_p(\alpha\mathfrak{p}^{-1}\mathfrak{D}_p).$$

Proof. The argument is the same as in Proposition 3.1; in particular, p is either inert in both K_1 and K_2 or inert in one of them and ramified in the other, so the argument included in the proof above applies here. The only difference is that the existence of ϕ such that $\mathrm{Nm}_{K_p/F_p}(\phi) = \alpha\beta_p^{-1}$ is now equivalent to $\rho_p(\alpha\mathfrak{p}^{-1}\mathfrak{D}_p)$ rather than $\rho_\ell(\alpha\mathfrak{D}_\ell)$, since the local factor of $\beta\widehat{\mathcal{O}}_F = \mathfrak{p}\mathfrak{D}^{-1}\widehat{\mathcal{O}}_F$ at p is now $\mathfrak{p}\mathfrak{D}_p^{-1}$ instead of just $\mathfrak{D}_\ell^{-1}$. Incorporating this difference gives the desired formula. □

For any fractional ideal $\mathfrak{b}$ of F, define $\rho(\mathfrak{b})$ to be the number of ideals $\mathfrak{B}$ of K such that $\mathrm{Nm}_{K/F}(\mathfrak{B}) = \mathfrak{b}$. In particular we have

$$\rho(\mathfrak{b}) = \prod_\ell \rho_\ell(\mathfrak{b}_\ell),$$

where $\mathfrak{b}_\ell = \mathfrak{b}\mathcal{O}_{F_\ell}$. Therefore Propositions 3.1 and 3.2 together imply the following corollary.

Corollary 3.3. *We have*

$$\prod_{\ell} \mathrm{O}_\ell(\alpha, E_1, E_2) = \rho(\alpha \mathfrak{p}^{-1}\mathfrak{D}).$$

Combining this with the results of the previous section, we obtain our final formula:

Corollary 3.4. *For each prime p, let $\mathfrak{p}$ be the unique prime of F over p which is the reflex prime of a pair (E_1, E_2) of elliptic curves over $\overline{\mathbb{F}_p}$ with complex multiplication by $\mathcal{O}_{K_1}$ and $\mathcal{O}_{K_2}$ respectively. Then for each totally positive $\alpha \in F^\times$ we have*

$$\deg \mathcal{X}_\alpha = \frac{1}{2} \sum_p \log(p) \operatorname{ord}_{\mathfrak{p}}(\alpha \mathfrak{p}\mathfrak{D}) \rho(\alpha \mathfrak{p}^{-1}\mathfrak{D}).$$

Note that we can assume that α is totally positive since otherwise $\mathcal{X}_\alpha$ will be empty, since $\deg_{\mathrm{CM}}$ is totally positive.

The only thing left is to relate this to the original formula of Gross and Zagier for singular moduli. Recall that the stacks $\mathcal{T}_m$ classify triples (E_1, E_2, j) with (E_1, E_2) as above and $j : E_1 \to E_2$ is an isogeny satisfying $\deg(j) = m$. We have the decomposition

$$\mathcal{T}_m = \bigsqcup_{\substack{\alpha \in F^\times \\ \mathrm{Tr}_{F/\mathbb{Q}}(\alpha) = m}} \mathcal{X}_\alpha$$

and so

$$\deg \mathcal{T}_m = \sum_{\substack{\alpha \in F^\times \\ \mathrm{Tr}_{F/\mathbb{Q}}(\alpha) = m}} \deg \mathcal{X}_\alpha,$$

which by Corollary 3.4 is

$$\frac{1}{2} \sum_{\substack{\alpha \in F^\times \\ \mathrm{Tr}_{F/\mathbb{Q}}(\alpha) = m}} \sum_p \log(p) \operatorname{ord}_{\mathfrak{p}}(\alpha \mathfrak{p}\mathfrak{D}) \rho(\alpha \mathfrak{p}^{-1}\mathfrak{D}).$$

We can restrict α to be totally positive and p to be nonsplit in both K_1 and K_2; since the summand is nonzero for only one prime $\mathfrak{p}$ over each p, we can allow $\mathfrak{p}$ to vary over both primes of F over p to remove the dependence on α. Therefore we have

$$\deg \mathcal{T}_m = \frac{1}{2} \sum_{\substack{\alpha \in F^\times \\ \alpha > 0 \\ \mathrm{Tr}_{F/\mathbb{Q}}(\alpha) = m}} \sum_p \log(p) \sum_{\mathfrak{p} \mid p} \operatorname{ord}_{\mathfrak{p}}(\alpha \mathfrak{p}\mathfrak{D}) \rho(\alpha \mathfrak{p}^{-1}\mathfrak{D})$$

where the sum over p is restricted to those p nonsplit in both K_i and $\alpha > 0$ means that α is totally positive. Since $\mathrm{Nm}_{F/\mathbb{Q}}(\mathfrak{p}) = p$ by our assumptions on p, we can rewrite this as

$$\frac{1}{2} \sum_{\substack{\alpha \in F^\times \\ \alpha > 0 \\ \mathrm{Tr}_{F/\mathbb{Q}}(\alpha) = m}} \sum_{\mathfrak{p}} \log(\mathrm{Nm}(\mathfrak{p})) \operatorname{ord}_{\mathfrak{p}}(\alpha \mathfrak{p}\mathfrak{D}) \rho(\alpha \mathfrak{p}^{-1}\mathfrak{D})$$

where the inner sum is over all prime ideals of F, with corresponding restrictions. If $\alpha\mathfrak{D}$ is not an integral ideal of $\mathcal{O}_F$, then $\rho(\alpha\mathfrak{p}^{-1}\mathfrak{D})$ will be 0, so we can additionally restrict to $\alpha \in \mathfrak{D}^{-1}$. In particular we can write $\alpha = \frac{x+y\sqrt{D}}{2\sqrt{D}}$ for some integers x, y.

Restricting to the case $m = 1$, we have $\mathrm{Tr}(\alpha) = y = 1$ and so we can assume $\alpha = \frac{x+\sqrt{D}}{2\sqrt{D}}$ for $x \in \mathbb{Z}$. In order for $\rho(\alpha\mathfrak{p}^{-1}\mathfrak{D})$ to be nonzero, we must have $\mathfrak{p}|\alpha\mathfrak{D}$ as ideals. We claim that in fact for any ideal $\mathfrak{b}$ of $\mathcal{O}_F$ we have

$$\sum_{\mathfrak{n}|\mathfrak{b}} \chi(\mathfrak{n}) \log(\mathrm{Nm}(\mathfrak{n})) = \frac{1}{2} \sum_{\mathfrak{p}|\mathfrak{b}} \log(\mathrm{Nm}(\mathfrak{p})) \,\mathrm{ord}_{\mathfrak{p}}(\mathfrak{p}\mathfrak{b})\rho(\mathfrak{p}^{-1}\mathfrak{b}),$$

where χ is the quadratic Hecke character associated to K/F as in section 1. We proceed by induction: supposing that this holds for two relatively prime ideals $\mathfrak{b}_1$ and $\mathfrak{b}_2$, we want to show that it holds for their product. We have

$$\begin{aligned}
\sum_{\mathfrak{n}|\mathfrak{b}_1\mathfrak{b}_2} \chi(\mathfrak{n}) \log(\mathrm{Nm}(\mathfrak{n})) &= \sum_{\substack{\mathfrak{n}_1|\mathfrak{b}_1 \\ \mathfrak{n}_2|\mathfrak{b}_2}} \chi(\mathfrak{n}_1\mathfrak{n}_2) \log(\mathrm{Nm}(\mathfrak{n}_1\mathfrak{n}_2)) \\
&= \sum_{\mathfrak{n}_1|\mathfrak{b}_1} \chi(\mathfrak{n}_1) \log(\mathrm{Nm}(\mathfrak{n}_1)) \sum_{\mathfrak{n}_2|\mathfrak{b}_2} \chi(\mathfrak{n}_2) + \sum_{\mathfrak{n}_1|\mathfrak{b}_1} \chi(\mathfrak{n}_1) \sum_{\mathfrak{n}_2|\mathfrak{b}_2} \chi(\mathfrak{n}_2) \log(\mathrm{Nm}(\mathfrak{n}_2)) \\
&= \frac{1}{2} \sum_{\mathfrak{p}|\mathfrak{b}_1} \log(\mathrm{Nm}(\mathfrak{p})) \,\mathrm{ord}_{\mathfrak{p}}(\mathfrak{p}\mathfrak{b}_1)\rho(\mathfrak{p}^{-1}\mathfrak{b}_1)\rho(\mathfrak{b}_2) \\
&\qquad + \frac{1}{2} \sum_{\mathfrak{p}|\mathfrak{b}_2} \log(\mathrm{Nm}(\mathfrak{p})) \,\mathrm{ord}_{\mathfrak{p}}(\mathfrak{p}\mathfrak{b}_2)\rho(\mathfrak{p}^{-1}\mathfrak{b}_2)\rho(\mathfrak{b}_1)
\end{aligned}$$

using the inductive hypothesis and the fact that $\sum_{\mathfrak{n}|\mathfrak{b}} \chi(\mathfrak{n}) = \rho(\mathfrak{b})$ (since both sides give the coefficients for $L(\chi, s)\zeta_F(s) = \zeta_K(s)$). Since each prime $\mathfrak{p}$ divides at most one of $\mathfrak{b}_1$ and $\mathfrak{b}_2$ and ρ is multiplicative (on relatively prime ideals), we can combine this to

$$\frac{1}{2} \sum_{\mathfrak{p}|\mathfrak{b}_1\mathfrak{b}_2} \log(\mathrm{Nm}(\mathfrak{p})) \,\mathrm{ord}_{\mathfrak{p}}(\mathfrak{p}\mathfrak{b}_1\mathfrak{b}_2)\rho(\mathfrak{p}^{-1}\mathfrak{b}_1\mathfrak{b}_2)$$

as desired. It remains only to check that the equality holds for prime powers $\mathfrak{b} = \mathfrak{p}^k$, in which case the left-hand side is

$$\sum_{i=1}^{k} \chi(\mathfrak{p})^k k \log(\mathrm{Nm}(\mathfrak{p}))$$

and the right-hand side is

$$\frac{1}{2} \log(\mathrm{Nm}(\mathfrak{p}))(k+1) \sum_{i=0}^{k-1} \chi(\mathfrak{p})^i.$$

By the restrictions on $\mathfrak{p}$, we always have $\chi(\mathfrak{p}) = 1$, so these expressions agree.

Taking $\mathfrak{b} = \alpha\mathfrak{D}$, we've proven that

$$\deg \mathcal{T}_1 = \sum_{\substack{\alpha \in \mathfrak{D}^{-1} \\ \alpha > 0 \\ \mathrm{Tr}_{F/\mathbb{Q}}(\alpha) = 1}} \sum_{\mathfrak{n}|\alpha\mathfrak{D}} \chi(\mathfrak{n}) \log(\mathrm{Nm}(\mathfrak{n})).$$

But in fact this is one of the forms of the main theorem of [2], as expressed in equation (7.1); we can put it in a more familiar form by noting that there is a one-to-one correspondence between ideal divisors of $\alpha\mathfrak{O}$ and divisors of $\mathrm{Nm}(\alpha\mathfrak{O}) = \frac{D-x^2}{4}$, using the expression for α we found above. The induced function $\epsilon(n) = \chi(\mathfrak{n})$ where $n = \mathrm{Nm}(\mathfrak{n})$ is well-defined in the relevant cases, and is the function of the same name defined in [2]; then translating our expression into this language we get

$$\deg \mathcal{T}_1 = \sum_{\substack{x \in \mathbb{Z} \\ x^2 < D \\ x^2 \equiv D \pmod 4}} \sum_{n \mid \frac{D-x^2}{4}} \epsilon(n) \log(n),$$

which is essentially the logarithm of the right-hand side of Gross-Zagier's Theorem 1.3.

As far as the left-hand side, observe that length $\mathcal{O}^{\mathrm{sh}}_{\mathcal{T}_1,x}$ can be interpreted as an intersection number: if $x = (E_1, E_2, k) \in \mathcal{T}_1(\overline{\mathbb{F}_p})$, so that k is an isomorphism (changing notation to avoid a conflict coming up shortly), this number is equal to the intersection number $E_1 \cdot E_2$ on the modular curve, with k giving the level 1 data. On the other hand we can rewrite this intersection number as follows: let X be the modular curve, base changed to $\overline{\mathbb{F}_p}$, and $\Delta \subset X \times X$ be the diagonal. We have the uniformization $j : X \xrightarrow{\sim} \mathbb{P}^1_{\overline{\mathbb{F}_p}}$ and thus $j \times j : X \times_{\overline{\mathbb{F}_p}} X \xrightarrow{\sim} \mathbb{P}^1_{\overline{\mathbb{F}_p}} \times_{\overline{\mathbb{F}_p}} \mathbb{P}^1_{\overline{\mathbb{F}_p}}$, with the diagonal cut out by $j_1 - j_2$ where j_i denotes j on the ith component; thus the intersection number of Δ with the point $E_1 \times E_2 \in X \times_{\overline{\mathbb{F}_p}} X$ is given by the valuation $\mathrm{ord}_p(j(E_1) - j(E_2))$. By reduction to the diagonal this is just $E_1 \cdot E_2$.

Thus we have

$$\deg \mathcal{T}_1 = \frac{1}{w_1 w_2} \sum_p \log(p) \sum_{E_1, E_2} \mathrm{ord}_p(j(E_1) - j(E_2))$$

where the inner sum is taken over pairs (E_1, E_2) of elliptic curves over $\overline{\mathbb{F}_p}$ with complex multiplication by $\mathcal{O}_{K_1}$ and $\mathcal{O}_{K_2}$ respectively, and we have used Lemma 2.1 to evaluate the $\mathrm{Aut}(x)$ term. For each E_i there is another curve $\overline{E}_i$ which is the same elliptic curve with the conjugate action of $\mathcal{O}_{K_i}$, which for the purposes of Gross and Zagier should be considered the same curve; taking these equivalence classes gives

$$\deg \mathcal{T}_1 = \frac{4}{w_1 w_2} \sum_p \log(p) \sum_{[E_1],[E_2]} \mathrm{ord}_p(j(E_1) - j(E_2))$$

where $[E_i]$ denotes the corresponding class. Rearranging, this gives essentially the logarithm of the left-hand side of Theorem 1.3 of [2].

References

[1] Benedict H Gross. On canonical and quasi-canonical liftings. *Inventiones mathematicae*, 84(2):321–326, 1986.

[2] Benedict H Gross and Don B Zagier. On singular moduli. *Journal für die reine und angewandte Mathematik*, 355:191–220, 1984.

[3] Benjamin Howard and Tonghai Yang. Singular moduli refined. *arXiv preprint arXiv:1202.6410*, 2012.