CM-values of p-adic Theta-functions

Daas, M.A.

CHAPTER 3

Moduli of false elliptic curves

Assisted by the PhD thesis written by Andrew Phillips [Phi15], this chapter aims to approach Theorem A geometrically to give a first proof of Giampietro's conjectures. We stress here once again that using these results, our proof of Theorem A is rather straightforward. Therefore, the weight and novelty of this thesis rests mostly on the forthcoming chapters instead. Throughout this chapter, we fix $N \in \{6, 10, 22\}$.

Recall that modular curve $X_0(1)$ acts as a coarse moduli space for the set of elliptic curves up to isomorphism. This is done by sending $\tau \in \mathcal{H}$ to the elliptic curve $E_\tau = \mathbb{C}/\Lambda_\tau$ where $\Lambda_\tau = \mathbb{Z} + \mathbb{Z}\tau$. As one can choose various bases for the lattice Λ_τ, this induces a bijection

$$Y_0(1) = \mathrm{SL}_2(\mathbb{Z}) \setminus \mathcal{H} \xrightarrow{\sim} \big\{E/\mathbb{C} \text{ an elliptic curve}\big\}/ \text{ iso.}$$

A similar construction realises X_N as the coarse moduli space of *false elliptic curves*; roughly speaking, these are abelian surfaces A with the property that the maximal order $R_N \subset B_N$ embeds into the endomorphism ring of A. We say that such surfaces have *quaternionic multiplication* by R_N. To $\tau \in \mathcal{H}$ one associates the lattice

$$\Lambda_\tau := R_N \cdot \begin{pmatrix} \tau \\ 1 \end{pmatrix} \subset \mathbb{C}^2.$$

By construction, this lattice is stable under left-multiplication by R_N and as such, this maximal order embeds into $\mathrm{End}(A_\tau)$, where $A = \mathbb{C}^2/\Lambda_\tau$. This association yields a bijection

$$X_N(\mathbb{C}) = R_{N,1}^\times \setminus \mathcal{H} \xrightarrow{\sim} \big\{A/\mathbb{C} \text{ a false elliptic curve}\big\}/ \text{ iso.}$$

We use this description to illustrate why it is natural to define CM-points on the Shimura curve X_N as the fixed point in $\mathcal{H}$ for the action of the fields K_i on $\mathcal{H}$ through some fixed embeddings $\alpha_i : \mathcal{O}_i \to R_N$ for $i \in \{1, 2\}$. Roughly, we say a false elliptic curve A has CM by an imaginary quadratic order $\mathcal{O}$ if there exists an embedding $\mathcal{O} \to \mathrm{End}_{R_N}(A)$; in other words, there must be a subring of endomorphisms isomorphic to $\mathcal{O}$ that commutes with the given subring of endomorphisms isomorphic to R_N. The following lemma explains that with these definitions, CM-points on X_N correspond to false elliptic curves with CM.

Lemma 3.0.1. *Let $P \in \mathcal{H}$ be the fixed point for the action of some embedding $\alpha_i : \mathcal{O}_i \to R_N$. Then $P \in X_N$ corresponds to a false elliptic curve with complex multiplication by $\mathcal{O}_i$.*

Proof. Let $A = \mathbb{C}^2/\Lambda_P$ with Λ_P as defined above. We must find for any $x \in \mathcal{O}_i$ an endomorphism $\kappa(x)$ that commutes with the R_N-action on A. Note that if for some $x \in \mathcal{O}$,

$$\alpha_i(x) = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad \text{then} \quad \alpha_i(x) \cdot \begin{pmatrix} P \\ 1 \end{pmatrix} = \begin{pmatrix} aP+b \\ cP+d \end{pmatrix} = (cP+d)\begin{pmatrix} P \\ 1 \end{pmatrix}.$$

So we set $\kappa(x)$ to be scalar multiplication by $cP + d$ on $A = \mathbb{C}^2/\Lambda_P$. It remains to show that this is a ring homomorphism. To this end, choose an embedding $K_i \to \mathbb{C}$ and assume without loss of generality that $c > 0$ if and only if $x \in \mathcal{H}$. This is possible since $\alpha_i(\sqrt{D_i})$ cannot be upper triangular, for if so, its square would have positive trace, whereas $D_i < 0$. For $x \in \mathcal{H}$ we compute that

$$cP^2 + dP = aP + b \iff P = \frac{a - d + \sqrt{D_i(x)}}{2c}$$

where

$$D_i(x) = (a-d)^2 + 4bc = \mathrm{Tr}(\alpha_i(x))^2 - 4\det(\alpha_i(x)) = \mathrm{tr}(x)^2 - 4\,\mathrm{Nm}(x).$$

Therefore, we find that

$$cP + d = \frac{\mathrm{tr}(\alpha_i(x)) + \sqrt{D_i(x)}}{2} = \frac{\mathrm{tr}(x) + \sqrt{\mathrm{tr}(x)^2 - 4\,\mathrm{Nm}(x)}}{2}.$$

This describes the unique solution in $\mathcal{H}$ to the equation $X^2 - \mathrm{tr}(x)X + \mathrm{Nm}(x) = 0$, which is x. Whence $cP + d = x$ and the homomorphism property is immediate. □

3.1 Arakelov degrees of stacks

Unfortunately, the curve X_N is only a coarse moduli space for false elliptic curves. To obtain a fine moduli space, we will need to work with algebraic stacks. An overview of the theory of stacks will not be given here, but for a brief yet clear introduction, we refer the reader to Section 7 of [Vis89]. We start with some definitions.

Definition 3.1.1. A *false elliptic curve* over a scheme S is a pair (A, ι) where $A \to S$ is an abelian scheme of relative dimension 2 and $\iota\colon R_N \to \mathrm{End}_S(A)$ is a ring homomorphism. For $i \in \{1, 2\}$, a false elliptic curve over an $\mathcal{O}_L$-scheme S with *complex multiplication* by $\mathcal{O}_i$ is a triple (A, ι, κ) where (A, ι) is a false elliptic curve over S and $\kappa\colon \mathcal{O}_i \to \mathrm{End}_{R_N}(A)$ is a ring map such that the action on the Lie algebra is through the natural structure map $\mathcal{O}_i \to \mathcal{O}_L \to \mathcal{O}_S(S)$.

Definition 3.1.2. Let $\mathcal{M}$ be the algebraic stack, regular and flat of relative dimension 1 over $\mathrm{Spec}(\mathcal{O}_L)$, such that $\mathcal{M}(S)$ for any $\mathcal{O}_L$-scheme S denotes the category of false elliptic curves (A, ι) over S satisfying for any $x \in R_N$ the property that any $s \in S$ has an affine open neighbourhood $\mathrm{Spec}(R) \to S$ such that $\mathrm{Lie}(A_{/R})$ is a free R-module of rank 2 and there is an equality of polynomials in $R[T]$ of the form

$$\mathrm{char}(\iota(x), \mathrm{Lie}(A_{/R}) = (T - x)(T - \overline{x}),$$

where $\overline{(\ldots)}$ denotes the main involution on B_N. This 2-dimensional stack $\mathcal{M}$ is usually referred to as (the integral model of) a Shimura curve.

We are interested in two particular substacks of this stack; those defining the false elliptic curves with complex multiplication by $\mathcal{O}_i$ for $i \in \{1, 2\}$. Let $\mathcal{Y}_i$ for $i \in \{1, 2\}$ be the algebraic stack over $\mathrm{Spec}(\mathcal{O}_L)$ with $\mathcal{Y}_i(S)$ the category of false elliptic curves over the $\mathcal{O}_L$-scheme S with complex multiplication by $\mathcal{O}_i$. By forgetting the CM-structure, we have a morphism of stacks $\mathcal{Y}_i \to \mathcal{M}$. We further define

$$\mathcal{J} := \mathcal{Y}_1 \times_{\mathcal{M}} \mathcal{Y}_2.$$

By definition of the pullback of stacks, $\mathcal{J}$ now denotes the algebraic stack over $\mathrm{Spec}(\mathcal{O}_L)$ with $\mathcal{J}(S)$ the category of triples $(\mathbf{A}_1, \mathbf{A}_2, f)$ where $\mathbf{A}_i = (A_i, \iota_i, \kappa_i)$ for $i \in \{1, 2\}$ is a false elliptic curve over the $\mathcal{O}_L$-scheme S with complex multiplication by $\mathcal{O}_i$ and where $f \colon \mathbf{A}_1 \to \mathbf{A}_2$ is an isomorphism of false elliptic curves.

Following [Phi15], we proceed to refine the stack $\mathcal{J}$ by associating to every triple $(\mathbf{A}_1, \mathbf{A}_2, f) \in \mathcal{J}(S)$ a pair of objects (ϑ, ν) as follows. It is easy to show that there exists a unique ideal $\mathfrak{m}_N \subset R_N$ of index N^2. For $i \in \{1, 2\}$, there is a unique surjective ring map $\theta_i \colon \mathcal{O}_i \to R_N/\mathfrak{m}_N$ making the following diagram commute, where $A_i[\mathfrak{m}_N]$ denotes the group

$$\begin{array}{ccc} \mathcal{O}_i & \longrightarrow & \mathrm{End}_{R_N/\mathfrak{m}_N}(A_i[\mathfrak{m}_N]) \\ & {\scriptstyle\theta_i}\searrow \quad \nearrow & \\ & R_N/\mathfrak{m}_N & \end{array}$$

scheme of the $\mathfrak{m}_N$-torsion inside A_i.

Since $\mathcal{O}_L = \mathcal{O}_1 \otimes_{\mathbb{Z}} \mathcal{O}_2$, we obtain a well-defined surjective ring map $\vartheta \colon \theta_1 \otimes \theta_2 \colon \mathcal{O}_L \to R_N/\mathfrak{m}_N$. For brevity, we will denote

$$\mathcal{V} := \mathrm{Hom}(\mathcal{O}_L, R/\mathfrak{m}_N).$$

We let $\mathfrak{a}_\vartheta = \ker(\vartheta) \cap \mathcal{O}_F$ be the *reflex ideal.* Since $\ker(\vartheta)$ is an $\mathcal{O}_L$-ideal of norm N^2, it follows that $\mathfrak{a}_\vartheta$ is an $\mathcal{O}_F$-ideal of norm N. As such, as $N = pq$, there are precisely four possibilities for $\mathfrak{a}_\vartheta$;

$$\mathfrak{a}_\vartheta \in \{\mathfrak{p}_1\mathfrak{q}_1, \mathfrak{p}_1\mathfrak{q}_2, \mathfrak{p}_2\mathfrak{q}_1, \mathfrak{p}_2\mathfrak{q}_2\} =: \mathcal{I}.$$

Next, as in Proposition 2.3 in [HY12], one can construct a map

$$\deg_{\mathrm{CM}} \colon \mathrm{Hom}_{R_N}(A_1, A_2) \to \mathcal{D}_F^{-1}$$

satisfying the defining property that $\mathrm{tr}_{\mathbb{Q}}^F(\deg_{\mathrm{CM}}(f)) = \deg^*(f)$, where $\deg^*(f)$ denotes the *false degree* of the morphism f as in Definition 2.2.15 in [Phi15], which satisfies the property that $\deg^*(f) = 1$ for all isomorphisms f. This construction is very similar to the one to be outlined in Section 4.4 of this thesis, so we will not give more details here. As such, we may consider the element $\nu = \deg_{\mathrm{CM}}(f) \in \mathcal{D}_F^{-1}$. Then $\mathrm{tr}(\nu) = 1$.

For any $\vartheta \in \mathcal{V}$, we define $\mathcal{X}_\vartheta$ to be the algebraic stack over $\mathrm{Spec}(\mathcal{O}_L)$ with $\mathcal{X}_\vartheta(S)$ for any $\mathcal{O}_L$-scheme S the category of triples $(\mathbf{A}_1, \mathbf{A}_2, f) \in \mathcal{J}(S)$ with the property that the pair $(\mathbf{A}_1, \mathbf{A}_2)$ induces the map $\vartheta \in \mathcal{V}$ by the construction outlined above.

For any $\nu \in \mathcal{D}_F^{-1}$, we let $\mathcal{X}_{\vartheta,\nu}$ denote the algebraic stack over $\mathrm{Spec}(\mathcal{O}_L)$ with $\mathcal{X}_{\vartheta,\nu}(S)$ for any $\mathcal{O}_L$-scheme S the category of triples $(\mathbf{A}_1, \mathbf{A}_2, f) \in \mathcal{X}_\vartheta(S)$ with the property that $\deg_{\mathrm{CM}}(f) = \nu$ on every component of S.

We then obtain the decompositions

$$\mathcal{J} = \bigsqcup_{\vartheta \in \mathcal{V}} \mathcal{X}_\vartheta \quad \text{and} \quad \mathcal{X}_\vartheta = \bigsqcup_{\substack{\nu \in \mathcal{D}_F^{-1} \\ \mathrm{tr}(\nu)=1}} \mathcal{X}_{\vartheta,\nu}.$$

The main result of [Phi15] concerns the *Arakelov degree* of the stacks $\mathcal{X}_\vartheta$, which is defined as

$$\deg(\mathcal{X}_\vartheta) := \sum_{\mathfrak{r} \subset \mathcal{O}_L} \log(|\mathbb{F}_\mathfrak{r}|) \sum_{x \in \mathcal{X}_\vartheta(k)} \frac{\mathrm{length}(\mathcal{O}^{\mathrm{sh}}_{\mathcal{X}_{\vartheta,x}})}{|\mathrm{Aut}(x)|},$$

where $\mathfrak{r} \subset \mathcal{O}_L$ is a prime, where $k = \overline{\mathbb{F}}_\mathfrak{r}$ and where $\mathcal{O}^{\mathrm{sh}}_{\mathcal{X}_{\vartheta,x}}$ denotes the strictly Henselian local ring of $\mathcal{X}_\vartheta$ for the étale topology at the geometric point x. By the decomposition above, we have

$$\deg(\mathcal{X}_\vartheta) = \sum_{\substack{\nu \in \mathcal{D}_F^{-1} \\ \mathrm{tr}(\nu)=1}} \deg(\mathcal{X}_{\vartheta,\nu}). \tag{3.1}$$

Lastly, we define the finite set

$$\mathrm{Diff}_\vartheta(\nu) = \mathrm{Diff}_{\mathfrak{a}_\vartheta}(\nu) := \{\mathfrak{r} \subset \mathcal{O}_F \mid \chi_\mathfrak{r}(\nu\mathfrak{a}_\vartheta^{-1}\mathcal{D}_F) = -1\},$$

where $\chi_\mathfrak{r}$ denotes the character defined by the unramified extension of local fields $L_\mathfrak{r}/F_\mathfrak{r}$, obtained by completing these fields at the prime $\mathfrak{r}$ and a prime of L above it. For $I \subset \mathcal{O}_F$, it holds that $\chi_\mathfrak{r}(I) = \chi(\mathfrak{r})^{\mathrm{ord}_\mathfrak{r}(I)}$. Theorem 2 in [Phi15] then says the following.

Theorem 3.1.3. *Let $\nu \in F$ satisfy $\mathrm{tr}(\nu) = 1$. Suppose that $\mathrm{Diff}_\vartheta(\nu) = \{\mathfrak{r}\}$ for some prime $\mathfrak{r} \subset \mathcal{O}_F$. If $r \nmid N$, the degree of $\mathcal{X}_{\vartheta,\nu}$ satisfies*

$$\exp(\deg(\mathcal{X}_{\vartheta,\nu})) = r^{t_r/2} \quad \textit{where} \quad t_r = \mathrm{ord}_\mathfrak{r}(\nu\mathfrak{r}\mathcal{D}_F) \cdot \rho(\nu\mathfrak{a}_\vartheta^{-1}\mathfrak{r}^{-1}\mathcal{D}_F).$$

If $r \mid N$, depending on whether $\mathfrak{r}$ divides $\mathfrak{a}_\vartheta$ or not, we must replace the term $\mathrm{ord}_\mathfrak{r}(\nu\mathfrak{r}\mathcal{D}_F)$ by $\mathrm{ord}_\mathfrak{r}(\nu)$ or $\mathrm{ord}_\mathfrak{r}(\nu\mathfrak{r})$ respectively.

If $\nu \notin \mathcal{D}_F^{-1}$ or $\#\mathrm{Diff}_\vartheta(\nu) \neq 1$, then the degree is always 0. In addition, if $\nu \not\gg 0$, then the degree is always 0.

This result gives us an explicit formula for the Arakelov degrees of the stacks $\mathcal{X}_{\vartheta,\nu}$ and as such, also of the degrees of the stacks $\mathcal{X}_\vartheta$. It is also clear from the result that the degree of the stack $\mathcal{X}_{\vartheta,\nu}$ only depends on the ideal $\mathfrak{a}_\vartheta \in \mathcal{I}$ and not on the precise map $\vartheta \in \mathcal{V}$. Therefore, the same holds true for the degree of $\mathcal{X}_\vartheta$ too. This allows us to define for any $\mathfrak{a} \in \mathcal{I}$ and $\nu \in F$ the quantities

$$X(\mathfrak{a}, \nu) := \deg(\mathcal{X}_{\vartheta,\nu}) \quad \text{and} \quad X(\mathfrak{a}) := \deg(\mathcal{X}_\vartheta),$$

where $\vartheta \in \mathcal{V}$ is arbitrary such that $\mathfrak{a}_\vartheta = \mathfrak{a}$. In the next section we will show that these expressions, when combined appropriately, constitute the right hand side of Theorem A. The remainder of this chapter aims to relate the degrees of the stacks $\mathcal{X}_\vartheta$ to the left hand side, ultimately establishing equality.

3.2 An elementary formula

We first prove a sequence of smaller lemmas, that each will take care of a separate part of the translation process between Phillips's more abstract ideal arithmetic and Gross and Zagier's and Giampietro's elementary formulas involving the F-function defined in Section 1.2.

Recall the definition of a *special prime* for a positive integer m as being a prime ℓ that divides m an odd number of times and such that each prime $\mathfrak{l}$ of F above ℓ satisfies $\chi(\mathfrak{l}) = -1$.

Lemma 3.2.1. *Let $\nu \in \mathcal{D}_F^{-1,+}$ with $\mathrm{tr}(\nu) = 1$. Then the ideal $\nu\mathcal{D}_F$ is integral, principal and primitive.*

Proof. We write $\nu = (x+\sqrt{D})/2\sqrt{D}$ for some odd integer x. Using that $\mathcal{D}_F = (\sqrt{D})$, we find that $\nu\mathcal{D}_F = ((x+\sqrt{D})/2)$. This is clearly integral and principal, and it is primitive because no rational prime r can divide it. Indeed, the element $(x+\sqrt{D})/2r$ can never be integral for a prime r. This completes the proof. □

Lemma 3.2.2. *Let $\nu = (x+\sqrt{D})/2\sqrt{D}$ for some integer x be such that some $\mathfrak{a} \in \mathcal{I}$ satisfies $\mathfrak{a} \mid \nu\mathcal{D}_F$. If $\mathfrak{r} \in \mathrm{Diff}_{\mathfrak{a}}(\nu)$ and $r = \mathfrak{r} \cap \mathbb{Z}$, then r is a special prime of the integer $(D - x^2)/4N$.*

Proof. Recall that for $I \subset \mathcal{O}_F$, it holds that $\chi_{\mathfrak{r}}(I) = \chi(\mathfrak{r})^{\mathrm{ord}_{\mathfrak{r}}(I)}$.

Suppose that $\mathfrak{r} \in \mathrm{Diff}_{\vartheta}(\nu)$, or in other words, $\chi_{\mathfrak{r}}(\nu\mathfrak{a}\mathcal{D}_F) = -1$. By the explicit description of $\chi_{\mathfrak{r}}$, it now follows that $\chi(\mathfrak{r}) = -1$, so $\mathfrak{r}$ is inert in L/F. Therefore, r is not inert in F.

Now note that $\chi_{\mathfrak{r}}(\nu\mathfrak{a}\mathcal{D}_F) = \chi_{\mathfrak{r}}(\nu\mathfrak{a}^{-1}\mathcal{D}_F)$, as squares of ideals are always in the kernel of $\chi_{\mathfrak{r}}$. By Lemma 3.2.1, this latter ideal is both integral and still primitive, and as such, only one of the two primes above r in F can occur in its factorisation. This multiplicity is then equal to the multiplicity with which r occurs in the norm of the ideal. As $\chi_{\mathfrak{r}}(\nu\mathcal{D}_F) = -1$, this number must be odd, establishing that r is indeed a special prime of the integer $(D - x^2)/4N$. □

Lemma 3.2.3. *Let $I \subset \mathcal{O}_F$ be an ideal with explicit prime factorisation $I = \prod_i \mathfrak{r}_i^{2m_i} \prod_j \mathfrak{s}_j^{n_j}$ where all the primes $\mathfrak{s}_j$ split in L/F and all $\mathfrak{r}_i$ are inert in L/F. Then we have*

$$\rho(I) = \prod_j (n_j + 1).$$

Proof. We look prime by prime. The unique ideal $\mathfrak{R}_i$ of L lying over $\mathfrak{r}_i$ has norm $\mathfrak{r}_i^2$. Hence only $\mathfrak{R}^{m_i}$ has norm $\mathfrak{r}^{2m_i}$.

For any of the $\mathfrak{s}_j$, we find two primes in L lying above it, say $\mathfrak{S}_j$ and $\mathfrak{S}'_j$. The norm of $\mathfrak{S}_j^a \mathfrak{S}_j'^b$ is equal to $\mathfrak{s}^{a+b}$ and so we find $n_j + 1$ possible ideals with norm $\mathfrak{s}_j^{n_j}$, corresponding to $a \in \{0, \ldots, n_j\}$. □

Lemma 3.2.4. *Let $\nu \in \mathcal{D}_F^{-1,+}$ with $\mathrm{tr}(\nu) = 1$. Then there is at most one ideal $\mathfrak{a} \in \mathcal{I}$ such that $\rho(\nu\mathfrak{a}^{-1}\mathcal{D}_F) > 0$.*

Proof. A necessary condition for the quantity $\rho(\nu\mathfrak{a}^{-1}\mathcal{D}_F)$ to be positive, is that the ideal $\nu\mathfrak{a}^{-1}\mathcal{D}_F$ be integral. In other words, we must have

$\mathfrak{a} \mid \nu\mathcal{D}_F$. However, by Lemma 3.2.1, this latter ideal is primitive, and two different such $\mathfrak{a} \in \mathcal{I}$ dividing it would mean that either p or q would also divide it. This proves the lemma. $\square$

Now note that $\mathfrak{a} \mid \nu\mathcal{D}_F$ if and only if $(x+\sqrt{D})/2 \in \mathfrak{a}$. Applying the nontrivial automorphism σ of $F/\mathbb{Q}$ to this inclusion, we see that

$$(x+\sqrt{D})/2 \in \mathfrak{a} \iff (-x+\sqrt{D})/2 \in \sigma(\mathfrak{a}).$$

The norm of $\nu\mathcal{D}_F$ is given by $(x^2-D)/4$, so if this is divisible by N, then x^2-D must be divisible by $2N$, and so $x^2 \equiv D \mod 2N$. Therefore, $\nu\mathcal{D}_F$ can only be divisible by some $\mathfrak{a} \in \mathcal{I}$ if $x \equiv \pm a, \pm b \mod 2N$, where a and b are as in Equation 2.1. Recall from the previous section that the *reflex ideal* $\mathfrak{a}_\vartheta$ must be an element of the set

$$\mathcal{I} := \{\mathfrak{p}_1\mathfrak{q}_1, \mathfrak{p}_1\mathfrak{q}_2, \mathfrak{p}_2\mathfrak{q}_1, \mathfrak{p}_2\mathfrak{q}_2\}.$$

The first and last are Galois conjugate and so are the second and third. Combining all this, we define

$$\delta(\vartheta) = \delta(\mathfrak{a}_\vartheta) := \begin{cases} +1 & \text{if } \mathfrak{a}_\vartheta \in \{\mathfrak{p}_1\mathfrak{q}_1, \mathfrak{p}_2\mathfrak{q}_2\}; \\ -1 & \text{if } \mathfrak{a}_\vartheta \in \{\mathfrak{p}_1\mathfrak{q}_2, \mathfrak{p}_2\mathfrak{q}_1\}, \end{cases}$$

with these Galois orbits chosen in such a way that this sign agrees with the choices from Equation 2.1. The following theorem will be the key consequence of Phillips's work in [Phi15]. It connects the degrees of certain stacks to the explicit formula found in Theorem A.

Theorem 3.2.5. *Let $\nu \in \mathcal{D}_F^{-1,+}$ with $\mathrm{tr}(\nu) = 1$. Then we can write $\nu = (x+\sqrt{D})/2\sqrt{D}$ for some integer x with $x^2 < D$. Furthermore,*

$$F\left(\frac{D-x^2}{4N}\right)^{\delta(x)} = \prod_{\mathfrak{a}\in\mathcal{I}} \exp\bigl(\delta(\mathfrak{a})X(\mathfrak{a},\nu)\bigr).$$

Proof. If the norm of $\nu\mathcal{D}_F$ is not divisible by N, then the ideal $\nu\mathfrak{a}_\vartheta^{-1}\mathfrak{r}^{-1}\mathcal{D}_F$ is not integral for any choice of $\mathfrak{a}_\vartheta$ and $\mathfrak{r}$. So no matter the case of Theorem 3.1.3 we are in, $X(\mathfrak{a},\nu) = 0$. The right hand side of the equation will thus be 1, as is the left hand side.

We thus assume that some $\mathfrak{a} \in \mathcal{I}$ divides $\nu\mathcal{D}$. By Lemma 3.2.4, there is then only one such $\mathfrak{a}$. By the same argument as above, any other ideal in $\mathcal{I}$ will not contribute to the product on the right hand side. Hence we may restrict our view to the unique $\mathfrak{a} \in \mathcal{I}$ dividing $\nu\mathcal{D}$. By definition, the signs $\delta(x)$ and $\delta(\mathfrak{a})$ will agree in this case. Thus we are left to prove

$$F\left(\frac{D-x^2}{4N}\right) = \exp(\deg(\mathcal{X}_{\vartheta,\nu})).$$

We distinguish two cases. First suppose that $\mathrm{Diff}_{\mathfrak{a}}(\nu)$ does not consist of exactly one prime. Then Theorem 3.1.3 tells us that the right hand side again becomes equal to 1. On the other hand, we note that we are in the situation of Lemma 3.2.2 and thus the primes occuring in $\mathrm{Diff}_{\mathfrak{a}}(\nu)$ biject with the special primes of $(D-x^2)/(4N)$. By definition, now that we do *not* have exactly one such prime, F equals 1 too.

We may thus from now on suppose that $\mathrm{Diff}_{\mathfrak{a}}(\nu)$ consists of exactly one prime $\mathfrak{r}$. We again distinguish two cases. First suppose that $r \nmid N$. Then we may use Theorem 3.1.3 to reduce to checking that

$$F\left(\frac{D-x^2}{4N}\right) = r^{t_r/2} \quad \text{where} \quad t_r = \mathrm{ord}_{\mathfrak{r}}(\nu\mathfrak{r}\mathcal{D}) \cdot \rho(\nu\mathfrak{a}^{-1}\mathfrak{r}^{-1}\mathcal{D}_F).$$

We claim that the ideal factorisation of $\nu\mathfrak{a}^{-1}\mathfrak{r}^{-1}\mathcal{D}_F$ is of the form as in Lemma 3.2.3. Let $\mathfrak{l}$ be a prime divisor of this ideal lying over the rational prime ℓ and let $n \in \mathbb{N}$ be such that $\mathfrak{l}^n \| \nu\mathfrak{a}^{-1}\mathfrak{r}^{-1}\mathcal{D}_F$.

If $\mathfrak{l}$ splits in L/F, there is nothing to show. If not, n being odd would imply that $\mathfrak{l} \in \mathrm{Diff}_{\mathfrak{a}}(\nu) = \{\mathfrak{r}\}$, yielding a contradiction unless $\mathfrak{l} = \mathfrak{r}$. However, in that case, the added factor of $\mathfrak{r}^{-1}$ makes the odd multiplicity of $\mathfrak{r}$ in $\nu\mathfrak{a}^{-1}\mathcal{D}_F$ even again.

We are thus in the position to apply Lemma 3.2.3 to $\nu\mathfrak{a}^{-1}\mathfrak{r}^{-1}\mathcal{D}_F$. Using the notation from said lemma, we compute that

$$\rho(\nu\mathfrak{a}^{-1}\mathfrak{r}^{-1}\mathcal{D}_F) = \prod_j (n_j + 1),$$

where the n_j are the multiplicities with which primes in F that split in L/F divide $\nu\mathfrak{a}^{-1}\mathfrak{r}^{-1}\mathcal{D}_F$. Again, by Lemma 3.2.1, this ideal is primitive so its ideal factorisation in F reflects the factorisation of its norm in $\mathbb{Z}$. Let $2k+1$ denote the odd multiplicity with which $\mathfrak{r}$ divides $\nu\mathcal{D}_F$. Then since $r \nmid N$, we compute that

$$\frac{\mathrm{ord}_{\mathfrak{r}}(\nu\mathfrak{r}\mathcal{D}_F)}{2} = k+1.$$

So, the right hand side becomes $(k+1)\prod_j(n_j+1)$. Indeed, this agrees with our definition of F, as the norm of $\nu\mathfrak{a}^{-1}\mathcal{D}_F$ is $(D-x^2)/(4N)$, completing the proof in this case.

Finally, we must consider the case of $r \mid N$. We claim that we are always in the case that the prime $\mathfrak{r} \in \mathrm{Diff}_\vartheta(\nu)$ above r divides $\mathfrak{a}$. Namely, by Lemma 3.2.4, the only prime ideals over r dividing $\nu\mathcal{D}_F$ are, by our choice of $\mathfrak{a}$, those occuring in $\mathfrak{a}$. Hence any prime over r occuring at all in the factorisation of $\nu\mathfrak{a}^{-1}\mathcal{D}_F$ must also divide $\mathfrak{a}$. Hence, we use Theorem 3.1.3 to reduce ourselves to proving that

$$F\left(\frac{D-x^2}{4N}\right) = r^{t_r/2} \quad \text{where} \quad t_r = \mathrm{ord}_{\mathfrak{p}}(\nu)\cdot\rho(\nu\mathfrak{a}^{-1}\mathfrak{p}^{-1}\mathcal{D}_F).$$

Our accounting for the factor contributed by $\rho(\nu\mathfrak{a}^{-1}\mathfrak{p}^{-1}\mathcal{D}_F)$ is very similar to the argument given above. For the other factor, we note that $\mathrm{ord}_{\mathfrak{p}}(\nu) = \mathrm{ord}_{\mathfrak{p}}(\nu\mathcal{D}_F)$ as we assume D and N to be coprime. Let $2k+1$ be the multiplicity with which $\mathfrak{r}$ divides $\nu\mathfrak{a}\mathcal{D}_F$, so it divides $\nu\mathcal{D}_F$ exactly $2k$ times. Together with the factor $1/2$, this contributes a factor of k to the exponent t_r on the right hand side. On the left hand side, we note that $2k$ is equal to the multiplicity with which r divides the norm $(D-x^2)/4$ of $\nu\mathcal{D}_F$. Hence the number $(D-x^2)/(4N)$ contains precisely $2k-1 = 2(k-1)+1$ factors of r. Thus indeed, using the definition of F, we also find on this side an added factor of $(k-1)+1 = k$. □

3.3 From $\mathcal{M}$ to X_N

The main goal of the sections that follow will be to reinterpret the Arakelov degrees of the stacks $\mathcal{X}_\vartheta$ for $\vartheta \in \mathcal{V}$ as quantities involving cross-ratios of the function $j_N : X_N \xrightarrow{\sim} \mathbb{P}^1$. Most terms appearing in the formula of the Arakelov degree are straightforward, the most profound one being the length of certain strictly Henselian local rings on stacks. This section aims to relate these numbers to lengths of rings associated with the algebraic curve X_N instead.

Proposition 3.3.1. *Recall that $w_i := \#\mathcal{O}_i^\times$. Then we have*

$$\deg(\mathcal{X}_\vartheta) = \frac{1}{w_1 w_2}\sum_{\mathfrak{r}\subset\mathcal{O}_L}\log(|\mathbb{F}_\mathfrak{r}|)\sum_{x\in\mathcal{X}_\vartheta(k)}\mathrm{length}(\mathcal{O}^{\mathrm{sh}}_{\mathcal{Y}_{1,x}}\otimes_{\mathcal{O}^{\mathrm{sh}}_{\mathcal{M}_x}}\mathcal{O}^{\mathrm{sh}}_{\mathcal{Y}_{2,x}}),$$

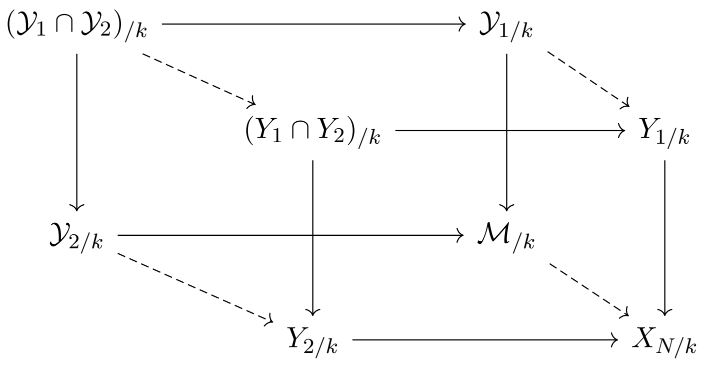
where the sum is taken over all isomorphism classes $x = (\boldsymbol{A}_1, \boldsymbol{A}_2, f) \in \mathcal{X}_\vartheta(k)$ and where $k = \overline{\mathbb{F}}_\mathfrak{r}$.

Proof. Recall that by definition, $\mathcal{J} = \mathcal{Y}_1 \times_{\mathcal{M}} \mathcal{Y}_2$. This means that

$$\mathcal{O}^{\mathrm{sh}}_{\mathcal{X}_{\vartheta,x}} = \mathcal{O}^{\mathrm{sh}}_{\mathcal{J}_x} = \mathcal{O}^{\mathrm{sh}}_{\mathcal{Y}_{1,x}}\otimes_{\mathcal{O}^{\mathrm{sh}}_{\mathcal{M}_x}}\mathcal{O}^{\mathrm{sh}}_{\mathcal{Y}_{2,x}}.$$

Further invoking Theorem 4.1.3 in [Phi15], which says that $|\mathrm{Aut}(x)| = w_1 w_2$ for all points x, the result follows from the definition of the Arakelov degree. □

Let $Y_i \to X_N$ be the closed subscheme supported on the $4h_i$ points with CM by $\mathcal{O}_i$ for $i \in \{1, 2\}$. As is outlined in Section II of [Vis89], we have a natural map $\pi : \mathcal{M} \to X_N$. As X_N is smooth and $\mathcal{M}$ is a Deligne-Mumford stack, by the *miracle flatness theorem*, the map π must in fact be flat. We have summarised the situation in the cube below.



We proceed with the following useful lemma.

Lemma 3.3.2. *Two triples* $(\boldsymbol{A}_1, \boldsymbol{A}_2, f), (\boldsymbol{A}'_1, \boldsymbol{A}'_2, g) \in \mathcal{X}_\vartheta(k)$ *are isomorphic if and only if* $\boldsymbol{A}_i \cong \boldsymbol{A}'_i$ *for* $i \in \{1, 2\}$.

Proof. To give a morphism $(\mathbf{A}_1, \mathbf{A}_2, f) \to (\mathbf{A}'_1, \mathbf{A}'_2, g)$ is to give morphisms $\varphi : \mathbf{A}_1 \to \mathbf{A}'_1$ and $\psi : \mathbf{A}_2 \to \mathbf{A}'_2$ such that the following diagram commutes:

$$\begin{array}{ccc} \mathbf{A}_1 & \xrightarrow{\varphi} & \mathbf{A}'_1 \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle g} \\ \mathbf{A}_2 & \xrightarrow{\psi} & \mathbf{A}'_2 \end{array}$$

Such a morphism $(\mathbf{A}_1, \mathbf{A}_2, f) \to (\mathbf{A}'_1, \mathbf{A}'_2, g)$ is an isomorphism if and only if both φ and ψ are isomorphisms. This proves one direction.

Conversely, consider two triples $(\mathbf{A}_1, \mathbf{A}_2, f)$ and $(\mathbf{A}'_1, \mathbf{A}'_2, g)$ and suppose that $\mathbf{A}_i$ and $\mathbf{A}'_i$ are isomorphic for $i \in \{1, 2\}$. Choose $\varphi : \mathbf{A}_1 \to \mathbf{A}'_1$ as such an isomorphism and set $\psi = g \circ \varphi \circ f^{-1}$. Being the composition of isomorphisms, this map is also an isomorphism and it makes the diagram commute; thus this describes an isomorphism between the triples $(\mathbf{A}_1, \mathbf{A}_2, f)$ and $(\mathbf{A}'_1, \mathbf{A}'_2, g)$ and the bijection has been proved. □

This is useful, as the set of CM-points without any additional information has a very well-understood structure, as we will see in the next section. For now, we content ourselves with proving the following key proposition, which establishes our goal for this section.

Proposition 3.3.3. *Fix a prime ideal* $\mathfrak{r} \subset \mathcal{O}_K$ *and a geometric point* $x = (\boldsymbol{A}_1, \boldsymbol{A}_2, f) \in \mathcal{X}_\vartheta(k)$ *where* $k = \overline{\mathbb{F}}_\mathfrak{r}$. *Then*

$$\operatorname{length}\big(\mathcal{O}^{\mathrm{sh}}_{\mathcal{X}_\vartheta, x}\big) = 2 \operatorname{length}\big(\mathcal{O}^{\mathrm{sh}}_{Y_1,x} \otimes_{\mathcal{O}^{\mathrm{sh}}_{X_N,x}} \mathcal{O}^{\mathrm{sh}}_{Y_2,x}\big).$$

Proof. We will use a few results on stacky intersection theory from [Vis89] for the map $\pi : \mathcal{M} \to X_N$. All local rings we consider are for the étale topology on the respective schemes. On the rational Chow group, Definition 3.6 states that the proper push forward of a cycle D on a stack is defined to be the image cycle multiplied by the relative degree of the map from the cycle and its image. Since k is perfect and the number of automorphisms for CM false elliptic curves is constant, Corollary 2.5 in [Vis89] implies that this degree is the reciprocal of the size of the automorphism group of our point. Using Lemma 4.1.3 in [Phi15], we then find

$$\pi_*(\mathcal{Y}_i) = \frac{1}{w_i} Y_i.$$

In addition, the above also shows that pushing forward the stacky intersection $\mathcal{Y}_1 \cap \mathcal{Y}_2$ along π will divide the result by $\operatorname{Aut}(x) = w_1 w_2$; whence

$$\pi_*(\mathcal{Y}_1 \cdot \mathcal{Y}_2)_x = \frac{1}{w_1 w_2} \operatorname{length}\big(\mathcal{O}^{\mathrm{sh}}_{\mathcal{X}_\vartheta, x}\big).$$

As we know π to be flat, we have a well-defined notion of a pull-back of cycles along π. A general false elliptic curve admits only two automorphisms, namely ± 1. Therefore, $\deg(\pi) = 1/2$. Very generally, one has the formulae

$$\pi^*(Y_i) = \deg(\pi) w_i \mathcal{Y}_i = \frac{w_i}{2} \mathcal{Y}_i, \quad \text{so that} \quad \pi^* \pi_* = \deg(\pi) = \frac{1}{2}.$$

We may now use the *projection formula* from stacky intersection theory (compare with the Stacks Project [0B0C]) to compute that on the other hand, it holds that

$$\begin{aligned}\pi_*(\mathcal{Y}_1\cdot\mathcal{Y}_2)_x &= \pi_*\Big(\frac{2}{w_1}\pi^*(Y_1)\cdot\mathcal{Y}_2\Big)_x\\ &= \frac{2}{w_1}\pi_*\left(\pi^*(Y_1)\cdot\mathcal{Y}_2\right)_x = \frac{2}{w_1}\left(Y_1\cdot\pi_*(\mathcal{Y}_2)\right)_x\\ &= \frac{2}{w_1}\Big(Y_1\cdot\frac{1}{w_2}Y_2\Big)_x = \frac{2}{w_1w_2}(Y_1\cdot Y_2)_x\\ &= \frac{2}{w_1w_2}\mathrm{length}\big(\mathcal{O}^{\mathrm{sh}}_{Y_1,x}\otimes_{\mathcal{O}^{\mathrm{sh}}_{X_N,x}}\mathcal{O}^{\mathrm{sh}}_{Y_2,x}\big).\end{aligned}$$

Now compare these two expressions for $\pi_*(\mathcal{Y}_1\cdot\mathcal{Y}_2)_x$. □

For notational convenience, we let $(Y_1\times Y_2)_\vartheta(k)$ denote the set of pairs of CM-points over k that induce $\vartheta:\mathcal{O}_L\to R_N/\mathfrak{m}_N$.

Corollary 3.3.4. *It holds that*

$$\deg(\mathcal{X}_\vartheta)=\frac{2}{w_1w_2}\sum_{\mathfrak{r}\subset\mathcal{O}_L}\log(|\mathbb{F}_\mathfrak{r}|)\sum_{(Y_1\times Y_2)_\vartheta(k)}\mathrm{length}\big(\mathcal{O}^{\mathrm{sh}}_{Y_1,\boldsymbol{A}_1}\otimes_{\mathcal{O}^{\mathrm{sh}}_{X_N}}\mathcal{O}^{\mathrm{sh}}_{Y_2,\boldsymbol{A}_2}\big).$$

Proof. Starting with Proposition 3.3.1, we use the independence proved in Lemma 3.3.2 of the isomorphism class of a triple from its third component to replace the sum over $x\in\mathcal{X}_\vartheta(k)$ by a sum $(\mathbf{A}_1,\mathbf{A}_2)\in(Y_1\times Y_2)_\vartheta(k)$, using that those pairs for which $\mathbf{A}_1$ and $\mathbf{A}_2$ are not isomorphic yield no contribution because the points do not intersect. Next, we replace $\mathrm{length}\big(\mathcal{O}^{\mathrm{sh}}_{\mathcal{X}_\vartheta,x}\big)$ by its scheme-theoretic analogue using Proposition 3.3.3 above to complete the proof. □

3.4 Group actions

Let $W_N=\{1,w_p,w_q,w_N\}$ denote the Atkin-Lehner group, consisting of the identity and three non-trivial involutions. It is explained in Phillips's thesis [Phi15] how the group $\mathrm{Pic}(K_i)\times W_N$ acts on the set of false elliptic curves with CM by $\mathcal{O}_i$ over any $\mathcal{O}_L$-scheme S. It is important to know how the group actions on these embeddings relate to the reflex ideal. This is established in the following quick lemmas.

Lemma 3.4.1. *Let* $(\boldsymbol{A}_1,\boldsymbol{A}_2)$ *be a CM-pair inducing the morphism* $\vartheta\in\mathcal{V}$*. Then for any pair of ideals* $([c_1],[c_2])\in\mathrm{Pic}(K_1)\times\mathrm{Pic}(K_2)$*, the CM-pair* $([c_1]\cdot\boldsymbol{A}_1,[c_2]\cdot\boldsymbol{A}_2)$ *also induces the map* $\vartheta\in\mathcal{V}$*.*

Proof. This is almost immediate from the disccusion in [Phi15] on page 39. There the action of the product of the Picard groups on the CM pairs of Shimura curves is described and it is shown that this leaves the induced ring maps $\mathcal{O}_{K_j} \to B_N/m_N$ invariant. □

Lemma 3.4.2. *Let $(\boldsymbol{A}_1, \boldsymbol{A}_2)$ be a CM-pair inducing the reflex ideal $\mathfrak{a} = \mathfrak{p}_i\mathfrak{q}_j \in \mathcal{I}$. Then the CM-pairs $(w_p \cdot \boldsymbol{A}_1, \boldsymbol{A}_2)$ and $(\boldsymbol{A}_1, w_p \cdot \boldsymbol{A}_2)$ induce reflex ideal $\mathfrak{p}_k\mathfrak{q}_j$ with $k \neq i$, and the CM-pairs $(w_q \cdot \boldsymbol{A}_1, \boldsymbol{A}_2)$ and $(\boldsymbol{A}_1, w_q \cdot \boldsymbol{A}_2)$ induce reflex ideal $\mathfrak{p}_i\mathfrak{q}_l$ with $l \neq j$.*

Proof. As described in [Phi15], the action of w_p is given by conjugation with an element π in B_N of norm p on the embedding $\iota : R_N \to \mathrm{End}(A)$. This means that the action on ϑ, which is induced by ι and κ, is also given by conjugation by π. Extending scalars to $\mathbb{Q}_p$, Equation (2.20) in [HY12] shows that we have the decomposition $R_N = \mathbb{Z}_{p^2} \oplus \mathbb{Z}_{p^2}\pi$ with the action of π given by $x\pi = \pi x^\sigma$, where σ is the unique automorphism of $\mathrm{Gal}(\mathbb{Q}_{p^2}/\mathbb{Q}_p)$. Here we may choose $\mathbb{Z}_{p^2} = \vartheta_1(K_1) \otimes \mathbb{Z}_p$. Then this shows that conjugating with π induces the non-trivial automorphism on the image of ϑ and thus will change the reflex prime above p, as claimed. The situation for w_q is analogous. □

Corollary 3.4.3. *For any given $\vartheta \in \mathcal{V}$, the space $(Y_1 \times Y_2)_\vartheta(k)$ is a principal homogeneous space for the action of $\mathrm{Pic}(K_1) \times \mathrm{Pic}(K_2)$. In addition, the set $\mathcal{V}$ itself is a principal homogenous space for the action of $W_N \times W_N$ and the set $\mathcal{I}$ is so for $W_N \subset W_N \times W_N$ acting diagonally.*

Proof. The first two claims follow from Lemma 3.4.1 and Lemma 3.4.2 above, together with the elementary fact that $\#\mathcal{V} = 16$ and the knowledge that the set of CM-points for $\mathcal{O}_i$ is a principal homogeneous space for the action of $\mathrm{Pic}(K_i) \times W_N$, as shown in [Phi15]. For the third, note that w_p and w_q change the reflex ideal at one prime, so in order to leave it invariant, we must act by the same operator on both CM-points. □

Lemma 3.4.4. *For any CM-point P, it holds that $P' \in \mathrm{Pic}(K_i) \cdot w_q(P)$.*

Proof. Recall that $P' := w_p(\mathrm{Frob}_p(P))$. By applying w_p to the above equation, it follows that it suffices to show that $\mathrm{Frob}_p(P) \in \mathrm{Pic}(K_i) \cdot w_N(P)$. As the set of CM-points for $\mathcal{O}_i$ is a principal homogeneous space for the action of $\mathrm{Pic}(K_i) \times W_N$, by Lemma 3.4.3 above we reduce to comparing the reflex ideal associated with the pairing of the points $\mathrm{Frob}_p(P)$ and $w_N(P)$ with any other CM-point. Now indeed, by Lemma 3.4.2, the latter induces the Galois conjugate reflex ideal compared to P, which coincides with the Galois action of $\mathrm{Frob}_p(P)$. □

3.5 Proof of Theorem A

In order to obtain a new formula for $\deg(X_\vartheta)$ for $\vartheta \in \mathcal{V}$, as a result of Corollary 3.3.4, we must proceed to analyse the quantities

$$\mathrm{length}\big(\mathcal{O}^{\mathrm{sh}}_{Y_1,\mathbf{A}_1} \otimes_{\mathcal{O}^{\mathrm{sh}}_{X_N}} \mathcal{O}^{\mathrm{sh}}_{Y_2,\mathbf{A}_2}\big)$$

for $(\mathbf{A}_1, \mathbf{A}_2) \in (Y_1 \times Y_2)_\vartheta(k)$. This analysis is facilitated by the existence of the isomorphism

$$j_N : X_N \xrightarrow{\sim} \mathbb{P}^1.$$

We will need the following theorem.

Theorem 3.5.1. *For any positive integer N, the Shimura curve X_N is semistable and has good reduction at all the primes not dividing N.*

This is proved for instance in Morita's master thesis [Mor70]. Let $\mathfrak{r} \subset \mathcal{O}_L$ be a prime and let $\mathfrak{X}_{N,\mathfrak{r}}$ be a semistable model of X_N over $\mathrm{Spec}(\mathcal{O}_{L,\mathfrak{r}})$. Further, let $W_\mathfrak{r}$ denote the ring of integers of the completion of the maximal unramified extension of $L_\mathfrak{r}$. By Theorem 3.5.1, if $\mathfrak{r} \nmid N$, the completed local ring of any $W_\mathfrak{r}$-point on $\mathfrak{X}_{N,\mathfrak{r}}$ must be isomorphic to $W_\mathfrak{r}[\![x]\!]$. If $\mathfrak{r} \mid N$, then because we chose a semistable model of $\mathfrak{X}_{N,r}$, at all geometric singular points on the special fibre the completed local ring is isomorphic to $W_\mathfrak{r}[\![x,y]\!]/(xy - \varpi)$, where ϖ denotes a uniformiser inside $W_\mathfrak{r}$. Because all CM-points are globally defined over the fields H_i for $i \in \{1,2\}$ by Corollary 2.1.5, both of which are unramified at r because we assume r be coprime to both D_i for $i \in \{1,2\}$, CM-points can never reduce to singular points on the special fibre of $\mathfrak{X}_{N,\mathfrak{r}}$ by Remark 2.4.3 in [Rom13]. As such, the completed local ring at a geometric CM-point on $\mathfrak{X}_{N,\mathfrak{r}}$ is always isomorphic to $W_\mathfrak{r}[\![x]\!]$.

Similar to Proposition 2.26 in [HY12], we find that the completion of the strictly Henselian local ring of a CM point on the special fibre is isomorphic to $W_\mathfrak{r}$. Therefore, for $x \in (Y_1 \times Y_2)_\vartheta(k)$, we obtain two maps

$$\mathrm{Spec}(W_\mathfrak{r}) \to \mathrm{Spec}(\mathcal{O}^{\mathrm{sh}}_{\mathfrak{X}_N,x}) \xrightarrow{\sim} \mathrm{Spec}(W_\mathfrak{r}[\![X]\!])$$

induced by the unique (up to local units) scalar multiple $j_{N,\mathfrak{r}}$ of j_N that induces an isomorphism over $W_\mathfrak{r}$ away from the singular points, if there are any. These maps correspond to two ring maps $W_\mathfrak{r}[\![X]\!] \to W_\mathfrak{r}$.

Lemma 3.5.2. *Let R be a commutative ring and consider two maps $f_1, f_2\colon R[x] \to R$ defined by $f_1(x) = a$ and $f_2(x) = b$ for certain $a, b \in R$. Then*

$$R \otimes_{f_1,R[x],f_2} R \cong R/(a-b).$$

We omit the proof, as it is just commutative algebra. If we let $P_{\mathbf{A}_i}$ denote the CM-point on X_N defining the CM-false elliptic curve $\mathbf{A}_i$, then the lemma above has the following immediate corollary.

Corollary 3.5.3. *For any prime $\mathfrak{r} \subset \mathcal{O}_L$ and pair of CM points $x = (\boldsymbol{A}_1, \boldsymbol{A}_2) \in (Y_1 \times Y_2)_\vartheta(k)$ where $k = \overline{\mathbb{F}}_\mathfrak{r}$, it holds that*

$$\operatorname{length}\big(\mathcal{O}^{\mathrm{sh}}_{Y_1,x} \otimes_{\mathcal{O}^{\mathrm{sh}}_{\mathfrak{X}_N,x}} \mathcal{O}^{\mathrm{sh}}_{Y_2,x}\big) = v_\mathfrak{r}\big(j_{N,\mathfrak{r}}(P_{\boldsymbol{A}_1}) - j_{N,\mathfrak{r}}(P_{\boldsymbol{A}_2})\big).$$

Proof. We apply Lemma 3.5.2 to equate the left hand side of the above expression to length $\big(W_\mathfrak{r}/\big(j_{N,\mathfrak{r}}(P_{\mathbf{A}_1}) - j_{N,\mathfrak{r}}(P_{\mathbf{A}_2})\big)\big)$. We leave it to the reader to check that this length is just the $\mathfrak{r}$-adic valuation. □

Corollary 3.5.4. *Let $\vartheta \in \mathcal{V}$. Then it holds that*

$$\deg(\mathcal{X}_\vartheta) = \frac{2}{w_1 w_2} \sum_{\mathfrak{r} \subset \mathcal{O}_L} \log(|\mathbb{F}_\mathfrak{r}|) \sum_{[c_1],[c_2]} v_\mathfrak{r}\big(j_{N,\mathfrak{r}}(P_{[c_1]\cdot \boldsymbol{A}_1}) - j_{N,\mathfrak{r}}(P_{[c_2]\cdot \boldsymbol{A}_2})\big),$$

where the latter sum ranges over all $[c_1] \in \operatorname{Pic}(K_1)$ and $[c_2] \in \operatorname{Pic}(K_2)$.

Proof. First substitute the result from Corollary 3.5.3 into the expression found in Corollary 3.3.4. The proof is then complete by Corollary 3.4.3, which identifies $(Y_1 \times Y_2)_\vartheta(k)$ as a principal homogeneous space for the action of the group $\operatorname{Pic}(K_1) \times \operatorname{Pic}(K_2)$. □

Now let $\mathcal{V}' = (W_q \times W_q) \cdot \vartheta \subset \mathcal{V}$ where $W_q = \{1, w_q\} \subset W_N$. We will study the sum

$$\sum_{\vartheta \in \mathcal{V}'} \delta(\vartheta) \deg(\mathcal{X}_\vartheta).$$

Proposition 3.5.5. *Let $\vartheta \in \mathcal{V}$. Then it holds that*

$$\sum_{\vartheta \in \mathcal{V}'} \delta(\vartheta) \deg(\mathcal{X}_\vartheta) = \frac{2}{w_1 w_2} \log \operatorname{Nm}\big[j_N(P_{\boldsymbol{A}_1}), j_N(P'_{\boldsymbol{A}_1}), j_N(P_{\boldsymbol{A}_2}), j_N(P'_{\boldsymbol{A}_2})\big].$$

Proof. The key idea is that for any prime $\mathfrak{r} \subset \mathcal{O}_L$, the sum

$$\sum_{\vartheta \in \mathcal{V}'} \delta(\vartheta) v_\mathfrak{r}\big(j_{N,\mathfrak{r}}(P_{\mathbf{A}_1}) - j_{N,\mathfrak{r}}(P_{\mathbf{A}_2})\big)$$

is equal to

$$v_\mathfrak{r}\left(\frac{j_{N,\mathfrak{r}}(P_{\mathbf{A}_1}) - j_{N,\mathfrak{r}}(P_{\mathbf{A}_2})}{j_{N,\mathfrak{r}}(w_q P_{\mathbf{A}_1}) - j_{N,\mathfrak{r}}(P_{\mathbf{A}_2})} \cdot \frac{j_{N,\mathfrak{r}}(w_q P_{\mathbf{A}_1}) - j_{N,\mathfrak{r}}(w_q P_{\mathbf{A}_2})}{j_{N,\mathfrak{r}}(P_{\mathbf{A}_1}) - j_{N,\mathfrak{r}}(w_q P_{\mathbf{A}_2})}\right).$$

This cross-ratio is independent of the precise way we scaled our function $j_{N,\mathfrak{r}}$, and as such, we may replace every instance of it by our original fixed choice of j_N. Next, by Lemma 3.4.4, we find that for certain classes $[d_i] \in \mathrm{Pic}(K_i)$ for $i \in \{1,2\}$, we have the equality $w_q P_{\mathbf{A}_i} = [d_i] \cdot P'_{\mathbf{A}_i}$. Therefore, we may further rewrite this sum to

$$v_{\mathfrak{r}}\left(\frac{j_N(P_{\mathbf{A}_1}) - j_N(P_{\mathbf{A}_2})}{j_N([d_1]\cdot P'_{\mathbf{A}_1}) - j_N(P_{\mathbf{A}_2})} \cdot \frac{j_N([d_1]\cdot P'_{\mathbf{A}_1}) - j_N([d_2]\cdot P'_{\mathbf{A}_2})}{j_N(P_{\mathbf{A}_1}) - j_N([d_2]\cdot P'_{\mathbf{A}_2})}\right).$$

If we now introduce the sum over $\mathrm{Pic}(K_1)\times\mathrm{Pic}(K_2)$, the twist by the classes $[d_i] \in \mathrm{Pic}(K_i)$ for $i \in \{1,2\}$ can be ignored, and we obtain

$$\sum_{([c_1],[c_2])} v_{\mathfrak{r}}\left(\frac{j_{N,\mathfrak{r}}(P_{[c_1]\cdot\mathbf{A}_1}) - j_{N,\mathfrak{r}}(P_{[c_2]\cdot\mathbf{A}_2})}{j_{N,\mathfrak{r}}(P'_{[c_1]\cdot\mathbf{A}_1}) - j_{N,\mathfrak{r}}(P_{[c_2]\cdot\mathbf{A}_2})} \cdot \frac{j_{N,\mathfrak{r}}(P'_{[c_1]\cdot\mathbf{A}_1}) - j_{N,\mathfrak{r}}(P'_{[c_2]\cdot\mathbf{A}_2})}{j_{N,\mathfrak{r}}(P_{[c_1]\cdot\mathbf{A}_1}) - j_{N,\mathfrak{r}}(P'_{[c_2]\cdot\mathbf{A}_2})}\right).$$

Now recall Shimura's reciprocity law, Corollary 2.1.5, which has the consequence that taking an average over the class groups amounts to taking the norm of the cross ratio above in the unramified field extension H_1H_2/L. In other words,

$$\prod_{[c_1],[c_2]} \left[j_N(P_{[c_1]\cdot\mathbf{A}_1}), j_N(P'_{[c_1]\cdot\mathbf{A}_1}), j_N(P_{[c_2]\cdot\mathbf{A}_2}), j_N(P'_{[c_2]\cdot\mathbf{A}_2})\right]$$

is equal to the norm $\mathrm{Nm}_L^{H_1H_2}[j_N(P_{\mathbf{A}_1}), j_N(P'_{\mathbf{A}_1}), j_N(P_{\mathbf{A}_2}), j_N(P'_{\mathbf{A}_2})]$. Combining all of this, using Corollary 3.5.4, we have proved that the left hand side of the proposition is equal to

$$\frac{2}{w_1w_2}\sum_{\mathfrak{r}\subset\mathcal{O}_L} \log(|\mathbb{F}_{\mathfrak{r}}|) v_{\mathfrak{r}}\left(\mathrm{Nm}_L^{H_1H_2}\left[j_N(P_{\mathbf{A}_1}), j_N(P'_{\mathbf{A}_1}), j_N(P_{\mathbf{A}_2}), j_N(P'_{\mathbf{A}_2})\right]\right).$$

We thus complete the proof is we can show for any $x \in L$ that

$$\sum_{\mathfrak{r}\subset\mathcal{O}_L} \log(|\mathbb{F}_{\mathfrak{r}}|)v_{\mathfrak{r}}(x) = \log(\mathrm{Nm}(x)), \quad \text{so that} \quad \prod_{r\subset\mathcal{O}_L} |\mathbb{F}_{\mathfrak{r}}|^{v_{\mathfrak{r}}(x)} = \mathrm{Nm}(x).$$

Indeed, this follows by factoring the principal ideal $x\mathcal{O}_L$ into prime ideals and then using the definition of the ideal norm. □

Proof. (of Theorem A) We exponentiate the result of Proposition 3.5.5 to find that

$$\prod_{\vartheta\in\mathcal{V}'} \exp\big(\delta(\vartheta)\deg(\mathcal{X}_\vartheta)\big) = \mathrm{Nm}\big[j_N(P_{\mathbf{A}_1}), j_N(P'_{\mathbf{A}_1}), j_N(P_{\mathbf{A}_2}), j_N(P'_{\mathbf{A}_2})\big]^{\frac{2}{w_1w_2}}$$

so that we reduce to showing that

$$\prod_{\vartheta\in\mathcal{V}'}\exp\big(\delta(\vartheta)\deg(\mathcal{X}_\vartheta)\big)=\pm\prod_{\substack{x^2<D\\ x^2\equiv D \bmod 4N}}F\left(\frac{D-x^2}{4N}\right)^{\delta(x)}.$$

Now we recall the result of Theorem 3.2.5, and on both sides we now take a product over all $\nu\in\mathcal{D}_F^{-1,+}$ with $\mathrm{tr}(\nu)=1$. We then obtain that

$$\begin{aligned}\prod_{\substack{x^2<D\\ x^2\equiv D \bmod 4N}}F\left(\frac{D-x^2}{4N}\right)^{\delta(x)}&=\prod_{\substack{\nu\in\mathcal{D}_F^{-1,+}\\ \mathrm{tr}(\nu)=1}}\prod_{\mathfrak{a}\in\mathcal{I}}\exp\big(\delta(\mathfrak{a})X(\mathfrak{a},\nu)\big)\\ &=\prod_{\mathfrak{a}\in\mathcal{I}}\exp\Big(\delta(\mathfrak{a})\sum_{\substack{\nu\in\mathcal{D}_F^{-1,+}\\ \mathrm{tr}(\nu)=1}}X(\mathfrak{a},\nu)\Big)=\prod_{\mathfrak{a}\in\mathcal{I}}\exp\big(\delta(\mathfrak{a})X(\mathfrak{a})\big).\end{aligned}$$

We have thus reduced to showing that

$$\prod_{\vartheta\in\mathcal{V}'}\exp\big(\delta(\vartheta)\deg(\mathcal{X}_\vartheta)\big)=\prod_{\mathfrak{a}\in\mathcal{I}}\exp\big(\delta(\mathfrak{a})X(\mathfrak{a})\big).$$

Both sides of this equation display a product with four factors, so we complete the proof if we make four pairs of equal factors. Choose $\vartheta\in\mathcal{V}'$ arbitrarily and assume without loss of generality that its associated reflex ideal equals $\mathfrak{a}_\vartheta=\mathfrak{p}_1\mathfrak{q}_1\in\mathcal{I}$. Then by construction,

$$\delta(\vartheta)\deg(\mathcal{X}_\vartheta)=\delta(\mathfrak{a})X(\mathfrak{a}).$$

By Lemma 3.4.2, the other elements of $\mathcal{V}'$, explicitly $(w_q,1)\cdot\vartheta$, $(1,w_q)\cdot\vartheta$ and $(w_q,w_q)\cdot\vartheta$, induce reflex ideals $\mathfrak{p}_1\mathfrak{q}_2$, $\mathfrak{p}_1\mathfrak{q}_2$ and $\mathfrak{a}$ respectively. To complete the proof, we will show that $X(\mathfrak{a})=X(\sigma(\mathfrak{a}))$ for any $\mathfrak{a}\in\mathcal{I}$. For if so, then the latter two elements of $\mathcal{V}'$ also have equal contributions as the ideals $\sigma(\mathfrak{p}_1\mathfrak{q}_2)=\mathfrak{p}_2\mathfrak{q}_1$ and $\sigma(\mathfrak{a})=\mathfrak{p}_2\mathfrak{q}_2$ respectively, and we win.

As $X(\mathfrak{a})$ is the sum over all $X(\mathfrak{a},\nu)$, it suffices to examine these latter quantities. Indeed, Theorem 3.1.3 shows that $X(\mathfrak{a},\nu)=X(\sigma(\mathfrak{a}),\sigma(\nu))$, as is obtained by applying σ to all quantities occurring in that theorem. Since we sum over all $\nu\in\mathcal{D}_F^{-1,+}$ of unit trace, a set which is stable under the action of σ, equality follows and the proof is complete. □