Michigan Math. J. 72 (2022), 145–207
https://doi.org/10.1307/mmj/20217221

The Derived Hecke Algebra for Dihedral Weight One Forms

Henri Darmon, Michael Harris,
Victor Rotger & Akshay Venkatesh

To Gopal Prasad on his 75th birthday

Abstract. We study the action of the derived Hecke algebra in the setting of dihedral weight one forms and prove a conjecture of the second- and fourth- named authors relating this action to certain Stark units associated to the symmetric square L-function. The proof exploits the theta correspondence between various Hecke modules as well as the ideas of Merel and Lecouturier on higher Eisenstein elements.

1. Introduction

In the theory of modular forms, the case of weight one is exceptional in several ways. The space of weight one forms, which can be interpreted as the global sections of the Hodge line bundle ω on a modular curve X, does not admit a simple dimension formula. This occurs precisely because the higher cohomology group $H^1(X, \omega)$ can be nontrivial—that is to say, the space of weight one forms manifests itself in two different cohomological degrees.

A conjecture proposed in [PV; GV18; Ven; HV] asserts that, in situations where spaces of automorphic forms occur across multiple cohomological degrees, the different degrees are related by means of a hidden action of a motivic cohomology group. The last mentioned paper [HV], in particular, formulates this story in the context of weight one forms for the modular curve and translates the general conjectures into a numerically testable statement. This statement, which is summarized in what follows, is the main topic of this paper.

Received October 18, 2021. Revision received April 1, 2022.

The first author was supported by an NSERC Discovery grant. The second and fourth authors were supported by the National Science Foundation under Grant No. DMS-1440140 while they were in residence at the Mathematical Sciences Research Institute in Berkeley, California, during the Spring 2019 semester. The second author was also supported by the National Science Foundation under Grants No. DMS-1701651 and DMS-2001369. The third author was supported by an ERC consolidator grant and Icrea Academia. The last-named author was supported by NSF grant DMS-1931087. This project has received funding from the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme (grant agreement No 682152).

1.1. The Shimura Class

Although the general definition of derived Hecke operators shall not be recalled here, one crucial ingredient in their construction is to take the cup product with a certain distinguished class in coherent cohomology, the so-called *Shimura class.*

As explained in detail in [HV, §3.1], the Shimura class attached to a prime $N \geq 5$ arises from the covering $X_1(N) \to X_0(N)$ of classical modular curves, which (at least away from elliptic points) is étale with deck group $(\mathbb{Z}/N\mathbb{Z})^\times$ and thus furnishes an element

$$\mathfrak{S}^\times \in H^1_{\text{et}}(X_0(N), (\mathbb{Z}/N\mathbb{Z})^\times \otimes \mathbb{Z}[1/6]).$$

(Here, and in what follows, modular curves will be regarded as schemes over the ring $Z = \mathbb{Z}[\frac{1}{6N}]$ to avoid any technical issues.)

Let $p > 3$ be a prime, let p^t be the highest power of p dividing $N - 1$, assume $t \geq 1$, and fix a surjective *discrete logarithm*

$$\log : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{Z}/p^t\mathbb{Z}. \tag{1}$$

This choice determines a class $\mathfrak{S} := \log(\mathfrak{S}^\times) \in H^1_{\text{et}}(X_0(N), \mathbb{Z}/p^t)$. Restricting to the fiber product of $X_0(N)$ over $\text{Spec}(Z)$ with $\text{Spec}(\mathbb{Z}/p^t\mathbb{Z})$, denoted by $\bar{X} = X_0(N)_{/\mathbb{Z}/p^t\mathbb{Z}}$, the resulting class can be pushed into Zariski cohomology using the inclusion of $\mathbb{Z}/p^t\mathbb{Z}$ into the étale sheaf represented by $\mathbb{G}_a$: in this way $\mathfrak{S}$ can be viewed as a class in coherent cohomology. It is called the *Shimura class,* denoted (by a slight abuse of notation)

$$\mathfrak{S} \in H^1(\bar{X}, \mathcal{O}_{\bar{X}}) = \text{Hom}(S_2(N), \mathbb{Z}/p^t\mathbb{Z}),$$

where the last identification is provided by Serre duality, and $S_2(N)$ is the space of weight N cusp forms (with q-expansions integral at p). Note that $\mathfrak{S}$ depends on N, on p, and on the choice of discrete logarithm.

1.2. The Main Result

Let $g \in H^0(X_1(d), \omega)$ be a Hecke new cusp form of weight 1, level d, and Nebentypus χ, and let $g^* \in H^0(X_1(d), \omega)$ be the dual newform whose Fourier expansion is related to that of g by complex conjugation and whose automorphic representation is obtained from that of g by twisting by χ^{-1}. Assume for simplicity that the primes N and p do not divide $6d$.

Let $\rho_g : G_{\mathbb{Q}} \longrightarrow \text{GL}_2(L) \simeq \text{Aut}(V_g)$ be the odd two-dimensional Artin representation attached by Deligne and Serre to g, acting on a two-dimensional L-vector space V_g for a suitable finite extension L of $\mathbb{Q}$ (containing the Fourier coefficients of g and contained in a cyclotomic field). Let $\text{Ad}(\rho_g)$ denote the three-dimensional subrepresentation of $\text{End}_L(V_g)$ consisting of L-linear endomorphisms of V_g of trace zero, equipped with the natural action of $G_{\mathbb{Q}}$ by conjugation.

Let R be the ring of integers of L with $6N$ inverted. The product $g(z)g^*(Nz)$ is a weight 2 cuspidal modular form of level Nd with trivial nebentypus character

and coefficients in R, and can thus be viewed as an element of the space $S_2(Nd) = H^0(X_0(Nd), \Omega^1)$ of global regular differential forms. Let

$$G(z) := \mathrm{Tr}_N^{Nd}(g(z)g^*(Nz)) \in S_2(N; R) = H^0(X_0(N)_{/R}, \Omega^1)$$

denote the trace of $g(z)g^*(Nz)$ to the space of modular forms of weight 2 and level N.

The pairing between G and the Shimura class $\mathfrak{S}$ arising from Serre duality gives rise to a numerical invariant

$$\langle G, \mathfrak{S} \rangle \in R/p^t,$$

see Section 1.5 for details. The conjecture of [HV] relates this quantity to the discrete logarithm of a suitable Stark unit attached to g, which we now proceed to describe.

The image of the integral group ring $R[G_{\mathbb{Q}}]$ in $\mathrm{Ad}(\rho_g)$ endows this space with a Galois-stable R-sublattice, which is denoted by $\mathrm{Ad}(\rho_g)^\circ$, and whose R-linear dual is denoted by $\mathrm{Ad}^*(\rho_g)^\circ$.

Let H denote the finite extension of $\mathbb{Q}$ which is cut out by $\mathrm{Ad}(\rho_g)$. Because complex conjugation acts with eigenvalues 1, -1, and -1 on this representation, Dirichlet's unit theorem asserts that the R-module

$$U_g := (\mathcal{O}_H^\times \otimes \mathrm{Ad}^*(\rho_g)^\circ)^{G_{\mathbb{Q}}}$$

is of rank one (cf. Lemma 2.7 of [HV]). The choice of a prime $\mathcal{N}$ of H above N gives rise to a Frobenius element σ_N, whose image under ρ_g is a natural element of $\mathrm{Ad}(\rho_g)^\circ$ which is invariant under the conjugation action of σ_N. Evaluation at σ_N thus gives rise to a homomorphism from $\mathrm{Ad}^*(\rho_g)^\circ$ to R which is σ_N-equivariant (for the trivial σ_N action on R). Combining this evaluation with the reduction modulo $\mathcal{N}$ gives a "mod N reduction map"

$$\mathrm{red}_N : U_g := (\mathcal{O}_H^\times \otimes \mathrm{Ad}^*(\rho_g)^\circ)^{G_{\mathbb{Q}}} \longrightarrow ((\mathcal{O}_H/\mathcal{N})^\times \otimes R)^{\sigma_N = 1} = (\mathbb{Z}/N\mathbb{Z})^\times \otimes R.$$

A version of the main conjecture of [HV] (Conjecture 3.1 in loc. cit.) may be phrased as follows.

CONJECTURE 1.1. *There exists an integer $m = m_g \geq 1$ and $u_g \in U_g$ such that, for all primes N and p as before,*

$$m \cdot \langle G, \mathfrak{S} \rangle = \log(\mathrm{red}_N(u_g)).$$

Note that both sides of this conjectured identity belong to R/p^t and that both depend linearly on the choice of discrete logarithm made in (1). The validity of Conjecture 1.1 is thus independent of this choice. Similarly, both sides of the conjecture are independent of the choice of $\mathcal{N}$. (In loc. cit. the conjecture was formulated differently and was slightly more precise about the primes dividing m; the version is more explicit and is what we will prove in certain cases.)

This article presents a proof of Conjecture 1.1 when g is *dihedral* under certain simplifying assumptions on ramification. Recall that g is said to be dihedral if the Galois representation ρ_g is induced from a ray class character ψ_1 of the Galois group of an (imaginary or real) quadratic extension K of $\mathbb{Q}$. In that case $g = \theta_{\psi_1}$

is Hecke's classical theta series associated to ψ_1, that is, the modular form whose L-series is given by $L(K, \psi_1)$. We assume throughout that $\psi_1^2 \neq 1$, as this implies that θ_{ψ_1} is cuspidal.

Let D denote the discriminant of K and $\delta = (\sqrt{D})$ its different.

THEOREM 1.2. *If K is imaginary, then assume that D is an odd prime and that ψ_1 is unramified. If K is real, then assume that D is odd and that ψ_1 has conductor dividing δ. Then Conjecture 1.1 is true for $g = \theta_{\psi_1}$.*

REMARK 1.3. The proof of Theorem 1.2 described in Section 5 shows that the integer m of Conjecture 1.1 divides 24 in the real case and that it divides 6 in the imaginary case unless the order of ψ_1^2 is a power of a prime ℓ, in which case m divides 6ℓ. No claim is made that these bounds for m are optimal; they are merely what comes directly out of the proofs.

The key idea in the proof of Theorem 1.2 is to express G as the theta lift of an appropriate *Heegner cycle,* and to compute the image of $\mathfrak{S}$ under the adjoint of the theta lift as a combination of *higher Eisenstein elements.* Although the latter computation is performed in full generality, the expression for G in terms of Heegner cycles has only been worked out in a nontrivial simple scenario.

In particular, the ramification conditions force the following simplifying feature. Let ψ_1' denote the $\mathrm{Gal}(K/\mathbb{Q})$-conjugate of ψ_1 and set $\psi = \psi_1/\psi_1'$. Then

$$\rho_g \otimes \rho_{g^*} = \mathrm{Ind}_{\mathbb{Q}}^K(1) \oplus \mathrm{Ind}_{\mathbb{Q}}^K(\psi) \tag{2}$$

decomposes as the direct sum of the induced representations of two characters of G_K, the trivial character 1, and an *unramified* character ψ. R. Zhang's forthcoming Ph.D thesis [Zha] will contain a proof under less restrictive ramification conditions for K imaginary. When K is real, we envisage a method for calculating G invoking Kudla–Millson theory, but in order to cover the general case, one needs to solve some issues related to the regularization of the theta lift from the split orthogonal group; see Section 1.4 for more details.

1.3. Trivial Cases

If K is imaginary quadratic and $N = \mathfrak{N} \cdot \mathfrak{N}'$ splits in K, then u_g belongs to $(\mathcal{O}_H^\times \otimes \mathrm{Ind}_{\mathbb{Q}}^K(\psi))^{G_{\mathbb{Q}}}$, whereas σ_N belongs to $\mathrm{Ind}_{\mathbb{Q}}^K(1)$. If K is real quadratic and N is inert in K, then u_g belongs to the unit group $\mathfrak{o}^\times$ of K, on which σ_N acts as -1. In both cases the regulator $\mathrm{red}_N(u_g)$ of Conjecture 1.1 vanishes trivially.

This is consistent with the fact that the modular form G is identically zero in these two scenarios. Indeed, the main theorem of [HK91] asserts that, for all newforms f of weight two on $\Gamma_0(N)$,

$$\langle G, f \rangle^2 = C \cdot L(f, g, g^*, 1), \tag{3}$$

where C is a product of local automorphic terms and $L(f, g, g^*, s)$ is the triple product L-series associated to f, g, and g^*. The Artin formalism applied to (2)

implies that

$$L(f, g, g^*, s) = L(f/K, s) \cdot L(f/K, \psi, s), \tag{4}$$

where the two L-functions appearing on the right-hand side are the ones associated to the base change of f to K, twisted by suitable characters. Since $(d, N) = 1$, both $L(f/K, s)$ and $L(f/K, \psi, s)$ satisfy a functional equation with $s = 1$ as the center of symmetry and the global sign $(\frac{-N}{K})$. This sign is -1, and hence

$$L(f/K, 1) = L(f/K, \psi, 1) = 0.$$

It follows that $\langle G, f \rangle = 0$ for all f, and hence that $G = 0$.

1.4. Outline of the Paper

The interesting cases of Theorem 1.2 occur when $(\frac{-N}{K}) = 1$, that is, when

- K is imaginary quadratic and N is inert in K;
- K is real quadratic and N is split in K.

The body of the article is devoted to the proof of Theorem 1.2 in these nontrivial cases referred to as the *definite* and *indefinite* cases respectively. The main idea is to transfer the computation to a suitable (definite, resp. indefinite) quaternion algebra B over $\mathbb{Q}$ by means of a theta lift Θ:

$$\Theta : \text{modular forms on } B^* \to S_2(N).$$

This allows the identity in Conjecture 1.1 to be recast on B^*. Indeed, G and $\mathfrak{S}$ are obtained via Θ from objects arising (respectively) from

(i) CM points or real quadratic closed geodesics;
(ii) Siegel units.

Let us examine these two key ingredients in further detail.

Ingredient (i), in general, takes the form

$$G =_{\mathfrak{S}} \Theta(Z_{K,\psi}), \tag{5}$$

where $Z_{K,\Psi}$ is a suitable Heegner cycle and the symbol "$=_{\mathfrak{S}}$" means equality up to modular forms that pair to 0 with the Shimura class (see Section 1.5 for some details). More precisely, $Z_{K,\Psi}$ is a formal linear combination of supersingular points in characteristic N, obtained as a weighted combination of the mod N reductions of CM elliptic curves in the definite case (Theorem 2.2), and a linear combination of real quadratic geodesics in the homology of $X_0(N)$ in the indefinite case (Theorem 3.1). Equality (5) can be interpreted as coming from a certain see-saw (Remark 1.4) although we give a rather direct proof.

The content of (ii) is the computation of the image of the Shimura class under the *adjoint* (dual, in other words) of the theta lift. The outcome is an expression

$$\Theta^*(\mathfrak{S}) = \text{explicit } \textit{higher Eisenstein element } \mathfrak{U}_N. \tag{6}$$

In the definite case, $\mathfrak{U}_N$ is obtained by restricting a suitable Siegel unit to the supersingular locus in characteristic N. In the indefinite case, $\mathfrak{U}_N$ is built out of the modular symbol arising from the (logarithmic derivative of the) same Siegel

unit. In all cases, the basic idea of proof is that $\Theta^*(\mathfrak{S})$ is *uniquely characterized by its behavior with respect to Hecke operators* and so can be proved to equal $\mathfrak{U}_N$, up to an irrelevant ambiguity, by a purely Hecke-theoretic computation. Most of the work for the proof of (6) is given in Section 4, building on ideas of Mazur, Merel, and Lecouturier on (higher) Eisenstein elements and the classical theory of modular units and modular symbols.

Combining (5) and (6) leads to an identity of the form

$$\langle G, \mathfrak{S}\rangle = \langle \Theta(Z_{K,\psi}), \mathfrak{S}\rangle = \langle Z_{K,\psi}, \Theta^*(\mathfrak{S})\rangle = \langle Z_{K,\psi}, \mathfrak{U}_N\rangle. \tag{7}$$

In the definite setting, the right-hand quantity can be interpreted as the discrete logarithm of an elliptic unit, obtained by evaluating the Siegel unit attached to $\mathfrak{U}_N$ on the CM divisor attached to $Z_{K,\psi}$. In the indefinite setting, the regulator involves only the logarithm of the fundamental unit of K, and this fundamental unit emerges in $\langle Z_{K,\psi}, \mathfrak{U}_N\rangle$ from the eigenvalues of certain hyperbolic matrices in $\Gamma_0(N)$. The details of these calculations, concluding with the proof of Theorem 1.2, are supplied in Section 5.

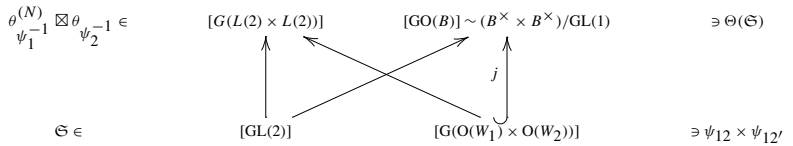
It is worth insisting on a crucial feature of the dihedral case, namely, that the desired units can be constructed explicitly as CM values of modular units in the definite case or as eigenvalues of suitable matrices in $\mathrm{SL}_2(\mathbb{Z})$ in the indefinite case. This is what accounts for Stark's conjecture being known for the adjoint L-functions of dihedral forms. It remains open, however, for the adjoint L-functions of so-called *exotic* weight one forms with nondihedral projective image. Although the existence and essential uniqueness of the predicted unit is still guaranteed by Dirichlet's unit theorem, no analogue of the Kronecker limit formula relating it to L-functions attached to g is available. The numerical experiments described in [HV] test Conjecture 1.1 numerically, but only in CM dihedral cases that now fall under the purview of Theorem 1.2. The article [Mar] provides numerical evidence for Conjecture 1.1 in several more interesting instances where g is exotic.

REMARK 1.4. It may be helpful to indicate the see-saw that underlies the crucial computation (5). We emphasize, however, that the proofs in Sections 2 and 3 do not use this in any explicit way.[1] Here we will proceed purely formally.

Set

$$G(L(2)\times L(2)) = \{(g_1, g_2) \in \mathrm{GL}(2)\times \mathrm{GL}(2), \det(g_1) = \det(g_2)\}.$$

We examine the following see-saw:



The arrow Θ^* from lower-left to upper-right is a realization of the Jacquet–Langlands correspondence, and we denote its formal adjoint simply by Θ. Of

[1] However, the representation-theoretic perspective appears to be indispensable to treat cases in which the Hecke characters have more general ramification.

course, $\mathfrak{S}$ is not in fact a characteristic zero modular form, but let us proceed as if it were; in the end the proof uses integral normalizations of the θ-correspondence to get around this. The see-saw principle and adjointness respectively give

$$\langle \theta^{(N)}_{\psi_1^{-1}} \theta_{\psi_2^{-1}}, \mathfrak{S} \rangle = \langle Z_{K,\psi}, \Theta^*(\mathfrak{S}) \rangle = \langle \Theta(Z_{K,\psi}), \mathfrak{S} \rangle,$$

where $Z_{K,\psi}$ arises from pushing forward $\psi_{12} \times \psi_{12'}$ under j. In the special case $\psi_2 = \psi_1^{-1}$, this recovers (5) from the point of view of the see-saw formalism.

1.5. Notation

We will fix here some notation that is used throughout the paper. This notation will also be introduced where we use it; we have gathered some of it here as a convenient reference.

Throughout the paper, K denotes a quadratic field with ring of integers $\mathfrak{o}$ and discriminant D. In Section 2 this field is imaginary, and in Section 3 it is real. The symbol $x \mapsto x'$ denotes the nontrivial automorphism of K, and we will allow ourselves to apply it to various associated constructions (elements of K, ideals, characters, etc.)

The narrow class group of K (i.e., the usual class group in the imaginary case) is denoted by $\mathcal{C}$. In Section 3, $\mathcal{C}_D$ will denote the ray class group of K allowing level δ, the different ideal of K. The symbols ψ_1 and ψ_2 denote characters of $\mathcal{C}_D$ with inverse central characters, and we put

$$\psi_{12} := \psi_1 \psi_2, \qquad \psi_{12'} := \psi_1 \psi_2', \tag{8}$$

which in all cases descend to characters of $\mathcal{C}$. In the special case $\psi_2 = \psi_1^{-1}$ which is germane to the proof of Theorem 1.2, the definitions simplify to

$$\psi_{12} = 1, \qquad \psi_{12'} = \psi_1/\psi_1' := \psi, \quad \text{say.} \tag{9}$$

We will use L for a coefficient field for characters ψ as before, that is, L is a number field containing the values of $\psi : \mathcal{C}$ or $\mathcal{C}_D \to L^\times$. In this context, R will denote a suitable ring of integers of L (possibly with denominators at some primes).

We will often denote by g (respectively h) the dihedral forms associated to ψ_1 (respectively ψ_2) with associated Galois representation $\rho_g : G_{\mathbb{Q}} \to \mathrm{GL}(V_g)$. In this situation, we will often denote

$$G := \text{trace to level } \Gamma_0(N) \text{ of } \theta_{\psi_1^{-1}}(Nz)\theta_{\psi_2^{-1}}(z),$$

which in particular becomes the trace of $\theta_{\psi_1}(z)\theta_{\psi_1^{-1}}(Nz)$ in the case $\psi_2 = \psi_1^{-1}$.

The integer $N > 3$ always denotes a prime, and Z denotes the ring $\mathbb{Z}[\frac{1}{6N}]$. The modular curves $X_0(N)$ and $X_1(N)$ are understood[2] to be schemes over Z. We write $H^1_{\text{et}}(X_0(N))$ and $H^1_{\text{B}}(X_0(N))$ to denote, respectively, the étale cohomology

[2]Note that the distinction between "stack" or the associated coarse moduli scheme will make very little difference for our purposes; the cover $X_1(N) \to X_0(N)$ is étale only when considering the stacks, but in any case we are interested only in the $(\mathbb{Z}/p^t)$-subcover which is also étale over the scheme.

of $X_0(N)$ as a scheme over Z, and the Betti cohomology of the Riemann surface $X_0(N)(\mathbb{C})$.

We define the space of cusp forms $S_2(N)$ and the space of modular forms $M_2(N)$ as (free) Z-modules accordingly and define

$$S_2(N)^\vee = \mathrm{Hom}(S_2(N), Z)$$

as their Z-linear duals. For R, a Z-algebra $S_2(N;R) := S_2(N) \otimes_Z R$ is similarly defined as the space of cusp forms with coefficients in R, and likewise for $M_2(N;R)$. For an element $f \in M_2(N;R)$, we will denote by $f^{(d)} \in M_2(Nd;R)$ the modular form with q-expansion $f(q^d)$.

Let p be an odd prime ≥ 5 and let p^t be the largest power of p dividing $N-1$. Fix a surjective "discrete logarithm"

$$\log : (\mathbb{Z}/N\mathbb{Z})^\times \longrightarrow \mathbb{Z}/p^t\mathbb{Z},$$

where p^t is the largest power of p dividing $N-1$. Note that this logarithm factors through the quotient G_N of (10)

$$G_N := (\mathbb{Z}/N\mathbb{Z})^\times/\langle \pm 1\rangle, \tag{10}$$

since p is assumed to be odd. This logarithm also extends uniquely to the multiplicative group of the quadratic extension $\mathbb{F}_{N^2}$ and this extension will also be denoted by log. All formulas will be independent of the choice of logarithm: both sides will scale the same way if one alters it.

REMARK 1.5. In the indefinite case the prime N splits in K and the correct definition of the discrete logarithm entails the choice of one of the two prime divisors of N. This choice is denoted by $\mathfrak{N}$ and the need to pin down a choice introduces a "breaking of symmetry" in the final formula Proposition 5.11 as well as in the intermediate calculations. The choice intervenes at the beginning of Section 3.2.

Given two modular forms F and G of level N, the notation

$$F =_{\mathfrak{S}} G$$

means that "F and G have the same pairing with the Shimura class." (Strictly, the prime p should have been included in the notation, but the choice of p is understood to be fixed.) More precisely, $F =_{\mathfrak{S}} G$ means that:

(1) F, G lie inside $M_2(N;R)$ for R the ring of p-integers in some algebraic number field, and
(2) the reductions $\bar{F}, \bar{G} \in M_2(N; R/p^tR) = H^0(X_0(N)_R, \Omega^1)$ have the same pairing with $\mathfrak{S}$ under the Serre duality pairing

$$H^0(X_0(N)_{R/p^t}, \Omega^1) \otimes H^1(X_0(N)_{R/p^t}, \mathcal{O}) \to R/p^t \tag{11}$$

obtained by taking the cup product to $H^1(X_0(N)_{R/p^t}, \Omega^1)$ and using the "trace" map on the latter. [3]

[3] In the current setting, if $t > 1$, this can be defined using Grothendieck duality for the structural morphism $X_0(N)_{R/p^t} \to \mathrm{Spec} R/p^t$, after for example adding auxiliary level structure to remove any "stacky" structure. This identifies $H^1(\Omega^1)$ with $\mathrm{Hom}(\mathrm{R}\pi_*\mathcal{O}, R/p^t)$, homomorphisms in

This notion is readily seen to be independent of R, that is, compatible with extension of scalars in the obvious sense.

2. A Trace Identity for Definite Theta Series

In [Gro87] and [GZ86], Gross and Zagier proved a formula for the central critical value (resp. derivative) of the L-function attached to the convolution of a cusp form f of weight 2 and a theta series g of weight 1 associated to a character of an imaginary quadratic field K. A substantial step in the proof of both formulas is the computation, for a given prime N, of the trace of the product $g(z)E(Nz)$ of g and a suitable Eisenstein series E to the space of modular forms of level N.

In this note we need to carry the computation of the trace of the product $g(z)h(Nz)$ of two cuspidal theta series attached to ray class characters of K. We did not attempt to adapt the computations of [Gro87, §7,8,9] to the present setting, but rather follow a different method invoking the Weil representation of $\mathrm{SL}_2(\mathbb{A}_f)$ (where $\mathbb{A}_f$ denotes the ring of finite adèles) on the space of Schwartz functions on the adélic points of the underlying quadratic spaces.

2.1. Setup on Heegner Points

The computation will be carried out in slightly greater generality than in Theorem 1.2 of the Introduction. Let K be an imaginary quadratic field of odd discriminant D with maximal order $\mathfrak{o}$, and let $\mathcal{C} = \mathrm{Pic}(\mathfrak{o})$ denote the class group. For I an ideal, note that the image I' by conjugation defines the same class in $\mathcal{C}$ as I^{-1}. Denote by a the number of distinct prime factors of D.

Let N be an odd prime with the property that $-N$ *is a square modulo* D. When D is *prime,* as assumed in the Introduction, this condition is equivalent to N being inert in K; in general it always implies that N remains inert but is a stricter condition.

Fix an algebraic closure $\overline{\mathbb{F}_N}$, and let $\mathbb{F}_{N^2}$ be the subfield of size N^2.

Choose an auxiliary odd prime q such that $q \equiv -N (\mathrm{mod} D)$. An elementary computation of quadratic symbols shows that q is split in K. Assume throughout that q is such that the ideals $\mathfrak{q}$, $\overline{\mathfrak{q}}$ in K above q are *principal.* The existence of such q is guaranteed by Cebotarev density theorem.

A calculation with Hilbert symbols (cf. [Vig80, §2.1]) shows that

$$B \simeq K + Kj \quad \text{with } j^2 = -qN \quad \text{and} \quad zj = jz' \quad \text{for all } z \in K \tag{12}$$

is the definite quaternion algebra over $\mathbb{Q}$ of discriminant N. Let $b \mapsto b'$ denote the canonical anti-involution on B; it coincides with complex conjugation when restricted to K. Let $n(b) = bb'$ denote the reduced norm on B.

An *orientation* on a maximal order $\mathcal{M}$ in B is a choice of homomorphism

$$\mathbf{o} : \mathcal{M} \to \mathbb{F}_{N^2}$$

---

the derived category of R/p^t modules. In particular, each element of $H^1(\Omega^1)$ induces (by passage to H^0) a map $R/p^t \to R/p^t$, that is, an element of R/p^t.

onto $\mathbb{F}_{N^2}$. Note that $\mathcal{M}$ admits exactly two possible orientations. Two oriented maximal orders $\vec{\mathcal{M}}_1 = (\mathcal{M}_1, \mathbf{o}_1)$, $\vec{\mathcal{M}}_2 = (\mathcal{M}_2, \mathbf{o}_2)$ are equivalent if there exists an isomorphism $i : \mathcal{M}_1 \to \mathcal{M}_2$ satisfying $\mathbf{o}_1 = \mathbf{o}_2 \circ i$.

Write $\mathrm{Pic}(B)$ for the set of equivalence classes of oriented maximal orders. By a classical result of Deuring (cf. [Voi, §42.3]), $\mathrm{Pic}(B)$ is in bijection with the set $\mathcal{E}$ of isomorphism classes of supersingular elliptic curves over $\overline{\mathbb{F}}_N$ as follows: we associate to an elliptic curve E the order $\mathrm{End}(E)$, which acquires an orientation by considering its action on the tangent space.

Fix a basepoint $\vec{\mathcal{M}} \in \mathrm{Pic}(B)$ containing $\mathfrak{o} \oplus \mathfrak{o}j$. Define the map

$$\iota : \mathrm{Pic}(\mathfrak{o}) \longrightarrow \mathrm{Pic}(B) \tag{13}$$

that takes an ideal class I to the oriented maximal order $\iota(I) = I^{-1}\vec{\mathcal{M}}I$.

2.2. *Statement of the Trace Identity*

Define $\mathrm{Div}(\mathcal{E})$ to be the module of $\mathbb{Z}$-valued functions on $\mathrm{Pic}(B)$, equipped with its natural action of the Hecke algebra $\mathbb{T}$ as described for example in [Gro87, §4]. If $\vec{\mathcal{M}} \in \mathrm{Pic}(B)$, then let $\mathcal{M}$ denote the underlying unoriented order and set $w_{\vec{\mathcal{M}}} = \frac{1}{2}|\mathcal{M}^\times|$. Denote by $e_x \in \mathrm{Div}(\mathcal{E})$ the characteristic function of $x \in \mathrm{Pic}(B)$ and set as in the Introduction $\Sigma_0 = \sum_x \frac{e_x}{w_x} \in \mathrm{Div}(\mathcal{E}) \otimes \mathbb{Q}$. The space $\mathrm{Div}(\mathcal{E})$ is endowed with a natural symmetric bilinear form

$$\langle , \rangle : \mathrm{Div}(\mathcal{E}) \times \mathrm{Div}(\mathcal{E}) \to \mathbb{Z}, \qquad \langle e_x, e_y \rangle := w_x \delta_{xy}, \tag{14}$$

relative to which the Hecke operators T_ℓ are self-adjoint *for all* ℓ, including for $\ell = N$.

The Jacquet–Langlands correspondence identifies $\mathrm{Div}(\mathcal{E})$ and $M_2(\Gamma_0(N))$ as Hecke modules. This identification can be described explicitly by means of the Θ-correspondence, which is the Hecke-equivariant map

$$\Theta : \mathrm{Div}(\mathcal{E}) \otimes_{\mathbb{T}} \mathrm{Div}(\mathcal{E}) \to M_2(\Gamma_0(N)) \tag{15}$$

given by (cf. e.g. [Eme02] and [Gro87, Prop. 5.6])

$$\Theta(\phi_1 \otimes \phi_2) = \frac{1}{2}\langle \phi_1, \Sigma_0 \rangle \langle \phi_2, \Sigma_0 \rangle + \sum_{m \geq 1} \langle \phi_1, T_m \phi_2 \rangle q^m. \tag{16}$$

REMARK 2.1. Formula (16) makes it clear that

$$\Theta(\phi_1 \otimes \phi_2) = \Theta(\phi_2 \otimes \phi_1),$$

because each T_m is self-adjoint, including for $m = N$.

Given a character $\psi : \mathrm{Pic}(\mathfrak{o}) \to L^\times$ with values in some finite field extension $L/\mathbb{Q}$, define

$$[\psi] := \iota_*(\psi) = \sum_{I \in \mathrm{Pic}(\mathfrak{o})} \psi(I)\iota(I) \in \mathrm{Div}(\mathcal{E}) \otimes L. \tag{17}$$

The main result of this section is the following. Let θ_ψ denote the theta series associated to ψ as recalled in (22). Note also that $\theta_\psi = \theta_{\psi^{-1}}$, because the characters of $\mathrm{Pic}(\mathfrak{o})$ are anticyclotomic in the sense that $\psi' = \psi^{-1}$; this accounts for the discrepancy in phrasing between the following statement and the analogous Theorem 3.1 in the RM scenario.

THEOREM 2.2. *Let ψ_1 and ψ_2 be characters of $\mathcal{C}$, and let θ_{ψ_i} be the newforms associated to ψ_i (equivalently: to ψ_i^{-1}). Put $\psi_{12} = \psi_1\psi_2$, $\psi_{12'} = \psi_1\psi_2'$. Then there exists p_0 such that, for any N and any $p \geq p_0$ with $p \mid N-1$,*

$$\mathsf{Tr}_N^{ND}(\theta_{\psi_1}(Nz)\theta_{\psi_2}(z)) =_{\mathfrak{S}} 4 \cdot \Theta([\psi_{12}] \otimes [\psi_{12'}]), \tag{18}$$

where, as in (5), the notation "$f =_{\mathfrak{S}} g$" means that both modular forms have the same pairing with the Shimura class of level N. If D is prime, (18) is a strict identity (not just up to $\mathfrak{S}$) for all primes p.

We expect a similar trace identity to hold for general ray class characters ψ_1, ψ_2 of K with opposite central character, which amounts to allowing the ring class characters ψ_{12}, $\psi_{12'}$ to have arbitrary conductor $c \geq 1$. In such generality, however, we do not expect the constant to be as simple as $C = 4$ and (18) should hold up to a suitable constant $C = C(\psi_1, \psi_2)$ that depends on ψ_1, ψ_2 but not on N. The reader is referred to R. Zhang's forthcoming Ph.D thesis [Zha] for the proof in greater generality in the adelic language.

Theorem 2.2 and Theorem 3.1 cover the simplest nontrivial settings in both definite and indefinite cases. The proofs are different because we chose to be as direct as possible in each case and avoid repetition, but the approaches in Sections 2 and 3 are in some ways complementary.

2.3. *Summary of the Proof*

Theorem 2.2 will be proved subject to three propositions given in what follows; these will be proved in the remaining subsections.

Define $\mathcal{O} \subset B$ via

$$\mathcal{O} = \mathcal{O}(q) := \mathfrak{o} \oplus \mathfrak{o}j. \tag{19}$$

An elementary computation using [Vig80, 1.4.7] shows that $\mathcal{O} = \mathcal{O}(q)$ has square-free discriminant DNq, and therefore (cf. [Vig80, 3.5.3]) $\mathcal{O}$ is an Eichler order, that is to say, the intersection of two maximal orders. Let us fix now and for the rest of this section a maximal order $\mathcal{M} \supset \mathcal{O}$ as well as an orientation on it. All other orders containing $\mathcal{O}$ can be obtained from $\mathcal{M}$ as

$$\mathcal{M}_d := \mathfrak{d}^{-1}\mathcal{M}\mathfrak{d}, \tag{20}$$

where d ranges over positive divisors $d \mid Dq$ and $\mathfrak{d}$ is an ideal in $\mathfrak{o}$ of norm d. This is because locally at every prime ℓ dividing Dq there are exactly two local maximal orders containing $\mathcal{O} \otimes \mathbb{Z}_\ell$: one is obtained from the other by conjugating by any element of norm ℓ normalizing $\mathcal{O} \otimes \mathbb{Z}_\ell$ (cf. e.g. [Vig80, §3.5]).

If I_1, I_2 are ideal classes for $\mathfrak{o}$, then we can form

$$I_1 \mathcal{O} I_2 = I_1 I_2 \oplus I_1 I_2' j \subset B.$$

By definition, the left-hand side means the additive subgroup of B generated by all threefold products $i_1 \cdot o \cdot i_2$.

We regard K and B as quadratic spaces by means of the norm and reduced norm respectively. For every ideal I in either $V = K$ or B, let

$$\theta_I = \theta(I) = \sum_{a \in I} q^{\frac{n(a)}{n(I)}} \tag{21}$$

denote the theta series associated to I; here $n(I)$ stands for the single positive generator of the ideal of $\mathbb{Q}$ spanned by the norms of all elements in I. The theta series θ_I is a modular form of weight $[V : \mathbb{Q}]/2$. With this normalization, θ_I only depends, in the case $V = K$, on the class of I up to principal ideals, since $\theta_I = \theta_{Ix}$ for any $x \in K^\times$. Moreover, for any character of $\mathcal{C}$,

$$\theta_\psi = \sum_{I \in \mathcal{C}} \psi(I)^{-1} \theta_I \tag{22}$$

is the new theta series associated to ψ, a classical modular newform of weight 1, level D, and nebentype character χ_K, the quadratic Dirichlet character associated to $K/\mathbb{Q}$. (As mentioned previously, in the current situation one could omit the inverse on the right-hand side, but the formulas with this convention are valid under less restrictive hypotheses, and this facilitates comparison with the RM case.)

For any $d \geq 1$, recall that $\theta^{(d)}(q) := \theta(q^d)$. We will include forward references to propositions in the RM case that play a similar role, although because of the slightly different setups the statements are not entirely parallel.

PROPOSITION 2.3 (See Section 2.4, cf. also Prop. 3.10). *For any pair of classes I_1, I_2 of $\mathcal{C}$, we have*

$$\mathrm{Tr}_N^{DN} \theta(I_1 I_2) \theta^{(N)}(I_1 I_2') = \frac{1}{2} \sum_{d | Dq} \theta(I_1 \mathcal{M}_d I_2), \tag{23}$$

where, on the left, Tr *is the trace from level $\Gamma_0(DN)$ to level $\Gamma_0(N)$, and $\mathcal{M}_d$ is as in* (20).

PROPOSITION 2.4 (See Section 2.5, cf. also Prop. 3.4). *For any pair of ideal classes I, J, we have*

$$\theta(J' \mathcal{M} I) = 2 \cdot \Theta(e_I \otimes e_J). \tag{24}$$

Here e_I, e_J are as in Section 2.2, where we use ι of (13) *to identify I, J with elements of* $\mathrm{Pic}(B)$.

For every quadratic character χ of $\mathcal{C}$, set

$$G_{DN}(\chi) = \theta^{(N)}_{\psi_1^{-1}\chi} \cdot \theta_{\psi_2^{-1}\chi} \quad \text{and} \quad G_{DN} := \sum_{\chi \in (\mathcal{C}/\mathcal{C}^2)^*} G_{DN}(\chi). \tag{25}$$

In the case when D is prime, the only quadratic character is trivial, so $G_{DN}(\chi) = G_{DN}$, and the following proposition is vacuous.

PROPOSITION 2.5 (See Section 2.6.). *With the notation of* (5),

$$\mathsf{Tr}_N^{DN}(G_{DN}(\chi)) \sim_{\mathfrak{S}} \mathsf{Tr}_N^{DN}(G_{DN}(\chi')),$$

for all quadratic characters χ, χ' of $\mathcal{C}$, so long as the prime p is sufficiently large relative to D.

Let us see how these three results imply the theorem. For every choice of a quadratic character χ, we have

$$G_{DN}(\chi) = \sum_{I,J\in\mathcal{C}} \chi(IJ)\psi_1(I)\psi_2(J)\theta_I^{(N)}\theta_J. \tag{26}$$

But $\sum_\chi \chi(IJ)$ is zero unless IJ is a square inside $\mathcal{C}$; in that case, it equals $\#\mathcal{C}[2]$. Moreover, any pair (I, J) with $IJ \in \mathcal{C}^2$ is of the form $(I_1 I_2', I_1 I_2)$ for precisely $\#\mathcal{C}[2]$ pairs (I_1, I_2) and then $\psi_1(I)\psi_2(J) = \psi_{12}(I_1)\psi_{12'}(I_2')$. It follows that

$$G_{DN} = \sum_{I_1,I_2\in\mathcal{C}} \psi_{12}(I_1)\psi_{12'}(I_2')\theta(I_1 I_2)\theta^{(N)}(I_1 I_2'). \tag{27}$$

Using Proposition 2.3 we get

$$\mathsf{Tr}_N^{DN}(G_{DN}) = \frac{1}{2}\sum_{I_1,I_2\in\mathcal{C}} \psi_{12}(I_1)\psi_{12'}(I_2')\Big(\sum_{d|Dq} \theta(\mathfrak{d}^{-1} I_1 \mathcal{M} I_2 \mathfrak{d})\Big). \tag{28}$$

Note, however, that all terms for every fixed d in (28) are equal: this follows after reindexing $(I_1, I_2) \leftrightarrow (\mathfrak{d}^{-1} I_1, I_2\mathfrak{d})$ and recalling that the class of the ideal $\mathfrak{d}$ has order 2 in $\mathcal{C}$ when $d \mid D$, whereas the class of $\mathfrak{q}$ is trivial. The number of such terms is equal to 2^{a+1} with a the number of prime factors of D. Hence

$$\begin{aligned}\mathsf{Tr}_N^{DN}(G_{DN}) &= 2^a \sum_{I_j} \psi_{12}(I_1)\psi_{12'}(I_2')\theta(I_1 \mathcal{M} I_2) \\ &= 2^a \sum_{I_j} \psi_{12}(I_1')\psi_{12'}(I_2')\theta(I_1' \mathcal{M} I_2).\end{aligned} \tag{29}$$

Proposition 2.4, as well as the symmetry of Θ in its arguments, can be invoked to transform the right-hand side to get

$$\begin{aligned}\mathsf{Tr}_N^{DN}(G_{DN}) &= 2^{a+1} \sum \psi_{12}^{-1}(I_1)\psi_{12'}^{-1}(I_2)\Theta(e_{I_2} \otimes e_{I_1}) \\ &= 2^{a+1}\Theta([\psi_{12}^{-1}] \otimes [\psi_{12'}^{-1}]).\end{aligned}$$

This directly yields Theorem 2.2 when D is prime, as in that case the order of $\mathcal{C}$ is odd and hence $G_{DN} = G$. When D is composite, Proposition 2.5 shows that we can replace G_{DN} on the left with $2^{a-1} G_{DN}(1)$ if we are only interested in pairing with the Shimura class, since $\mathcal{C}[2]$ has rank $a - 1$ by genus theory (cf. e.g.

[Coh03, §13]). Unwinding the notation

$$\mathrm{Tr}_N^{ND}(\theta_{\psi_1^{-1}}(Nz)\theta_{\psi_2^{-1}}(z)) \sim_{\mathfrak{S}} 4\cdot\Theta([\psi_{12}^{-1}]\otimes[\psi_{12'}^{-1}]).$$

This proves Theorem 2.2 after recalling that $\theta_{\psi_i} = \theta_{\psi_i^{-1}}$.

2.4. *Proof of Proposition 2.3*

We must show that

$$\mathrm{Tr}_N^{DN}\theta(I_1I_2)\theta^{(N)}(I_1I_2') = \frac{1}{2}\sum_{d|Dq}\theta(I_1\mathcal{M}_dI_2). \tag{30}$$

Let T_q denote the Hecke operator at q and $\mathrm{Tr}_{N_1}^{N_2}$ the trace map from modular forms of level N_2 to level N_1 for any $N_1 \mid N_2$. Then

$$\mathrm{Tr}_{DN}^{DNq}\theta_J^{(Nq)} = T_q\cdot\theta_J^{(N)} = \theta_{J\mathfrak{q}}^{(N)} + \theta_{J\mathfrak{q}'}^{(N)} = 2\theta_J^{(N)},$$

where the second equality follows from, for example, [Kan12, §2] and the third since we are supposing that $\mathfrak{q}$ is principal. Hence

$$\mathrm{Tr}_N^{DNq}\theta_{J_1}\theta_{J_2}^{(Nq)} = \mathrm{Tr}_N^{DN}\theta_{J_1}(\mathrm{Tr}_{DN}^{DNq}\theta_{J_2}^{(Nq)}) = 2\mathrm{Tr}_N^{DN}\theta_{J_1}\theta_{J_2}^{(N)}.$$

Taking $J_1 = I_1I_2$, $J_2 = I_1I_2'$ and switching sides, we get

$$\mathrm{Tr}_N^{DN}\theta_{I_1I_2}\theta_{I_1I_2'}^{(N)} = \frac{1}{2}\mathrm{Tr}_N^{DNq}\theta_{I_1\mathcal{O}I_2}, \tag{31}$$

where we noted that $\theta_{I_1\mathcal{O}I_2} = \theta_{I_1I_2\oplus I_1I_2'j} = \theta_{I_1I_2}\theta_{I_1I_2'}^{(Nq)}$ since $j^2 = -qN$. So Proposition 2.3 reduces to the following.

PROPOSITION 2.6. *For any pair of classes I_1, I_2 of* $\mathrm{Pic}(\mathfrak{o})$,

$$\mathrm{Tr}_N^{DNq}(\theta_{I_1\mathcal{O}I_2}) = \sum_{d|Dq}\theta(I_1\mathcal{M}_dI_2). \tag{32}$$

In order to prove Proposition 2.6, note that—with $V = B$ or K as before—the rule that associates to every lattice L a modular form θ_L of weight $\dim(V)/2$ may be extended to the space of Schwartz functions on $V\otimes\mathbb{A}_f$ where $\mathbb{A}_f$ denotes the ring of finite adèles of $\mathbb{Q}$ (cf. e.g. [GH11] for background). Namely, such a function may be identified with a function Φ supported on some lattice $L\subset V$ and constant on the cosets of a sublattice of L. We can form the θ-function

$$\theta_\Phi := \sum_{z\in V}\Phi(z)q^{Q(z)} \tag{33}$$

with Q the norm form (or, as we will actually use, a rescaling of it). This is compatible with the previous definition in the sense that $\theta_{[L]} = \theta_L$, where $[L]$ is the characteristic function of the closure of a lattice L inside $V\otimes\mathbb{A}_f$.

The function $\Phi\mapsto\theta_\Phi$ is equivariant for the action of $\mathrm{SL}_2(\mathbb{A}_f)$ on Schwartz functions arising from the Weil representation on one side, and the natural action on the space of modular forms on the other; this is a straightforward consequence of the adelic interpretation of θ-series; we will give a more detailed sketch of

a similar equivariance in the more complicated RM setting in Section 3.5. This equivariance implies that the trace, from level DNq to N, of $\theta_{I_1\mathcal{O}I_2}$ can be computed by first computing the corresponding trace

$$\mathsf{Tr}_N^{DNq} \text{ of the Schwartz function } [I_1\mathcal{O}I_2]. \tag{34}$$

Proposition 2.6 thus follows after computing the trace of $[I_1\mathcal{O}I_2]$ with reference to the $\mathrm{SL}_2(\mathbb{A}_f)$-action on Schwartz functions, taking into account that we have an equality of rescaling factors $n(I_1\mathcal{M}_d I_2) = n(I_1\mathcal{O}I_2)$ (this can be readily deduced from the fact that I_1, I_2 are locally principal).

This Weil representation is a tensor product of representations of $\mathrm{SL}_2(\mathbb{Q}_\ell)$ on Schwartz functions on $V \otimes \mathbb{Q}_\ell$. We review the formulas in Section 3.5 and will summarize them here. Given a prime ℓ, let $\mu : \mathbb{Q}_\ell \to \mathbb{C}^\times$ be the restriction of the standard character of $\mathbb{A}/\mathbb{Q}$ which is given by $x \mapsto e^{2\pi i x}$ on $\mathbb{R}$ and is trivial on each $\mathbb{Z}_p$. In particular μ is trivial on $\mathbb{Z}_\ell$ but not on $\ell^{-1}\mathbb{Z}_\ell$. For any $t \in \mathbb{Q}_\ell$, denote $m(t) = \left(\begin{smallmatrix} 1 & t \\ 0 & 1 \end{smallmatrix}\right)$ and set $w = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$. Given a Schwartz function Φ_ℓ on $V \otimes \mathbb{Q}_\ell$:

$$\begin{aligned} m(t) \cdot \Phi_\ell(x) &= \mu(t\langle x, x\rangle)\Phi_\ell(x) \quad \text{for any } t \in \mathbb{Q}_\ell, \\ w \cdot \Phi_\ell(y) &= \gamma_\ell \int_{V\otimes\mathbb{Q}_\ell} \Phi_\ell(x)\mu(\langle y, x\rangle)\, dx, \end{aligned} \tag{35}$$

where, in particular, $\gamma_\ell = 1$ for ℓ not dividing N. Here dx is taken to be the self-dual Haar measure.

The desired trace from (34) can be calculated piecewise at every prime $\ell \mid Dq$ and then packaging together the local outputs.

Lemma 2.7. *Let ℓ be a prime divisor of Dq. Let $(W, \langle,\rangle)$ be the quadratic space over $\mathbb{Q}_\ell$ given by $K \otimes \mathbb{Q}_\ell$ equipped with the norm form divided by $N(I_1 I_2)$, and let $L \subset W$ be a maximal integral lattice. Let $(W', L', \langle,\rangle')$ be obtained from $(W, L, \langle,\rangle)$ by multiplying the form $\langle,\rangle$ by $-qN$.*

Then—for the Weil representation action of $\mathrm{SL}_2(\mathbb{Q}_\ell)$ on Schwartz functions on $W \oplus W'$—the characteristic function $1_{L\oplus L'}$ of $L \oplus L'$ is invariant by $\Gamma_0(\ell) \subset \mathrm{SL}_2(\mathbb{Z}_\ell)$, and

$$\mathsf{Tr}_{\Gamma_0(\ell)}^{\mathrm{SL}_2(\mathbb{Z}_\ell)} 1_{L\oplus L'} = 1_{\mathcal{M}_+} + 1_{\mathcal{M}_-}, \tag{36}$$

where $\mathcal{M}_\pm$ are the two self-dual integral lattices containing $(L \oplus L')$.

Before we prove Lemma 2.7, we explain why it implies Proposition 2.6. There is no loss of generality in choosing I_1, I_2 relatively prime to Dq. It follows from (12) that $W \oplus W'$ is isometric to $B \otimes \mathbb{Q}_\ell$ with its reduced norm form, and this identification carries $L \oplus L'$ to the closure of $I_1\mathcal{O}I_2$. Thus, combining together (37) at all primes $\ell \mid Dq$, Proposition 2.6 follows after noticing that if we take the self-dual lattice $\mathcal{M}_+$ to be the localization at ℓ of the global maximal order $\mathcal{M}_d$ for some d with $\ell \nmid d$, then $\mathcal{M}_- = \mathcal{M}_{d\ell} \otimes \mathbb{Z}_\ell$.

Proof of Lemma 2.7. Write $\mathbf{e}$ for the characteristic function of $L \oplus L'$ and $\mathbf{e}^*$ for the characteristic function of the dual lattice $(L \oplus L')^*$. Note that we have inclusions

$$(L \oplus L') \subset \mathcal{M}_+, \mathcal{M}_- \subset (L \oplus L')^*,$$

with both inclusions of index ℓ, and indeed the quotient $\frac{(L\oplus L')^*}{L\oplus L'}$ is isomorphic to $(\mathbb{Z}/\ell\mathbb{Z})^2$ where the induced $\mathbb{Q}_\ell/\mathbb{Z}_\ell$-valued quadratic form takes the form $(x_1, x_2) \mapsto \ell^{-1}(x_1^2 - x_2^2)$; in these coordinates $\mathcal{M}_\pm$ corresponds to $x_1 = \pm x_2$. Invariance of $\mathbf{e}$ by $\Gamma_0(\ell)$ follows readily from the definitions. Now a set of coset representatives for $\Gamma_0(\ell)$ in $\mathrm{SL}_2(\mathbb{Z}_\ell)$ is

$$\{w\} \cup \{wm(t)w : t \in \mathbb{Z}/\ell\mathbb{Z}\}.$$

Note that $w\mathbf{e} = \ell^{-1}\mathbf{e}^*$:

- for $y \notin (L \oplus L')^*$, $w\mathbf{e}(y)$ is the integral on $L \oplus L'$ of the character $\mu(\langle y, x\rangle)$, which vanishes since that character is not trivial;
- for $y \in (L \oplus L')^*$, we have $w\mathbf{e}(y) = \mathrm{vol}(L)\mathrm{vol}(L') = \ell^{-1}$ (the self-dual Haar measure on $W \oplus W'$ assigns mass ℓ^{-1} to $L \oplus L'$).

It thus follows that

$$\left(\sum_{t\in\mathbb{Z}/\ell\mathbb{Z}} m(t)\right) w\mathbf{e} = 1_S,$$

where $S = \{x \in (L \oplus L')^* : \langle x, x\rangle \in \mathbb{Z}_\ell\}$. But S is just the union of $\mathcal{M}_+$ and $\mathcal{M}_-$, and also $\mathcal{M}_+ \cap \mathcal{M}_- = L \oplus L'$. Thus $1_S = 1_{\mathcal{M}_+} + 1_{\mathcal{M}_-} - \mathbf{e}$, and we deduce that

$$\mathsf{Tr}\mathbf{e} = w\mathbf{e} + w1_{\mathcal{M}_+} + w1_{\mathcal{M}_-} - w\mathbf{e} = 1_{\mathcal{M}_+} + 1_{\mathcal{M}_-}. \tag{37}$$

□

2.5. *Proof of Proposition 2.4*

Let E_I denote the supersingular elliptic curve associated to $\iota(I)$ and e_I for the corresponding element in $\mathrm{Div}(\mathcal{E})$. Set $w_I = w_{\iota(I)}$.

In order to prove (24), it suffices to show that both sides have the same Fourier coefficients for all $m \geq 1$. The mth Fourier coefficient of the r.h.s. of (24) is

$$2a_m(\Theta(e_I \otimes e_J)) = 2\langle T_m e_I, e_J\rangle = 2w_J B_{I,J}(m). \tag{38}$$

Here $B(m)$ is the mth Brandt matrix and $B_{I,J}(m)$ is the entry in $B(m)$ associated to E_I and E_J (cf. [Gro87, §1, §2]). The equalities in (38) follow from the definition of Θ in (16) and [Gro87, 4.4, 4.5, 4.6]. Since $2w_J = |\mathrm{Aut}(E_J)|$, it follows from [Gro87, Prop. 2.3] that $2w_J B_{I,J}(m)$ is also equal to the number of isogenies of degree m from the supersingular elliptic curve E_I to E_J; see also the proof of [Gro87, Prop. 2.7 (6)] on p. 128 of loc. cit. The $\mathbb{Z}$-module of such isogenies is identified with $J^{-1}\mathcal{M}I$, where the degree is identified with $z \mapsto n(z)n(J)/n(I)$ (cf. [Gro87, 2.1] combined with the definition of M_{ij} on p. 118 of loc. cit.). Consequently,

$$2a_m(\Theta(e_I \otimes e_J)) = |\{z \in J^{-1}\mathcal{M}I : n(z)n(J)/n(I) = m\}|.$$

This in turn is the mth Fourier coefficient of the l.h.s. of (24), as $J^{-1}\mathcal{M}I$ is homothetic to $J'\mathcal{M}I$.

2.6. *Proof of Proposition 2.5*

Recall that this proposition is used only for the case of D composite, and thus is not strictly necessary, for example, for the statement of Theorem 1.2.

Each quadratic character χ cuts out an extension H_χ/K which is the composition of K and a quadratic extension $\mathbb{Q}_\chi/\mathbb{Q}$ of discriminant dividing D. Hence χ may be regarded as the restriction to G_K of the Dirichlet character of conductor dividing D attached to $\mathbb{Q}_\chi/\mathbb{Q}$ that we still denote by the same symbol. As it is readily seen by comparing the associated Galois representations, $\theta_{\psi_1^{-1}\chi}$ is the twist of $g = \theta_{\psi_1^{-1}}$ by χ, and $\theta_{\psi_2^{-1}\chi}$ is the twist of $h = \theta_{\psi_2^{-1}}$ by χ.

Let π_1, π_2 be the automorphic representations for GL_2 associated to g, h. Let $K_0(D) \subset \mathrm{GL}_2(\mathbb{A}_f)$ be the standard compact open subgroup, and let $K_1(D)$ be the kernel of the natural "diagonal" maps $K_0(D) \to ((\mathbb{Z}/D\mathbb{Z})^\times)^2$. Note that $K_1(D)$ in the GL_2 context is sometimes defined to only impose *one* constraint, but here we understand that both the diagonal entries are congruent to 1 modulo D.

Set

$$X_1(D) = \mathrm{GL}_2(\mathbb{Q})\backslash\mathcal{H}^* \times \mathrm{GL}_2(\mathbb{A}_f)/K_1(D),$$

whose set of connected components identified with

$$\mathbb{Q}^\times\backslash\mathbb{A}_f^\times/\det(K_1(D)) = (\mathbb{Z}/D\mathbb{Z})^\times.$$

There are embeddings

$$\pi_{1,f}^{K_1(D)} \text{ and } \pi_{2,f}^{K_1(D)} \hookrightarrow H^0(X_1(D), \omega_{X_1(D)})$$

carrying the new vectors to g and h respectively.

The new vectors are characterized, uniquely up to scalar, by the fact that they transform under

$$k = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \subset K_0(D)$$

by the character $k \mapsto \chi_K(a)$. For each χ as before, we can consider the "pseudo-new" vector

$$g^\chi \text{ or } h^\chi \in \pi_{1,f}^{K_1(D)} \quad \text{or} \quad \pi_{2,f}^{K_1(D)}$$

uniquely characterized up to scalar by similarly transforming by the character $k \mapsto \chi_K(a)\chi(ad)$. (The uniqueness of such a vector follows by applying the usual new vector theory to the representation $\pi_{1,f} \otimes \chi$, which has the same conductor as $\pi_{1,f}$. Explicitly, we may construct a pseudo-new vector from a new vector by multiplying the associated function in the Kirillov model by the character χ; this statement is the representation-theoretic manifestation of the fact that twisting by χ multiplies coefficients of the q-expansion by χ. A nice short reference for basic properties of the Kirillov model and new vectors is the paper [Sch02], and a more encyclopaedic treatment is [JL70], in particular Theorem 2.13.)

With this construction, we have the following properties:

(a) The standard newforms g_χ and h_χ in the twisted automorphic representation correspond to the cup products:

$$g_\chi = g^\chi \cdot \chi, h_\chi = h^\chi \cdot \chi,$$

where we pull back χ to a complex-valued function on $X_1(D)$ by means of the map $X_1(D) \to (\mathbb{Z}/D\mathbb{Z})^\times$ to the group of connected components.

(b) $\langle g^\chi, h^\chi \rangle = \langle g, h \rangle$ with reference to any nontrivial $\mathrm{GL}_2(\mathbb{A}_f)$-invariant pairing $\pi_{1,f} \times \pi_{2,f} \to \mathbb{C}$.

Let $X_{10}(D, N)$ be obtained from $X_1(D)$ by imposing a further $K_0(N)$-level structure. Let $\mathfrak{S}_{DN} \in H^1(X_{10}(D, N), \omega) \otimes \mathbb{Z}/p^t\mathbb{Z}$ denote the pull-back of the Shimura class. Let $\pi_1, \pi_2 : X_{10}(D, N) \longrightarrow X_1(D)$ denote the two forgetful maps intertwined by the Atkin–Lehner involution at N. It follows that

$$\langle \mathrm{Tr}_N^{DN} G_{DN}(\chi), \mathfrak{S} \rangle = \langle G_{DN}(\chi), \mathfrak{S}_{DN} \rangle = \int \pi_1^*(g_\chi) \cup \pi_2^*(h_\chi) \cup \mathfrak{S}_{DN}$$

$$= \int \pi_1^*(g^\chi) \cup \pi_2^*(h^\chi) \cup \mathfrak{S}_{DN},$$

where $\int : H^1(X_1(D)_{\mathbb{Z}/p^t\mathbb{Z}}, \omega) \to \mathbb{Z}/p^t\mathbb{Z}$ is the trace map. It remains to verify that

$$\int \pi_1^*(g^\chi) \cup \pi_2^*(h^\chi) \cup \mathfrak{S}_{DN} = \int \pi_1^*(g) \cup \pi_2^*(h) \cup \mathfrak{S}_{DN}. \tag{39}$$

Now (b) implies that $g^\chi \otimes h^\chi$ and $g \otimes h$ have the same image in the diagonal coinvariants on $\pi_{1,f} \otimes \pi_{2,f}$. That is to say, considered inside $\pi_{1,f} \otimes \pi_{2,f}$,

$$g^\chi \otimes h^\chi - g \otimes h = \sum_{i \in I} c_i [s_i v_1 \otimes s_i v_2 - (v_1 \otimes v_2)], \tag{40}$$

where $c_i \in \mathbb{C}$ and $s_i \in \prod_{v|D} \mathrm{GL}_2(\mathbb{Q}_v)$. Moreover, a straightforward argument with rational structures shows that we may even take c_i to belong to the field $L = \mathbb{Q}(\psi_1, \psi_2)$, and similarly v_1 and v_2 to be L-rational modular forms; and for sufficiently large p, we can suppose c_i, v_1, v_2, and $D(D-1)$ to be p-integral. Then

$$\int (s_i v_1) \cup (s_i v_2) \cup \mathfrak{S} = \int v_1 \cup v_2 \cup \mathfrak{S},$$

where $\mathfrak{S}$ is a Shimura class at a sufficiently deep level $N \cdot D^r$; this follows from the invariance of the Shimura class under the adèle group away from N after pullback to a further cover. Therefore (40) implies the desired (39).

3. A Trace Identity for Indefinite Theta Series

The goal of this section is to prove the counterpart of Theorem 2.2 in the case where $(g, h) = (\theta_{\psi_1^{-1}}, \theta_{\psi_2^{-1}})$ is a pair of new weight one θ-series associated to ray class characters ψ_1 and ψ_2 of a common *real quadratic* field K, whose central characters, denoted by χ_1 and χ_2 respectively, satisfy $\chi_1 = \chi_2^{-1}$. Let D denote

the discriminant of K, and let $\delta = (\sqrt{D})$ be its different. We will assume that the discriminant D is odd.

Since g and h are holomorphic, the characters ψ_1 and ψ_2, whose induced representations are odd two-dimensional Artin representations, are necessarily of mixed signature at ∞. This means that the hypotheses of Section 2, in which ψ_1 and ψ_2 were assumed to be unramified, are restrictive to the point of being vacuous: indeed, the presence of the unit -1 precludes the existence of unramified idèle class characters of K of mixed signature. It will therefore only be assumed that the conductors of ψ_1 and ψ_2 divide the different $\delta := (\sqrt{D})$ of K, which means that the levels of

$$g = \theta_{\psi_1^{-1}}, \qquad h = \theta_{\psi_2^{-1}}$$

divide D^2. In particular, these forms belong to the spaces $M_1(\Gamma_1(D^2), \chi^{-1})$ and $M_1(\Gamma_1(D^2), \chi)$ respectively.

Because the θ-series for ψ_2 and its Galois conjugate ψ_2' coincide, it is harmless to suppose that ψ_1 and ψ_2 both have the same signature at ∞, namely the one for which ψ_1 and ψ_2 are trivial relative to the standard real embedding of K.

Because the restrictions of ψ_1 and ψ_2 (viewed as characters of the idèles $\mathbb{A}_K^\times$ of K) to the group $\mathbb{A}_\mathbb{Q}^\times$ of idèles of $\mathbb{Q}$ are inverses of each other, it follows that, for all primes v of K dividing D where ψ_1 and ψ_2 are possibly ramified,

$$\psi_{1,v}|_{\mathcal{O}_v^\times} = \psi_{2,v}^{-1}|_{\mathcal{O}_v^\times}.$$

But the Galois conjugation map $x \mapsto x'$ induces the identity on the residue fields of K_v for such v, and hence the characters

$$\psi_{12} := \psi_1\psi_2, \qquad \psi_{12'} := \psi_1\psi_2' \tag{41}$$

appearing in Theorem 2.2 are trivial on $\mathcal{O}_v^\times$ for all primes v, including those dividing D. It follows that ψ_{12} and $\psi_{12'}$ are everywhere unramified. The character ψ_{12} is furthermore totally even, and $\psi_{12'}$ is totally odd.

The existence of the odd unramified character $\psi_{12'}$ implies that the narrow class number of K is twice its class number, and hence that all the units of K have positive norm. The fundamental unit ε is chosen so that $\varepsilon > 1$ relative to the fixed standard real embedding $K \hookrightarrow \mathbb{R}$ of K evoked in the Introduction.

In fact, it will be shown in what follows that any pair of unramified characters of K with trivial restrictions to $\mathbb{A}_\mathbb{Q}^\times$ and opposite pure signatures can be obtained from a pair (ψ_1, ψ_2) as previously, in an essentially unique way; this fact plays a crucial role in the proof of Theorem 3.1, because it eliminates the need for an analogue of Proposition 2.5 and thus leads to a more precise result.

3.1. Setup on Heegner Cycles

As before, K is a real quadratic field of odd discriminant D, all of whose units have norm 1. Let $\mathfrak{o}$ be the maximal order of K. Let $N \nmid D$ be an odd prime that splits in K.

Choose $\delta_N \in \mathbb{Z}$ satisfying

$$\delta_N^2 \equiv D \pmod{N}.$$

This choice determines an ideal $\mathfrak{N} = (N, \delta_N - \sqrt{D})$ of $\mathfrak{o}$ of norm N. Also, let

$$M_0(N) := \left\{ \begin{pmatrix} a & b \\ Nc & d \end{pmatrix} \text{ with } a, b, c, d \in \mathbb{Z} \right\} \subset M_2(\mathbb{Z})$$

be the standard Eichler order of level N in the matrix ring $M_2(\mathbb{Z})$. This Eichler order is equipped with the standard orientation

$$\mathbf{o} : M_0(N) \to \mathbb{F}_N = (\mathbb{Z}/N\mathbb{Z})$$

onto the field of N elements, sending a matrix to the mod N residue class of its upper left-hand entry.

Let $I \subset \mathfrak{o}$ be an ideal. Writing $I \cap \mathbb{Z} = (a)$ with $a > 0$, we can write

$$I = \left(a, \frac{-b + \sqrt{D}}{2} \right)$$

with b uniquely determined modulo a. The action of $\mathfrak{o}$ on I with respect to the basis $(a, (-b + \sqrt{D})/2)$ gives a homomorphism

$$\alpha : \mathfrak{o} \to M_2(\mathbb{Z}), \qquad \sqrt{D} \mapsto \begin{bmatrix} b & -2c \\ 2a & -b \end{bmatrix}, \tag{42}$$

where c is defined by stipulating that the binary quadratic form $ax^2 + bxy + cy^2$ has discriminant D.

An eigenvector $v \in K^2$ for the action of $\alpha(K)$ is given by

$$v = \begin{pmatrix} (b + \sqrt{D})/2 \\ a \end{pmatrix}.$$

Write $\tau := \frac{b+\sqrt{D}}{2a}$, and let v' and τ' denote the algebraic conjugates of v and τ respectively over K.

Suppose that I is divisible by $\mathfrak{N}$ but not by $\mathfrak{N}'$. Then a is divisible by N, b is congruent to δ_N modulo N, and α is an embedding of $\mathfrak{o}$ into $M_0(N)$. Indeed, the basis vector $a \in I$ belongs to $\mathfrak{N}'I$ since it is divisible by N, and its image in I/NI generates the index N subgroup $\mathfrak{N}'I/NI$, which is preserved under multiplication by $\mathfrak{o}$. Hence multiplication by any element of $\mathfrak{o}$ is represented by a matrix in $M_0(N)$ relative to the basis $(a, (b + \sqrt{D})/2)$. Moreover the composition $\mathbf{o} \circ \alpha : \mathfrak{o} \to \mathbb{F}_N$ of α with the orientation $\mathbf{o} : M_0(N) \to \mathbb{F}_N$ is reduction modulo $\mathfrak{N}$.

Replacing the basis $(a, (b + \sqrt{D})/2)$ of I with another positively oriented[4] basis of the same form conjugates the resulting embedding by an element of $\Gamma_0(N)$, hence the embedding α attached to I is independent of this choice of basis up to conjugation in $\Gamma_0(N)$.

[4]Here, a basis $(e_1 e_2)$ is said to be positively oriented if it is in the $\mathrm{SL}_2(\mathbb{Z})$-orbit of the specified one, or, said more intrinsically, $e_1 \wedge e_2$ equals the norm of I multiplied by $1 \wedge \sqrt{D}/2$.

The standard real embedding $K \hookrightarrow \mathbb{R}$ that was fixed previously yields a geodesic $(\tau, \tau') \subset \mathcal{H}$ in the upper half-plane. Recall the fundamental unit $\varepsilon \in \mathfrak{o}_1^\times$ of K of norm one, and let

$$\gamma_I = \alpha(\varepsilon)^{\mathbb{Z}} \backslash (\tau, \tau') \tag{43}$$

denote the closed geodesics on $\Gamma_0(N)\backslash\mathcal{H}$ attached to I. We regard it as oriented *from* τ *to* τ'. This depends only on the class of I in

$$\mathcal{C} := \text{ the narrow ideal class group of } K, \tag{44}$$

and correspondingly we will freely write γ_I for $I \in \mathcal{C}$.

Note that $\tau' < \tau$ and moreover the derivative of the fractional linear transformation of $\mathbb{R}$ induced by $\alpha(\varepsilon)$ at τ' (resp. τ) is given by $(\varepsilon')^{-2}$ (resp. ε^{-2}). Since $\varepsilon > 1 > \varepsilon'$, we conclude that the action of $\alpha(\varepsilon)$ on (τ, τ') moves along the direction opposite to the orientation of the geodesic.

3.2. Statement of the Trace Identity

Given two narrow ideal classes, choose representatives I_1 and I_2 that are divisible by $\mathfrak{N}$ but not by $\mathfrak{N}'$. Let α_i for $i \in \{1, 2\}$ denote the two embeddings attached to I_1 and I_2 as in Section 3.1, and let $v_i, v_i' \in K^2$ and $\tau_i, \tau_i' \in K$ be the associated eigenvectors and fixed points, respectively.

Write $\langle \gamma_{I_1} \cdot T_m \gamma_{I_2} \rangle_N$ for the topological intersection pairing of the homology cycles γ_{I_1} and $T_m \gamma_{I_2}$ on the Riemann surface $X_0(N)(\mathbb{C})$. The generating series

$$\Theta(\gamma_{I_1} \otimes \gamma_{I_2}) := \sum_{m=1}^{\infty} \langle \gamma_{I_1} \cdot T_m \gamma_{I_2} \rangle_N q^m \tag{45}$$

is a cusp form of weight two and level N. This definition can be extended by linearity to arbitrary linear combinations of RM geodesics, notably the paths

$$\gamma_{\psi_{12}}(q) = \sum_{I \in \mathcal{C}} \psi_{12}(I) \gamma_I, \qquad \gamma_{\psi_{12'}}(q) = \sum_{I \in \mathcal{C}} \psi_{12'}(I) \gamma_I \tag{46}$$

associated to the unramified characters ψ_{12} and $\psi_{12'}$ respectively.

The following theorem, which is the main result of this section, relates the trace of products of binary theta series to modular generating series of real quadratic geodesic cycles as in (45).

THEOREM 3.1. *For all theta series* $g = \theta_{\psi_1^{-1}}$ *and* $h = \theta_{\psi_2^{-1}}$ *of* K *as before,*

$$\mathrm{Tr}_N^{ND^2}(\theta_{\psi_1^{-1}}(Nz)\theta_{\psi_2^{-1}}(z)) = C \cdot \psi_1(\mathfrak{N}') \cdot \Theta(\gamma_{\psi_{12}} \otimes \gamma_{\psi_{12'}}),$$

where

$$C = D \sum_{D = D_1 D_2} \mu(D_1) \cdot D_2 \cdot \psi_{12}\psi_{12'}(j_{D_1}) = D \prod_{p \mid D} (p - \psi_{12}\psi_{12'}(j_p)), \tag{47}$$

and j_{D_1} *is the order two element represented by the ideal* $(D_1, \sqrt{D})$ *in the narrow class group of* K.

The reader should compare this theorem to Theorem 2.2, which is less precise. It turns out that allowing the ray class characters ψ_i to be ramified at primes dividing the discriminant simplifies rather than complicates the situation. Transposing the proof of Theorem 3.1 to the setting of Section 2 would presumably lead to a refined and slightly more general variant of Theorem 2.2.

REMARK 3.2. In the extension of the generating series (45) to linear combinations of geodesics we are always taking representatives of $I \in \mathcal{C}$ that are divisible by $\mathfrak{N}$ but not by $\mathfrak{N}'$. This choice introduces an asymmetry that reappears throughout this section and explains the appearance of the factor $\psi_1(\mathfrak{N}')$ on the right-hand side of the identity in the theorem. Since the right-hand side is invariant under exchange of $\mathfrak{N}$ and $\mathfrak{N}'$, the second factor $\Theta(\gamma_{\psi_{12}} \otimes \gamma_{\psi_{12'}})$ must also depend on the choice of $\mathfrak{N}$.

The proof of Theorem 3.1 is summarized in Section 3.3, and the details of this sketch are fleshed out in the remainder of the section.

3.3. Summary of the Proof

Let

$$\mathcal{C} := \mathscr{I}(\mathfrak{o})/\mathrm{P}_+(\mathfrak{o}), \qquad \mathcal{C}_D := \mathscr{I}_\delta(\mathfrak{o})/\mathrm{P}_{\delta,+}(\mathfrak{o})$$

be the narrow class group and generalized class group of conductor δ, defined by letting

- $\mathscr{I}(\mathfrak{o})$, resp. $\mathscr{I}_\delta(\mathfrak{o})$, be the semi-group of ideals of $\mathfrak{o}$, resp. the ideals that are prime to δ;
- $\mathrm{P}_+(\mathfrak{o})$ be the semi-group of principal ideals with a totally positive generator;
- $\mathrm{P}_{\delta,+}(\mathfrak{o})$ be the semi-group of principal ideals with a totally positive generator that is congruent to 1 modulo δ.

Given ideals I_1 and I_2, let

$$\mathcal{A} := \{(x, y) \in (\mathfrak{N}' I_1)_+ \times (I_2)_- \text{ satisfying } x \equiv y \pmod{\delta}\}, \tag{48}$$

and the $+$ and $-$ subscripts mean, respectively, positive and negative norm. The group

$$\mathcal{U} := \{\pm(\varepsilon^a, \varepsilon^b) \text{ satisfying } a \equiv b \pmod 2\} \tag{49}$$

operates naturally on $\mathcal{A}$. Let

$$\begin{aligned}\Theta^\sharp(I_1, I_2) &:= \sum_{(x,y)\in\mathcal{A}/(\varepsilon^{2\mathbb{Z}}\times\varepsilon^{2\mathbb{Z}})} \mathrm{sign}(x)\cdot\mathrm{sign}(y)\cdot q^{\frac{xx'}{D\mathrm{N}(I_1)}-\frac{yy'}{D\mathrm{N}(I_2)}} \\ &= 4\sum_{(x,y)\in\mathcal{A}/\mathcal{U}} \mathrm{sign}(x)\cdot\mathrm{sign}(y)\cdot q^{\frac{xx'}{D\mathrm{N}(I_1)}-\frac{yy'}{D\mathrm{N}(I_2)}}.\end{aligned} \tag{50}$$

The function $\Theta^\sharp(I_1, I_2)(e^{2\pi i\tau})$ is a finite sum of suitable pairs of indefinite binary theta series attached to certain cosets in $I_1 \oplus I_2$, and is a modular form of

weight two. It is readily verified that it depends only on the classes of I_1 and I_2 in $\mathcal{C}_D$.

The proof of Theorem 3.1 follows from two key propositions. The first will be proved in Section 3.6 and the second in Section 3.7.

PROPOSITION 3.3 (See Section 3.6, also cf. (29)). *There is an equality of modular forms on* $\Gamma_0(N)$:

$$\begin{aligned}&\mathrm{Tr}_N^{ND^2}(\theta_{\psi_1^{-1}}(q^N)\cdot\theta_{\psi_2^{-1}}(q))\\&\quad=\psi_1(\mathfrak{N}')\cdot\frac{C}{4}\cdot\sum_{\mathcal{C}\times\mathcal{C}}\psi_{12}(I_1)\psi_{12'}(I_2)\cdot\Theta^\sharp(I_1I_2,I_1I_2'),\end{aligned}$$

where C *is as in* (47).

PROPOSITION 3.4 (See Section 3.7, also cf. Prop. 2.4). *The generating series of* (45) *is equal to*

$$\Theta(\gamma_{I_1}\otimes\gamma_{I_2})(q)=\frac{1}{4}\cdot\Theta^\sharp(I_1I_2,I_1I_2')(q).$$

Taken together, these two propositions imply that the trace appearing in Proposition 3.3 is equal to

$$\psi_1(\mathfrak{N}')\cdot C\cdot\sum_{\mathcal{C}\times\mathcal{C}}\psi_{12}(I_1)\psi_{12'}(I_2)\cdot\Theta(\gamma_{I_1}\otimes\gamma_{I_2}),$$

and the sum appearing here, by definition, equals $\Theta(\gamma_{\psi_{12}}\otimes\gamma_{\psi_{21}})$. That is precisely the statement of Theorem 3.1.

3.4. Setup on Class Groups

The running assumption that all units of K have norm one implies that equivalence of ideals in the narrow sense is strictly finer than equivalence in the wide sense, that is, that the narrow class number of K is twice its class number. It also implies, by genus theory, that the odd discriminant D is a product of two negative fundamental discriminants, and hence is not prime. Let $a\geq 2$ be the number of prime divisors of D.

Although K possesses no unramified idèle class characters of mixed signature, such characters *always appear* in conductor dividing the different δ of K, since the units of $\mathfrak{o}$ which are 1 modulo δ are all totally positive.

Let

$$\iota:=\text{ the class of }\varepsilon\text{ modulo }\delta.$$

It is one of the 2^a-2 possible *nontrivial* ($\neq\pm1$) square roots of 1 in $\mathfrak{o}/\delta=\mathbb{Z}/D\mathbb{Z}$. For if $\iota=\pm1$, the fundamental unit $\pm\varepsilon$ gives rise to a solution $(x,y)\in\mathbb{Z}^2$ of Pell's equation

$$x^2-Dy^2=1,\qquad x\equiv1\pmod D,\qquad x\text{ odd},\qquad y\text{ even}\quad\text{or}\qquad(51)$$

$$x^2-Dy^2=4,\qquad x\equiv2\pmod D,\qquad x,y\text{ odd}.\qquad(52)$$

In the second case, the factorization of $Dy^2 = (x-2)(x+2)$ into relatively prime integers implies that

$$x + 2 = \pm u^2 \quad \text{and} \quad x - 2 = \pm Dv^2$$

for some $(u, v) \in \mathbb{Z}^2$, and hence (u, v) is a solution of the equation $u^2 - Dv^2 = \pm 4$ of height strictly smaller than that of (x, y). Likewise, a solution to (51) leads to a pair (u, v) satisfying

$$x + 1 = \pm 2u^2 \quad \text{and} \quad x - 1 = \pm 2Dv^2,$$

and hence to a unit of $\mathfrak{o}$ of smaller height, contradicting in both cases the assumption that ε is a fundamental unit.

There is a natural exact sequence

$$0 \longrightarrow \langle \iota \rangle \longrightarrow (\mathbb{Z}/D\mathbb{Z})^\times \longrightarrow \mathcal{C}_D \longrightarrow \mathcal{C} \longrightarrow 0,$$

where the first inclusion sends $t \in (\mathbb{Z}/D\mathbb{Z})^\times$ to the principal ideal generated by any totally positive integer congruent to t modulo δ. Let

$$Z := \ker(\mathcal{C}_D \longrightarrow \mathcal{C}) \simeq (\mathbb{Z}/D\mathbb{Z})^\times/\iota$$

be the kernel of the natural projection. Next, let $W \subset (\mathbb{Z}/D\mathbb{Z})^\times$ be the index 2 subgroup which is the kernel of the quadratic Dirichlet character associated to K, and

$$\mathrm{N} : \mathcal{C}_D \to W \subset (\mathbb{Z}/D\mathbb{Z})^\times \tag{53}$$

be the norm map sending the class of an ideal to the mod D residue class of its norm. The triviality of the Herbrand quotient of the finite group $\mathcal{C}_D$ as a $\mathrm{Gal}(K/\mathbb{Q})$-module implies that

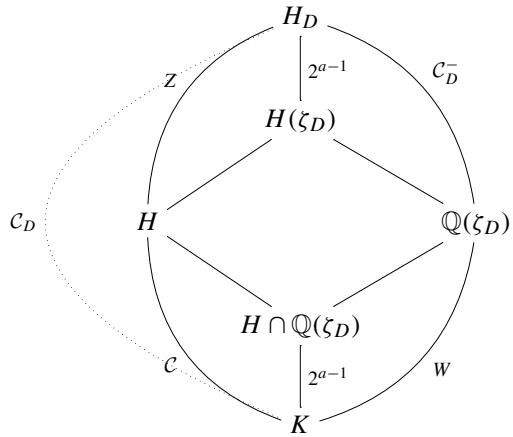
$$\mathcal{C}_D^- := \text{kernel of } \mathrm{N} = \{g/g' \text{ with } g \in \mathcal{C}_D\},$$

where $g \mapsto g'$ is induced by the Galois automorphism of K over $\mathbb{Q}$; thus W is now identified with $\mathcal{C}_D/\mathcal{C}_D^-$.

The groups Z and W have the same cardinality $\varphi(D)/2$, but the natural homomorphism $Z \longrightarrow W$ obtained by composing the inclusion $Z \hookrightarrow \mathcal{C}_D$ with the surjection $\mathcal{C}_D \to W$ is not an isomorphism; its kernel is the two-torsion subgroup of Z, of cardinality 2^{a-1}.

Global class field theory identifies $\mathcal{C}$ with the Galois group of the Hilbert class field H over K, and $\mathcal{C}_D$ with the Galois group of H_D over K, where H_D is the ray class field of K of conductor δ, an extension of H of degree $\varphi(D)/2$. The subgroup $\mathcal{C}_D^-$ is identified with the Galois group of H_D over the maximal subfield of H_D which is Galois and abelian over $\mathbb{Q}$, namely, the cyclotomic field $\mathbb{Q}(\zeta_D)$. The group W is identified with the Galois group of $\mathbb{Q}(\zeta_D)$ over K, an index two

subgroup of $(\mathbb{Z}/D\mathbb{Z})^\times$. The situation is summarized in the field diagram.



We can now state and prove the crucial lemma.

LEMMA 3.5. *There is an isomorphism*

$$\xi : \mathcal{C}^2 \longrightarrow (\mathcal{C}_D \times_W \mathcal{C}_D)/Z, \qquad (I_1, I_2) \mapsto (I_1 I_2, I_1 I_2'), \tag{54}$$

where the target is defined after choosing lifts I_1 and I_2 of the eponymous ideal classes $I_1, I_2 \in \mathcal{C}$ to the ray class group $\mathcal{C}_D$.

The validity of this lemma is the main reason that the current (RM) section obtains a more precise result than the CM section.

Proof. Observe, first, that the map is well defined, since the kernel of $\mathcal{C}_D \to \mathcal{C}$ is the image of $(\mathbb{Z}/D\mathbb{Z})^\times$, represented by principal ideals (t) for $t \in \mathbb{Z}$, and multiplying I_1 or I_2 by such a principal ideal of norm prime to D only changes $(I_1 I_2, I_1 I_2')$ by an element of the diagonally embedded Z. The two groups have the same cardinality by the previous discussion; so it is enough to prove that ξ is surjective. But clearly a pair (J_1, J_2) lies in the image if and only if $J_2 J_1^{-1}$ has the form I_2/I_2', that is, belongs to $\mathcal{C}_D^-$. □

3.5. Setup on Binary θ Series

For the lack of a reference, let us briefly sketch the general situation before specializing to the case of a quadratic space arising from the quadratic field K.

Consider a $2n$-dimensional anisotropic quadratic space (V, q) over $\mathbb{Q}$. The space of Schwartz functions on $V \otimes \mathbb{A}_f$ is endowed with an action of $\mathrm{SL}_2(\mathbb{A}_f)$ via the Weil representation which at any finite prime of $\mathbb{Q}$ is given by the following formulas:

$$r_\mu \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} f(x) = \mu(aq(x)) f(x),$$

$$r_\mu \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} f(x) = |a|\omega(a) f(ax), \tag{55}$$
$$r_\mu \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} f(x) = \gamma \widehat{f}(x).$$

Here μ is a chosen additive character, ω is the quadratic discriminant character corresponding to the space V, the function $\widehat{f}$ is Fourier transform of f relative to μ and a self-dual Haar measure on V, and γ is an eighth root of unity. We apply this only in the case when $V \otimes \mathbb{Q}_\ell$ is a *split* 4-dimensional quadratic space; in this case $\omega = 1$ and also $\gamma = 1$ (for the latter, see [Wei64, p. 176]).

Now suppose $\dim V = 2$, that (V, q) has signature $(1, 1)$, and suppose that Ψ_f is a Schwartz function on $V \otimes \mathbb{A}_f$ with stabilizer $\Gamma \leq \mathrm{SO}_q(\mathbb{Q})$.

PROPOSITION 3.6. *Let*

$$\theta_{\Psi_f}(z) := \sum_{\substack{v \in \Gamma\backslash V, \\ q(v)>0}} \mathrm{sign}(v) e^{2\pi i q(v) z} \Psi_f(v), \tag{56}$$

where $\mathrm{sign}(v)$ *is positive on one connected component of* $q(v) > 0$ *and negative on the other. Then* $\theta_{\Psi_f}(z)$ *is a modular form on* SL_2*, and the association* $\Psi_f \mapsto \theta_{\Psi_f}$ *is equivariant for the action of* $\mathrm{SL}_2(\mathbb{A}_f)$ *via the Weil representation. The same conclusion applies replacing the condition* $q(v) > 0$ *with* $q(v) < 0$ *and* $e^{2\pi i q(v) z}$ *with* $e^{-2\pi i q(v) z}$.

Sketch of Proof. To check this, we use the dual pair $\mathrm{SO}_q \times \mathrm{SL}_2$. Fix an isomorphism $(V \otimes \mathbb{R}, q) \simeq (\mathbb{R}^2, xy)$, let $\Psi_\infty(x, y) = (x + y) e^{-\pi(x^2+y^2)}$, and let $\Psi = \Psi_\infty \otimes \Psi_f$ be the associated Schwartz function on $V \otimes \mathbb{A}$. The function Ψ_∞ is chosen so that its average $\overline{\Psi}_\infty$ over the connected component of $\mathrm{SO}_q(\mathbb{R})$ is explicitly computable:

$$\begin{aligned} \overline{\Psi}_\infty(x, y) &= \int_{\lambda \in \mathbb{R}_+^\times} (\lambda x + \lambda^{-1} y) e^{-\pi(\lambda^2 x^2 + \lambda^{-2} y^2)} \frac{d\lambda}{\lambda} \\ &= \begin{cases} \mathrm{sign}(x) e^{-2\pi xy} & \text{if } xy > 0, \\ 0 & \text{otherwise.} \end{cases} \end{aligned}$$

In particular, fixing $h \in \mathrm{SO}_q(\mathbb{A})$, the rule

$$g \mapsto \tilde{\theta}_\Psi(g, h) := \sum_{x \in V} (g, h) \cdot \Psi(x),$$

where $(g, h) \cdot \Psi$ refers to the actions of $g \in \mathrm{SL}_2(\mathbb{A})$ on Ψ via the Weil representation, and of $h \in \mathrm{SO}_q(\mathbb{A})$ via translation on the arguments, defines an automorphic form on $\mathrm{SL}_2(\mathbb{A})$. The rule $\Psi \mapsto \tilde{\theta}_\Psi$ is equivariant for the $\mathrm{SL}_2(\mathbb{A})$-actions on both sides. We now integrate over $h \in \Gamma\backslash\mathrm{SO}_q(\mathbb{R})$ to check that

$$(g_\infty, g_f) \in \mathrm{SL}_2(\mathbb{A}) \mapsto \theta := \sum_{x \in \Gamma\backslash V} \overline{\Psi}_\infty^{g_\infty}(x) \cdot \Psi_f^{g_f}(x)$$

is again a modular form for $\mathrm{SL}_2(\mathbb{A})$. This gives the claimed statement. □

Now, we will explicitly take V to be K together with a suitable rescaling of the norm as quadratic form and explicate the above construction when Ψ_f is given by suitable characteristic functions.

Given any fractional ideal I of $\mathfrak{o}$ of norm $\mathrm{N}(I) \in \mathbb{Q}^{>0}$, which is relatively prime to δ, the group $\varepsilon^{2\mathbb{Z}}$ preserves the intersection I^+ (resp. I^-) of I with the cone of elements of positive (resp. negative) norm in $K \otimes \mathbb{R}$, as well as the subsets

$$I_1^+ := \{x \in I^+ \text{ with } x \equiv 1 \pmod{\delta}\},$$
$$I_1^- := \{x \in I^- \text{ with } x \equiv 1 \pmod{\delta}\}.$$

Taking Ψ_f to be the characteristic function of $\{x \in I \otimes \hat{\mathbb{Z}} : x \equiv 1(\delta)\}$, we recover Hecke's partial theta series

$$\vartheta^+(I)(q) := \sum_{x \in I_1^+/\varepsilon^{2\mathbb{Z}}} \mathrm{sign}(x) \cdot q^{xx'/D\mathrm{N}(I)},$$
$$\vartheta^-(I)(q) := \sum_{x \in I_1^-/\varepsilon^{2\mathbb{Z}}} \mathrm{sign}(x) \cdot q^{-xx'/D\mathrm{N}(I)}.$$

These theta series depend only on the image of I in the ray class group $\mathcal{C}_D$ and are modular forms of weight one on a suitable congruence subgroup. More precisely, by (55) or [HIM86, §1] we have the following:

LEMMA 3.7. *For all* $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(D)$,

$$\vartheta^+(I)\left(\frac{a\tau+b}{c\tau+d}\right) = \left(\frac{D}{|d|}\right) e^{\frac{-2\pi i ab}{D\mathrm{N}(I)}} (c\tau+d) \cdot \vartheta^+(aI)(\tau),$$
$$\vartheta^-(I)\left(\frac{a\tau+b}{c\tau+d}\right) = \left(\frac{D}{|d|}\right) e^{\frac{2\pi i ab}{D\mathrm{N}(I)}} (c\tau+d) \cdot \vartheta^-(aI)(\tau).$$

LEMMA 3.8. *We have*

$$2\theta_{\psi_1^{-1}} = \sum_{I \in \mathcal{C}_D} \psi_1(I)\vartheta^+(I)(q^D), \tag{57}$$
$$2\theta_{\psi_2^{-1}} = \sum_{I \in \mathcal{C}_D} \psi_2(I)\vartheta^-(I)(q^D). \tag{58}$$

Here, by convention, $\psi_1(J)$ *simply means the value of* ψ_1 *applied to the image of* J *in the ray class group* $\mathcal{C}_D$.

Proof. Rewrite the right-hand side of (57) as

$$\theta^+_{\psi_1^{-1}} := \sum_{\substack{I \in \mathcal{C}_D, \\ x \in I_1^+/\varepsilon^{2\mathbb{Z}}}} \psi_1(I) \cdot \mathrm{sign}(x) \cdot q^{xx'/\mathrm{N}(I)}, \tag{59}$$

where we have made the slight abuse of notation of choosing a representative I for each class in $\mathcal{C}_D$, and I_1^+ consists of elements in I of positive norm and congruent to 1 modulo δ. The set I_1^+ is the union of its totally positive and totally negative elements. Sending a pair (I, x) in the range of summation of the right-hand side

of (59), where x is totally positive (resp. totally negative), to the integral ideal $I^{-1}x$ determines two bijections:

$$(I, x \in I_1^+ \text{ totally positive}) \mapsto I^{-1}x, \tag{60}$$

$$(I, x \in I_1^+ \text{ totally negative}) \mapsto I^{-1}x, \tag{61}$$

to the set of integral prime-to-δ ideals. These two bijections are interchanged by precomposing with the involution $(I, x) \mapsto ((z)I, z \cdot x)$, where z is any totally negative element congruent to 1 modulo δ. Therefore, for a given integral prime-to-δ ideal J, the preimages (I, x) and (I', x') under these two bijections do not coincide; rather, the classes of I and I' in $\mathcal{C}_D$ differ by the image of $(-1) \in (\mathbb{Z}/D\mathbb{Z})^\times$ in $\mathcal{C}_D$. Being of mixed signature, the character ψ_1 sends this element to -1, and reindexing via $J = I^{-1}x$ allows us to rewrite (59) as $2\sum_J \psi_1^{-1}(J)q^{\mathrm{N}(J)}$, which is (up to the factor of 2) the standard expression for the θ-series $\theta_{\psi_1^{-1}}(q)$ attached to ψ_1^{-1}. This proves (57), and the proof of (58) is essentially the same. □

3.6. *Proof of Proposition 3.3*

With preliminaries on θ-series in hand, we proceed the proof of the first key step, Proposition 3.3.

Recall that N is a prime that splits in K as a product $\mathfrak{N}\mathfrak{N}'$ of two prime ideals of norm N. If I_1 and I_2 are (representatives of) elements of $\mathcal{C}_D$, thus, fractional ideals of K, the modular form

$$\Theta(I_1, I_2) = \vartheta^+(\mathfrak{N}'I_1)(q^N) \cdot \vartheta^-(I_2)(q) \tag{62}$$

is of weight two on $\Gamma(D) \cap \Gamma_0(N)$. Define

$$\Theta^{(1)}(I_1, I_2) = \text{trace of } \Theta(I_1, I_2) \text{ to level } \Gamma_0(N) \cap \Gamma_1(D),$$

$$\Theta^{(0)}(I_1, I_2) = \text{trace of } \Theta(I_1, I_2) \text{ to level } \Gamma_0(N) \cap \Gamma_0(D),$$

$$\Theta^{(\emptyset)}(I_1, I_2) = \text{trace of } \Theta(I_1, I_2) \text{ to level } \Gamma_0(N).$$

The superscripts here are intended to remind the reader of the level structure at D.

LEMMA 3.9. *For all ideals I_1 and I_2 of $\mathcal{C}_D$,*

$$\Theta^{(1)}(I_1, I_2) = \begin{cases} D \cdot \vartheta^+(\mathfrak{N}'I_1)(q^N) \cdot \vartheta^-(I_2)(q), & \text{if } \mathrm{N}(I_1) = \mathrm{N}(I_2), \\ 0 & \text{otherwise.} \end{cases} \tag{63}$$

Here, N *is the norm of* (53). *Moreover* $\Theta^{(0)}(I_1, I_2)$, *which therefore vanishes unless* (I_1, I_2) *belongs to the fiber product*

$$\mathcal{C}_D \times_W \mathcal{C}_D := \{(I_1, I_2) \in \mathcal{C}_D \times \mathcal{C}_D \text{ satisfying } \mathrm{N}(I_1) = \mathrm{N}(I_2)\},$$

depends only on the image of (I_1, I_2) *in the quotient* $(\mathcal{C}_D \times_W \mathcal{C}_D)/Z$.

Proof. The nonzero terms in the Fourier expansion of $\vartheta^+(\mathfrak{N}'I_1)(q^N)\cdot\vartheta^-(I_2)(q)$ are concentrated at powers of the form $q^{m/D}$, where

$$m \equiv 1/\mathrm{N}(I_1) - 1/\mathrm{N}(I_2) \pmod{D},$$

and the result follows, since the trace from $\Gamma(D)$ to $\Gamma_1(D)$ annihilates any term of the form $q^{m/D}$ with D not dividing m and multiplies the others by a factor of D. The final assertion follows from the explicit formula

$$\Theta^{(0)}(I_1, I_2) = \sum_{a\in(\mathbb{Z}/D\mathbb{Z})^\times} \Theta^{(1)}(aI_1, aI_2), \tag{64}$$

which is an immediate consequence of Lemma 3.7. □

Note that if (I_1, I_2) belongs to $(\mathcal{C}_D \times_W \mathcal{C}_D)$, then the same is true of (I_1, eI_2), where e is any element of $K^\times$ whose associated fractional ideal is prime to δ and satisfies $e^2 = 1 \pmod{\delta}$.

Proposition 3.10 (cf. Prop. 2.3). *For all $(I_1, I_2) \in (\mathcal{C}_D \times_W \mathcal{C}_D)/Z$, we have*

$$\Theta^{(\emptyset)}(I_1, I_2) = D\cdot \sum_{D=D_1D_2} \mu(D_1)\cdot D_2 \cdot \Theta^\sharp(I_1, \varepsilon_{D_1} I_2), \tag{65}$$

where μ is the Möbius function, and

(1) *$\Theta^\sharp(I_1, I_2)$ is the modular form defined in (50);*
(2) *The sum on the right is taken over all factorizations of D into (relatively prime) fundamental discriminants D_1, D_2;*
(3) *ε_{D_1} is a totally positive element which is congruent to -1 (resp 1) modulo the primes dividing D_1 (resp. D_2).*

Proof. By Lemma 3.9, it may be assumed that I_1 and I_2 have the same norm and are represented by ideals that are relatively prime to δ. We must prove an equality of the form

$$\text{Trace of } \Theta(I_1, I_2) \text{ from } \Gamma(D)\cap\Gamma_0(N) \text{ to } \Gamma_0(N) = \text{sum of } \Theta'\text{s}.$$

We will do this in a fashion very similar to the proof of Proposition 2.6, that is, by reducing it to a local question about Weil representations. Both $\Theta(I_1, I_2)$ and $\Theta^\sharp(I_1, I_2)$ have the general form

$$\Theta_\Psi(q) := \sum_{(x,y)\in V_\pm} \Psi(x, y)\,\mathrm{sign}(x)\cdot\mathrm{sign}(y)\cdot q^{Q(x,y)}, \tag{66}$$

where:

- $V = K \oplus K$ is considered as a quadratic space over $\mathbb{Q}$: we consider it as a $\mathbb{Q}$-vector space and endow it with the quadratic form

$$Q(x, y) = \frac{xx'}{D\mathrm{N}(I_1)} - \frac{yy'}{D\mathrm{N}(I_2)}.$$

- $V_\pm$ are elements (x, y) with $xx' > 0$ and $yy' < 0$.
- Ψ is a Schwartz function on $V\otimes\mathbb{A}_f$ (with $\mathbb{A}_f$ the ring of finite adeles), invariant by the action of the subgroup $\mathcal{U}$ of the unit group $\mathfrak{o}_1^\times\mathfrak{o}_1^\times$.

In the situation of (66) the map $\Psi \mapsto \Theta_\Psi$ is equivariant for the Weil representation action of $\mathrm{SL}_2(\mathbb{A}_f)$ on Schwartz functions on $V \otimes \mathbb{A}_f$; this action preserves the invariance condition on Ψ. Indeed this is a product of two copies of the situation already discussed in Section 3.5, and the Weil representation for a direct sum of quadratic spaces is simply the tensor product of the individual factors.

The action of $\mathrm{SL}_2(\mathbb{A}_f)$ on Schwartz functions just mentioned factors as a (restricted) tensor product of actions of $\mathrm{SL}_2(\mathbb{Q}_p)$ on the space of Schwartz functions on $V \otimes \mathbb{Q}_p$. The factor at p is the Weil representation of $\mathrm{SL}_2(\mathbb{Q}_p)$ on the Schwartz functions on the quadratic space (V_p, Q_p), where

$$V_p = (K \oplus K) \otimes \mathbb{Q}_p, \qquad Q_p(x, y) = \frac{xx'}{D\mathrm{N}(I_1)} - \frac{yy'}{D\mathrm{N}(I_2)}.$$

In this way, we are reduced to a problem in explicitly computing with this Weil representation: the question of computing the trace of $\Theta^\sharp(I_1, I_2)$ from $\Gamma_0(N) \cap \Gamma(D)$ to $\Gamma_0(N)$ reduces, thereby, to a product of local computations over p dividing D, which we will spell out in what follows. □

LEMMA 3.11 (cf. Lemma 2.7). *Let ℓ divide D.*

Let $(W, L, \langle , \rangle)$ be the quadratic space over $\mathbb{Q}_\ell$ given by $K \otimes \mathbb{Q}_\ell$ equipped with the norm form, multiplied by $(DN(I_1))^{-1}$ and L be the ring of integers. Let $(W', L', \langle , \rangle')$ be similarly defined but multiplying the form by $-(DN(I_2))^{-1}$ and taking L' to be the ring of integers.

Call $\mathbf{e}_1$ the characteristic function of

$$\{(x \in L, x' \in L') : x \equiv x' \equiv 1 \in (\mathbb{Z}/\ell)\},$$

considered as a Schwartz function on $W \oplus W'$. (Here the map from L to $\mathbb{Z}/\ell$ is given by reduction at the maximal ideal.)

Then, for the Weil representation action of $\mathrm{SL}_2(\mathbb{Q}_\ell)$ on Schwartz functions on $W \oplus W'$, the trace

$$\mathrm{Tr}^{\mathrm{SL}_2(\mathbb{Z}_\ell)}_{\Gamma(\ell)} \mathbf{e}_1 = \ell(\ell 1_{\mathcal{M}_+} - 1_{\mathcal{M}_-}),$$

where $\mathcal{M}_\pm$ are the two self-dual integral lattices contained in $(L \oplus L')$, is defined in (68).

Proposition 3.10 follows readily from this lemma. Indeed, from (62) we can write $\Theta(I_1, I_2)$ in the notation of (66) as the series Θ_Ψ with $\Psi = \otimes \Psi_\ell$ and Ψ_ℓ simply the characteristic function of $\mathfrak{N}' I_1 \oplus I_2$ for ℓ not dividing D, and $\Psi_\ell = \mathbf{e}_1$ for ℓ dividing D. We must only observe that, given a factorization $D = D_1 D_2$, the value of the corresponding Θ series where we replace the role of $\mathbf{e}_1$ with $\mathcal{M}_+$ for $\ell | D_1$ and with $\mathcal{M}_-$ for $\ell | D_2$ is exactly $\Theta^\sharp(I_1, I_2)$ but replacing $x \equiv y(\delta)$ with $x \equiv \varepsilon_{D_1} y(\delta)$, and this in turn coincides with $\Theta^\sharp(I_1, \varepsilon_{D_1} I_2)$ by means of the substitution $y \leftarrow \varepsilon_{D_1} y$.

Proof of Lemma 3.11. First we define $\mathcal{M}_\pm$. Let $(L \oplus L')^*$ be the dual lattice with respect to the quadratic form Q on $W \oplus W'$ and similarly define L^*, $(L')^*$. Then

L^* corresponds simply to the maximal ideal inside L, and similarly for L', so there are canonical identifications

$$(L/L^*) \simeq (\mathbb{Z}/\ell) \simeq L'/(L')^*, \qquad \frac{(L \oplus L')}{(L \oplus L')^*} \simeq (\mathbb{Z}/\ell)^2. \tag{67}$$

We let

$$\mathcal{M}_\pm = \text{ preimages of the lines } x_1 \equiv \pm x_2 \text{ in } (\mathbb{Z}/\ell\mathbb{Z})^2. \tag{68}$$

The function $\mathbf{e}_1$ is readily verified, using the formulas in (55), to be invariant by the principal congruence subgroup $\Gamma(\ell)$ of level ℓ inside $\mathrm{SL}_2(\mathbb{Z}_\ell)$. Indeed, using the Iwahori factorization of $\Gamma(\ell)$, it suffices to prove this for upper triangular unipotent elements, diagonal elements, and lower triangular unipotent elements congruent to the identity modulo ℓ. For the first two, this is obvious from the first two lines of (55); to conclude, we write the lower triangular unipotent subgroup with the conjugate of the upper triangular subgroup by the element

$$w = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

that appears on the last line of (55). Since the Weil constant $\gamma = 1$, it suffices to observe that w^{-1} acts as the inverse of the Fourier transform.

We must compute its trace to $\mathrm{SL}_2(\mathbb{Z}_\ell)$-invariants. Clearly, this projection is the same as if we first average over the diagonal subgroup, which has the effect of replacing $\mathbf{e}_1$ with $\frac{\sum_{j\neq 0} \mathbf{e}_j}{\ell-1}$ where $\mathbf{e}_j$ is the Schwartz function defined similarly to $\mathbf{e}_j$ but now considering $x_1 \equiv x_2 \equiv j$ modulo ℓ. Now $1_{\mathcal{M}_+} = \sum_j \mathbf{e}_j$, and so

$$\sum_{j\neq 0} \mathbf{e}_j = 1_{\mathcal{M}_+} - \mathbf{e}_0.$$

Now this is in fact invariant by $K_0(\ell) \subset \mathrm{SL}_2(\mathbb{Z}_\ell)$. Indeed $1_{\mathcal{M}_+}$ is already invariant by $\mathrm{SL}_2(\mathbb{Z}_\ell)$ since it is self-dual and integral for the quadratic form, and $\mathbf{e}_0$ is the characteristic function of $(L \oplus L')^*$, on which the quadratic form is integral. We will prove that (cf. (36))

$$\mathrm{trace}_{K_0(\ell)}^{\mathrm{SL}_2(\mathbb{Z}_\ell)} \mathbf{e}_0 = 1_{\mathcal{M}_+} + 1_{\mathcal{M}_-}. \tag{69}$$

From this it follows that the corresponding trace of $\sum_{j\neq 0} \mathbf{e}_j$ equals $\ell 1_{\mathcal{M}_+} - 1_{\mathcal{M}_-}$ and the lemma follows from this, taking into account the index $[K_0(\ell) : K(\ell)] = (\ell - 1)\ell$.

The proof of (69) is very similar to the computation carried out in Proposition 2.6 of the previous section and, more specifically, to (37). The role of $\mathcal{M}_\pm$ arises from the fact that

$$\{x \in L \oplus L' : Q(x) \in \mathbb{Z}_\ell\} = \mathcal{M}_+ \cup \mathcal{M}_-,$$

and indeed the function induced by the quadratic form upon the right-hand group of (67) is proportional to $(x_1, x_2) \in (\mathbb{Z}/\ell\mathbb{Z})^2 \mapsto \ell^{-1}(x_1^2 - x_2^2) \in \ell^{-1}\mathbb{Z}/\mathbb{Z}$. Let notation be as in (35); as discussed there, a system of coset representatives for

$\mathrm{SL}_2(\mathbb{Z}_\ell)/K_0(\ell)$ is given by w together with $wm(t)w$, where $1 \le t \le \ell$. We get $w\mathbf{e}_0 = \ell^{-1}1_{L\oplus L'}$, and thus

$$\sum_t m(t)w\mathbf{e}_0 = 1_{\mathcal{M}_+} + 1_{\mathcal{M}_-} - \mathbf{e}_0.$$

Therefore, $(w\sum_t m(t)w)\mathbf{e}_0 = 1_{\mathcal{M}_+} + 1_{\mathcal{M}_-} - w\mathbf{e}_0$, and so the trace of $\mathbf{e}_0$ is $1_{\mathcal{M}_+} + 1_{\mathcal{M}_-}$ as desired. □

We will now parlay Proposition 3.10 into an expression for the trace of the product $\theta_{\psi_1^{-1}}(q^N)\theta_{\psi_2^{-1}}(q)$ of weight one theta series. The following result immediately implies the desired Proposition 3.3 after performing a change of variables via the isomorphism $\mathcal{C}^2 \longrightarrow (\mathcal{C}_D \times_W \mathcal{C}_D)/Z$ of Lemma 3.5, given explicitly by $(I_1, I_2) \mapsto (I_1 I_2, I_1 I_2')$.

PROPOSITION 3.12. *Let*

$$G_{ND^2}(q) := \theta_{\psi_1^{-1}}(q^N) \cdot \theta_{\psi_2^{-1}}(q),$$

which belongs to the space $M_2(\Gamma_0(ND^2))$ of modular forms of level ND^2 with trivial nebentypus character. Then

$$\mathrm{Tr}_{ND}^{ND^2}(G_{ND^2}) = \psi_1(\mathfrak{N}')\frac{1}{4}\sum_{(\mathcal{C}_D\times_W\mathcal{C}_D)/Z} \psi_1(I_1)\psi_2(I_2)\cdot\Theta^{(0)}(I_1, I_2),$$

$$\mathrm{Tr}_{N}^{ND^2}(G_{ND^2}) = \psi_1(\mathfrak{N}')\cdot\frac{C}{4}\cdot\sum_{(\mathcal{C}_D\times_W\mathcal{C}_D)/Z} \psi_1(I_1)\psi_2(I_2)\cdot\Theta^{\sharp}(I_1, I_2),$$

where

$$C := D\sum_{D=D_1D_2}\mu(D_1)\cdot D_2\cdot\psi_1(\varepsilon_{D_1}) = D\prod_{p\mid D}(p - \psi_1(\varepsilon_p))$$

is a constant that depends on (ψ_1, ψ_2) and D but not on N.

Proof. By Lemma 3.8,

$$G_{ND^2}(q) = \frac{1}{4}\sum_{(I_1,I_2)\in\mathcal{C}_D^2} \psi_1(\mathfrak{N}'I_1)\vartheta^+(\mathfrak{N}'I_1)(q^{ND})\cdot\psi_2(I_2)\vartheta^-(I_2)(q^D),$$

where we re-indexed the sum for $\theta_{\psi_1^{-1}}$ via $I \leftarrow \mathfrak{N}'I$.

Because the restrictions to Z of the characters ψ_1 and ψ_2 are inverses of each other, the right-hand side can be rewritten as

$$\frac{1}{4}\sum_{\mathcal{C}_D^2/Z}\psi_1(\mathfrak{N}'I_1)\psi_2(I_2)\sum_{j\in Z}\vartheta^+(j\mathfrak{N}'I_1)(q^{ND})\vartheta^-(jI_2)(q^D),$$

where $Z \subset \mathcal{C}_D^2$ is embedded diagonally. It follows from (64) and (63) that

$$G_{ND^2}(q) = \frac{1}{4D}\sum_{\mathcal{C}_D^2/Z}\psi_1(\mathfrak{N}'I_1)\psi_2(I_2)\cdot\Theta^{(0)}(I_1, I_2)(q^D). \tag{70}$$

Both the left- and right-hand sides in this identity are modular forms on $\Gamma_0(ND^2)$. Let U_D be the Hecke operator which on q-expansions is given by

$$U_D\left(\sum a_n q^n\right) = \sum_{n\in\mathbb{Z}} a_{nD} q^n.$$

The trace from level D^2 to level D amounts to an application of $D \cdot U_D$, and by the same reasoning as in Lemma 3.9, we have

$$U_D(\Theta^{(0)}(I_1, I_2)(q^D)) = \begin{cases} \Theta^{(0)}(I_1, I_2)(q) & \text{if } \mathrm{N}(I_1) \equiv \mathrm{N}(I_2), \\ 0 & \text{otherwise.} \end{cases}$$

Applying the trace to level ND to both sides of (70) therefore gives

$$\mathrm{Tr}_{ND}^{ND^2}(G_{ND^2}) = \psi_1(\mathfrak{N}') \cdot \frac{1}{4} \cdot \sum_{(\mathcal{C}_D \times_W \mathcal{C}_D)/Z} \psi_1(I_1)\psi_2(I_2)\Theta^{(0)}(I_1, I_2)(q),$$

and the first equation in Proposition 3.12 follows directly. The second follows from this and (65), taking into account that ψ_2 and ψ_1 agree on ε_p. □

3.7. *Proof of Proposition 3.4*

Recall now the setup of Section 3.2. We choose narrow ideal classes I_1 and I_2 and, by choosing representatives by ideals that are divisible by $\mathfrak{N}$ but not $\mathfrak{N}'$, obtain a pair of real quadratic geodesics $\gamma_1 := \gamma_{I_1}$ and $\gamma_2 := \gamma_{I_2}$ in $\Gamma_0(N)\backslash\mathcal{H}$ with the same discriminant D. We also obtain embeddings α_i for $i \in \{1, 2\}$ attached to I_1 and I_2; similarly, we get eigenvectors $v_i, v_i' \in K^2$ and fixed points $\tau_i, \tau_i' \in K$ for the action of $\alpha_i(K^\times)$.

Proposition 3.4 asserts that the generating series of (45) is equal to

$$\Theta(\gamma_1 \otimes \gamma_2)(q) = \frac{1}{4} \cdot \Theta^\sharp(I_1 I_2, I_1 I_2')(q).$$

The proof proceeds, much as in the proof of the Gross–Zagier formula, by the most powerful technique known to number theory—*compute and compare.*

Examining the definition of $\Theta^\sharp(I_1, I_2)$ from (50), we see that

$$m\text{th Fourier coefficient of } \Theta^\sharp = 4 \sum_{(x,y)\in\mathcal{A}_m/\mathcal{U}} \mathrm{sign}(xy), \tag{71}$$

where $\mathcal{A}_m$ consists of the pairs $(x, y) \in \mathfrak{N}' I_1 I_2 \times I_1 I_2'$ satisfying

$$xx' > 0,\ yy' < 0, \qquad \frac{xx' - yy'}{a_1 a_2} = Dm, \tag{72}$$

where $a_1 = N(I_1)$, $a_2 = N(I_2)$ and $\mathcal{U}$ is the subgroup of $\mathfrak{o}_1^\times \times \mathfrak{o}_1^\times$ introduced in (49).

Now we turn to the left-hand side, which is more involved, and will take up the remainder of the subsection. We must compute the mth Fourier coefficient

$$a_m := \langle \gamma_1 \cdot T_m \gamma_2 \rangle_N.$$

Letting $M_0(N)_m$ be the set of elements of $M_0(N)$ of determinant m, and letting

$$\Gamma_1 := \alpha_1(\mathfrak{o}_1^\times), \qquad \Gamma_2 := \alpha_2(\mathfrak{o}_1^\times),$$

this intersection number can be rewritten as

$$a_m = \sum_{A \in \Gamma_1 \backslash M_0(N)_m / \Gamma_2} \langle (\tau_1, \tau_1') \cdot (A\tau_2, A\tau_2') \rangle. \tag{73}$$

(Note that in (73) the intersection numbers are now being computed on the upper half-plane and not on the modular curve.) The calculation proceeds by rewriting the coefficient a_m of (73) as a sum over certain ideals of K, by exploiting the map

$$\eta : M_2(\mathbb{Q}) \hookrightarrow K \oplus K, \qquad \eta(A) := (\det(v_1, Av_2), \det(v_1, Av_2')).$$

The map η sets up a $K \otimes K$-module isomorphism from $M_2(\mathbb{Q})$ to $K \oplus K$, the module structures being given by

$$(a \otimes b)M := \alpha_1(a')M\alpha_2(b) \quad \text{and} \quad (a \otimes b)(x, y) = (abx, ab'y) \tag{74}$$

respectively.

It is also an isomorphism of quadratic spaces, after equipping $K \oplus K$ with the quadratic form $Q(x, y) = \frac{xx'-yy'}{Da_1a_2}$.

LEMMA 3.13. *If $\eta(A) = (x, y)$, then*

$$\det(A) = \frac{xx' - yy'}{Da_1a_2}.$$

Proof. The source and the target of η are both cyclic $(K \otimes K)$-modules, as in (74), and both sides transform the same way, which reduces us to verifying the assertion for a single generator; taking A to be the identity and using $Da_1a_2 = \det(v_1, v_1')\det(v_2, v_2')$ this follows from the identity

$$\det(v_1, v_1')\det(v_2, v_2') - \det(v_1, v_2)\det(v_1', v_2') + \det(v_1, v_2')\det(v_1', v_2) = 0,$$

which can be derived by considering the determinant of the 4×4 matrix whose rows are two copies of $[v_1, v_1', v_2, v_2']$. □

PROPOSITION 3.14. *The image of $M_0(N)$ under η is equal to*

$$\eta(M_0(N)) = \{(x, y) \in \mathfrak{N}'I_1I_2 \times I_1I_2' \text{ with } x \equiv y \pmod{\delta}\},$$

and η induces a bijection between $\Gamma_1 \backslash M_0(N)_m / \Gamma_2$ and $\mathcal{A}_m/\mathcal{U}$.

Proof. Note that $K \otimes K$ is naturally identified with $K \oplus K$ via the map ϱ sending $a \otimes b$ to

$$\varrho(a \otimes b) = (ab, ab').$$

For $1 \le i, j \le 2$, let E_{ij} be the elementary matrix having a 1 in the ij entry and 0s elsewhere, and set $\beta_j = (-b_j + \sqrt{D})/2$. By the definition of η,

$$\eta(E_{11}) = \varrho(-a_1 \otimes \beta_2) \qquad \eta(E_{12}) = \varrho(-a_1 \otimes a_2),$$
$$\eta(E_{21}) = \varrho(\beta_1 \otimes \beta_2), \qquad \eta(E_{22}) = \varrho(\beta_1 \otimes a_2).$$

It follows that $\eta(M_2(\mathbb{Z}))$ is contained in the index D subgroup of $I_1 I_2 \times I_1 I_2'$ consisting of pairs that are congruent modulo δ. The fact that this containment is an equality follows by comparing the determinants of the pairing matrices for the two lattices relative to the quadratic forms $\det(A)$ and $\frac{xx'-yy'}{Da_1a_2}$ respectively. Furthermore, the lattice $\eta(M_0(N))$ is obtained by replacing the $\mathbb{Z}$-module generator $\eta(E_{21})$ with $N\eta(E_{21})$. A local analysis at N shows that

$$\eta(M_0(N)) \subset \mathfrak{N}' I_1 I_2 \times I_1 I_2'.$$

Since it is of index at most N in $\eta(M_2(\mathbb{Z}))$, it must be equal to

$$\{(x, y) \in \mathfrak{N}' I_1 I_2 \times I_1 I_2' \text{ with } x \equiv y \pmod{\delta}\},$$

as claimed. In particular, the map η identifies $M_0(N)_m$ with $\mathcal{A}_m$, and the last assertion follows from the fact that η transforms the left action of $\varepsilon \in \Gamma_1$ (resp. the right action of $\varepsilon \in \Gamma_2$) into multiplication by $(\varepsilon, \varepsilon)$ (resp. by $(\varepsilon, \varepsilon^{-1})$), which together generate $\mathcal{U}$. □

It is also crucial to interpret the intersection pairing $\langle \gamma_1 \cdot A\gamma_2 \rangle \in \{-1, 0, 1\}$ in terms of $\eta(A)$.

LEMMA 3.15. *If* $\det(A) = m > 0$, *then the intersection* $\langle \gamma_1 \cdot A\gamma_2 \rangle$ *is nonzero if and only if* $xx' > 0$ *and* $yy' < 0$, *where* $\eta(A) = (x, y)$. *In that case, it is given* (*after suitable choice of orientation conventions for the intersection*) *by* $\operatorname{sign}(xy)$.

Proof. Given any four distinct elements t_1, t_1', t_2, t_2' of $\mathbb{P}_1(\mathbb{R})$, the hyperbolic geodesics (t_1, t_1') and (t_2, t_2') intersect nontrivially if and only if the cross-ratios $[t_1, t_2'; t_2, t_1']$ and $[t_1, t_2; t_2', t_1']$ belong to the open interval $(0, 1) \subset \mathbb{R}$. This can be seen by exploiting the invariance of the cross ratio under Möbius transformations to reduce this statement to the special case in which $(t_1, t_1', t_2, t_2') = (0, \infty, 1, t)$, where it can be verified directly. In particular, the geodesics $(\gamma_1, A\gamma_2)$ intersect precisely when the following cross ratios belong to $(0, 1) \subset \mathbb{R}$:

$$\frac{xx'}{mDa_1a_2} = \frac{\det(v_1, Av_2)\det(v_1', Av_2')}{\det(v_1, v_1')\det(Av_2, Av_2')} = [\tau_1, A\tau_2'; A\tau_2, \tau_1'], \tag{75}$$

$$\frac{-yy'}{Da_1a_2} = \det(A)\frac{\det(\tau_1, A\tau_2')\det(\tau_1', A\tau_2)}{\det(\tau_1, \tau_1')\det(A\tau_2', A\tau_2)} = \det(A)[\tau_1, A\tau_2; A\tau_2', \tau_1']. \tag{76}$$

The first assertion follows. As to the second, the sign of

$$xy = \det(v_1, Av_2)\det(v_1', Av_2)$$

determines whether or not τ_1 lands inside or outside of the geodesic from $A\tau_2$ to $A\tau_2'$, and hence determines the sign of the nonzero intersection, given a suitable choice of orientation on $\mathcal{H}$. □

Recall that $\mathcal{U}$ acts naturally on the set $\mathcal{A}_m$ from (72). By combining Lemmas 3.13, 3.14, and 3.15, we obtain the following.

PROPOSITION 3.16. *For all $m \geq 1$,*

$$a_m = \sum_{(x,y)\in \mathcal{A}_m/\mathcal{U}} \operatorname{sign}(xy).$$

Comparing this proposition with (71) shows that

$$\Theta(\gamma_{I_1}, \gamma_{I_2}) = \frac{1}{4}\Theta^\sharp(I_1 I_2, I_1 I_2'),$$

and Proposition 3.4 follows.

4. Higher Eisenstein Elements

This section is devoted to a review of "higher Eisenstein elements" in the sense of Merel and Lecouturier [Mer96; Lec], that is, elements in suitable spaces of modular forms that are not killed by the Eisenstein ideal but by its square, see Definition 4.6. We will provide explicit formulas for Eisenstein and higher Eisenstein elements in

- the space $\mathbb{M}$ of modular forms (Proposition 4.1);
- the dual space $\mathbb{M}^*$ to modular forms (Theorem 4.9);
- the positive part of cohomology $\mathbb{H}^+$ of the modular curve (Theorem 4.8);
- the negative part of cohomology $\mathbb{H}^-$ of the modular curve (Section 4.4; here we do not need higher elements), and finally
- the supersingular module $\mathbb{D}$ (Theorem 4.11).

Each of these spaces $\mathbb{M}, \mathbb{H}^+, \mathbb{H}^-, \mathbb{D}$ is the completion of a suitable Hecke module at Mazur's Eisenstein ideal in the Hecke algebra.

4.1. Higher Eisenstein Series

As in Section 1.5, let $N > 3$ be a prime, let $M_2(N)$ be the module of weight two modular forms with Fourier coefficients in $Z = \mathbb{Z}[\frac{1}{6N}]$ for the Hecke congruence group $\Gamma_0(N)$, and let $S_2(N) \subset M_2(N)$ denote the submodule of cusp forms. Denote by $\mathbb{T}(N)$ the ring generated by the Hecke operators T_n (with $N \nmid n$) together with $T_N := U_N$, acting faithfully on $M_2(N)$.

The vector space $M_2(N) \otimes \mathbb{Q}$ is generated by $S_2(N) \otimes \mathbb{Q}$ along with the weight two Eisenstein series whose q-expansion is given by

$$E_2^{(N)}(q) = \frac{N-1}{24} + \sum_{n=1}^{\infty} \sigma_1^{(N)}(n) q^n \quad \text{where } \sigma_1^{(N)}(n) = \sum_{\substack{d|n,\\ N\nmid d}} d. \tag{77}$$

The homomorphism

$$\varphi_{\mathrm{Eis}} : \mathbb{T}(N) \longrightarrow \mathbb{Z}, \qquad \varphi_{\mathrm{Eis}}(T_n) := \sigma_1^{(N)}(n)$$

by which $\mathbb{T}(N)$ acts on $E_2^{(N)}$ is called the *Eisenstein homomorphism,* and its kernel I_{Eis} is called the *Eisenstein ideal.*

For any maximal ideal $\mathfrak{m}$ of $\mathbb{T}(N)$ and any $\mathbb{T}(N)$-module M, let $M_{\mathfrak{m}}$ denote the completion of M at $\mathfrak{m}$. The maximal ideal $\mathfrak{m}$ is said to be *Gorenstein* if

$\mathbb{T} := \mathbb{T}(N)_{\mathfrak{m}}$ is a Gorenstein ring. It is known that all maximal ideals of $\mathbb{T}(N)$ containing a prime $p > 3$ are Gorenstein by a result of Mazur [Maz77, cor. II.16.3].

Let $p > 3$ be a prime divisor of $N - 1$. The maximal ideal $\mathfrak{m} := (p, I_{\mathrm{Eis}})$ of $\mathbb{T}(N)$ is called the p-Eisenstein ideal. Let

$$\mathbb{T} := \mathbb{T}(N)_{\mathfrak{m}}, \qquad \mathbb{M} := M_2(N)_{\mathfrak{m}}$$

denote the completions of $\mathbb{T}(N)$ and $M_2(N)$ relative to this ideal. The ring $\mathbb{T}$ is a complete local ring which is free of finite rank as a $\mathbb{Z}_p$-module. The module $\mathbb{M}$ is canonically dual to $\mathbb{T}$ via the pairing $\mathbb{M} \times \mathbb{T} \longrightarrow \mathbb{Z}_p$ given by $\langle f, T\rangle = a_1(Tf)$, and hence $\mathbb{M}$ is free of rank one as a $\mathbb{T}$-module, since $\mathbb{T}$ is Gorenstein. The $\mathbb{Z}_p$-rank of $\mathbb{T}$ is strictly greater than one because p divides $N - 1$. We fix a discrete $\log (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{Z}/p^t\mathbb{Z}$ as in Section 1.5.

The following proposition is due to Lecouturier [Lec], but the details of the proof have been provided for the sake of being self-contained.

PROPOSITION 4.1. *There is a modular form $E' \in M_2(N) \otimes (\mathbb{Z}/p^t\mathbb{Z})$ having Fourier expansion of the form*

$$E' = \mathcal{M} - \sum_{n=1}^{\infty}\Big(\sum_{d|n'} \log(d^2/n')d\Big)q^n$$

for some $\mathcal{M} \in \mathbb{Z}/p^t\mathbb{Z}$, where n' denotes the prime-to-N part of n. It satisfies $(U_N - 1)E' = 0$ and, for all primes $\ell \neq N$,

$$(T_\ell - (\ell + 1))E' = (\ell - 1)\log(\ell)E_2^{(N)}.$$

The modular form E' mod p^t is called the *higher Eisenstein series* of weight 2 and level N. We will discuss abstractly such elements in other Hecke modules in Section 4.2.

Proof. Recall that $Z := \mathbb{Z}[1/6N]$ and let I denote the augmentation ideal in the group ring $Z[G_N]$, where G_N is as in (10). For d an integer prime to N, we shall denote by σ_d the corresponding element of G_N, arising from d by means of the homomorphism $\mathbb{Z} \to (\mathbb{Z}/N)^\times \to G_N$. Let $\mathbb{E}$ and $\mathbb{F}$ be the formal q-expansions with coefficients in $Z[G_N]$ given by

$$\mathbb{E} := \mathfrak{M} - \sum_{n=1}^{\infty}\Big(\sum_{\substack{d|n,\\ N\nmid d}} d\sigma_d\Big)q^n, \qquad \mathbb{F} := -\sum_{n=1}^{\infty}\Big(\sum_{\substack{d|n,\\ N\nmid n/d}} d\sigma_{n/d}\Big)q^n, \tag{78}$$

where

$$\mathfrak{M} := \frac{1}{2}\sum_{j=1}^{N-1}\theta_j \cdot \sigma_j \quad \text{with } \theta_j := \frac{N}{2}B_2(j/N),\ B_2(x) := x^2 - x + 1/6.$$

These formal q-expansions satisfy, for every Dirichlet character χ of modulus N,

$$\chi(\mathbb{E}) = \begin{cases} E_2^{(N)} = E_2(1, 1_N) & \text{if } \chi = 1; \\ E_2(1, \chi) & \text{otherwise,} \end{cases} \qquad \chi(\mathbb{F}) = \begin{cases} E_2(1_N, 1) & \text{if } \chi = 1; \\ E_2(\chi, 1) & \text{otherwise,} \end{cases}$$

where 1_N denotes the trivial character, but viewed as having modulus N, and $E_2(1,\chi)$ and $E_2(\chi,1)$ are the usual Eisenstein series associated to the Galois representations $\chi\omega \oplus 1$ and $\omega \oplus \chi$ respectively with ω the cyclotomic character, whose Fourier expansions are given by

$$E_2(1,\chi)(q) = -L(-1,\chi)/2 - \sum_{n=1}^{\infty}\Big(\sum_{d|n}\chi(d)d\Big)q^n,$$

$$E_2(\chi,1)(q) = -\sum_{n=1}^{\infty}\Big(\sum_{d|n}\chi(n/d)d\Big)q^n.$$

These Eisenstein series are classical modular forms of weight two on the congruence group $\Gamma_1(N)$, with the exception of $E_2(1_N,1)$. The latter is (the holomorphic part of) a *nearly holomorphic* form in the sense of Shimura, as we see via

$$E_2(1_N,1) = E_2(q) - E_2(Nq) + \frac{\text{const}}{y}$$
$$\text{with } E_2 = (8\pi y)^{-1} - \frac{1}{24} + \sum_{n}\Big(\sum_{d|n} d\Big)q^n.$$

Denote by $M_2^{\mathrm{nh}}(\Gamma_1(N);Z)$ the abelian group of q-expansions of such nearly holomorphic forms, so that $E_2(1_N,1) \in M_2^{\mathrm{nh}}$.

It follows that $\mathbb{E}$ is a classical modular form with coefficients in $Z[G_N]$. As for $\mathbb{F} := \sum_{\sigma\in G_N} F_\sigma \cdot \sigma$, although the individual coefficients $F_\sigma \in M_2^{\mathrm{nh}}(\Gamma_1(N);Z)$ are merely nearly holomorphic, their pairwise differences $F_{\sigma_1} - F_{\sigma_2}$ are in fact holomorphic, since they lie in the linear span of the $E_2(\chi,1)$ with χ nontrivial. It follows that one can write

$$\mathbb{F} = \mathbb{F}_0 + \eta\cdot\mathbf{N},$$

where

$$\mathbb{F}_0 \in M_2(\Gamma_1(N);Z[G_N]), \qquad \eta \in M_2^{\mathrm{nh}}(\Gamma_1(N);Z), \qquad \mathbf{N} = \sum_{\sigma\in G_N}\sigma.$$

Since the q-series $E_2(1,1_N)$ and $E_2(1_N,1)$ agree modulo p^t, and the image of the norm element $\mathbf{N}$ in $\mathbb{Z}/p^t\mathbb{Z}[G_N]$ belongs to I^2, the mod p^t reduction of the difference $\mathbb{E}-\mathbb{F}$ belongs to $M_2(\Gamma_1(N);\mathbb{Z}/p^t\mathbb{Z})\otimes I$. It follows that its natural image, denoted by $\overline{\mathbb{E}-\mathbb{F}}$, in $M_2(\Gamma_1(N);\mathbb{Z}/p^t\mathbb{Z})\otimes(I/I^2)$ gives rise to an element

$$\overline{\mathbb{E}-\mathbb{F}} \in M_2(\Gamma_1(N);\mathbb{Z}/p^t\mathbb{Z})\otimes(I/I^2) = M_2(\Gamma_1(N);\mathbb{Z}/p^t\mathbb{Z})\otimes G_N,$$

which is invariant under the diamond operators. At the last stage we have used the isomorphism $(I/I^2)\simeq G_N\otimes Z$ uniquely characterized by the fact that $\sum a_j\sigma_j \mapsto \prod j^{a_j}\otimes 1$ when $a_j\in\mathbb{Z}$. Consequently, $\overline{\mathbb{E}-\mathbb{F}}$ arises from a unique element of $M_2(\Gamma_0(N);\mathbb{Z}/p^t\mathbb{Z})\otimes G_N$, to be denoted by the same letter. One then readily checks that the modular form E' given by

$$E' := \log(\overline{\mathbb{E}-\mathbb{F}})$$

has all the properties claimed in the proposition. For instance, since $\mathbb{E}$ and $\mathbb{F}$ are eigenvectors for T_ℓ with eigenvalue $(1+\ell\sigma_\ell)$ and $(\sigma_\ell+\ell)$ respectively,

$$\begin{aligned}(T_\ell-(\ell+1))(\mathbb{E}-\mathbb{F}) &= (\ell\sigma_\ell-\ell)\mathbb{E}-(\sigma_\ell-1)\mathbb{F}\\ &= (\ell-1)(\sigma_\ell-1)E_2^{(N)} \pmod{I^2[[q]]},\end{aligned}$$

and therefore, after reducing modulo I^2 and taking the discrete logarithms on both sides,

$$(T_\ell-(\ell+1))E' = (\ell-1)\log(\ell)E_2^{(N)},$$

as claimed. □

REMARK 4.2. The proof of Proposition 4.1 yields an explicit formula for the constant term $\mathcal{M}$ of E'. It is attached to the Mazur–Tate, or Stickelberger element $\mathfrak{M}$, which is characterized as the unique element of $Z[G_N]$ satisfying

$$\chi(\mathfrak{M}) = \begin{cases}(1-N)/24 & \text{if } \chi=1;\\ -L(-1,\chi)/2 & \text{otherwise,}\end{cases} \qquad \text{for all } \chi : G_N \longrightarrow \mathbb{C}^\times.$$

This Mazur–Tate element belongs to the augmentation ideal I of the group ring $(\mathbb{Z}/p^t\mathbb{Z})[G_N]$, and its natural image in $I/I^2 = G_N \otimes (\mathbb{Z}/p^t\mathbb{Z})$, denoted by $\mathfrak{M}'$, is called the *"Mazur–Tate derivative"* of $\mathfrak{M}$. The constant term $\mathcal{M}$ is the discrete logarithm of this Mazur–Tate derivative

$$\mathcal{M} = \log(\mathfrak{M}'). \tag{79}$$

This explicit formula for $\mathcal{M}$, which was first obtained (under a slightly different guise) by Loic Merel [Mer96], will play no role in the argument.

4.2. *General Higher Eisenstein Elements*

From now on, the symbol I_{Eis} shall also be used to denote the Eisenstein ideal in the completed Hecke algebra $\mathbb{T}$, whose associated quotient $\mathbb{T}/I_{\mathrm{Eis}}$ is isomorphic to $\mathbb{Z}_p$.

Mazur has proved that $\mathbb{T}$ is generated by a single element as a $\mathbb{Z}_p$-algebra, that is, $\mathbb{T} = \mathbb{Z}_p[x]$ for suitable $x \in \mathbb{T}$. Indeed, one may take $x = T_\ell - \ell - 1$ for suitable ℓ, and x may be taken to generate I_{Eis}. See [Maz77, §II, Prop. 18.10], as well as the discussion at the start of Section 19 therein. The following result is also proved by Mazur (*loc. cit.* Proposition 18.8); we sketch a direct proof.

COROLLARY 4.3. *There is an isomorphism*

$$\eta : I_{\mathrm{Eis}}/I_{\mathrm{Eis}}^2 = \mathbb{Z}_p \otimes (\mathbb{Z}/N\mathbb{Z})^\times \simeq (\mathbb{Z}/p^t\mathbb{Z})$$

sending the element $(T_\ell-(\ell+1))$ *to* $(\ell-1)\otimes\ell$ *for all primes* $\ell \neq N$, *and sending* U_N *to* 1.

Sketch of proof. The modular form $E_2^{(N)} + \varepsilon E'$ with coefficients in the ring $\mathbb{Z}/p^t\mathbb{Z}[\varepsilon]$ of dual numbers is a Hecke eigenform on $\Gamma_0(N)$ and gives rise to a surjective homomorphism with kernel I_{Eis}^2

$$\begin{aligned} &\tilde{\varphi}_{\mathrm{Eis}} : \mathbb{T} \longrightarrow \mathbb{Z}/p^t\mathbb{Z}[\varepsilon], \qquad \tilde{\varphi}(U_N) = 1, \\ &\tilde{\varphi}(T_\ell) = (\ell+1) + (\ell-1)\log(\ell)\varepsilon. \end{aligned} \tag{80}$$

The quantity $\tilde{\varphi}(T_\ell - (\ell+1))$ is equal to $\log \circ \eta(T_\ell - (\ell+1))$, and the corollary follows. □

Let $\mathbb{X}$ be a free $\mathbb{T}$-module of rank one.

LEMMA 4.4. *The module $\mathbb{X}[I_{\mathrm{Eis}}]$ of elements $m \in \mathbb{X}$ satisfying*

$$(T_\ell - (\ell+1))m = 0 \quad \textit{for all primes } \ell \neq N, \qquad U_N m = m,$$

is free of rank one over $\mathbb{Z}_p$.

Proof. Since the localization of $\mathbb{T}$ at I_{Eis} is Gorenstein, the I_{Eis}-torsion submodule of X is isomorphic to $\mathbb{X}/I_{\mathrm{Eis}}\mathbb{X}$, and the result therefore follows from the fact that $\mathbb{T}/I_{\mathrm{Eis}}$ is isomorphic to $\mathbb{Z}_p$. □

A generator of the $\mathbb{Z}_p$-module $\mathbb{X}[I_{\mathrm{Eis}}]$ is called an *Eisenstein element* in $\mathbb{X}$. Although such generators are only well defined up to scaling by $\mathbb{Z}_p^\times$, the concrete Hecke modules that arise in practice are frequently equipped with a distinguished choice of Eisenstein element m_0. Corollary 4.3 implies the following lemma.

LEMMA 4.5. *There is an element $m_1 \in \mathbb{X}/p^t\mathbb{X}$ satisfying $U_N m_1 = m_1$ and*

$$\begin{aligned} &(T_\ell - (\ell+1))m_1 = (\ell-1)\log(\ell)m_0 \pmod{p^t} \\ &\quad \textit{for every prime } \ell \neq N, \end{aligned} \tag{81}$$

and the choice of m_0 uniquely specifies m_1 up to the addition of a multiple of m_0.

The element m_1 depends linearly on the choice of discrete logarithm, namely, replacing log with $a \cdot \log$ with $a \in (\mathbb{Z}/p^t\mathbb{Z})^\times$ has the effect of replacing m_1 with am_1.

DEFINITION 4.6. The element m_1 is called the *higher Eisenstein element* in $\mathbb{X}/p^t$ (associated to m_0 and to the choice of discrete logarithm).

For example, (the Eisenstein completion) $\mathbb{M} = M_2(N)_{\mathfrak{m}}$ of the module of modular forms has a distinguished Eisenstein element $m_0 = E_2^{(N)}$. Proposition 4.1 supplies an explicit description of the higher Eisenstein element $m_1 = E'$ in $\mathbb{M} \otimes (\mathbb{Z}/p^t\mathbb{Z})$. The proof of Conjecture 1.1 for dihedral forms rests crucially on similar explicit expressions of the higher Eisenstein element in various other Hecke modules, which will be described in the forthcoming sections.

REMARK 4.7. When $\mathcal{M} \equiv 0 \pmod{p^u}$ with $u \leq t$, there is also a *second higher Eisenstein element* $m_2 \in \mathbb{X} \otimes (\mathbb{Z}/p^u\mathbb{Z})$ satisfying, for all primes $\ell \neq N$,

$$(T_\ell - (\ell+1))m_2 = (\ell-1)\log(\ell)m_1 \pmod{m_0\mathbb{X}}.$$

In fact, in $\mathbb{X} \otimes (\mathbb{Z}/p\mathbb{Z})$ there is an entire sequence $m_0, m_1, \ldots, m_r \in \mathbb{X} \otimes (\mathbb{Z}/p\mathbb{Z})$ of higher Eisenstein elements obeying similar inductive relations, where $r+1$ is the $\mathbb{Z}_p$-rank of $\mathbb{T}$. These higher Eisenstein elements have been studied systematically in [Lec], but only the first higher Eisenstein elements will play a role in this work. Henceforth, the terminology "higher Eisenstein series" or "higher Eisenstein element" shall always refer to what might be called the "first higher Eisenstein element" in [Lec].

4.3. The Betti Cohomology Relative to the Cusps

One of the settings which turns out to be relevant to the proof of Conjecture 1.1 for RM dihedral forms occurs when $\mathbb{X} := \mathbb{H}^+$ is the p-Eisenstein completion of the relative cohomology $H^1_{\mathrm{B}}(X_0(N); \{0,\infty\}; Z)^+$ with coefficients in the ring $Z := \mathbb{Z}[1/6N]$, where the superscript $+$ denotes the subspace which is fixed by complex conjugation. As discussed in Section 1.5, the subscript B means that we take the singular cohomology of the *complex points* of $X_0(N)$. This relative cohomology is dual to $H^1_{\mathrm{B}}(Y_0(N), Z)^-$, which is isomorphic, after tensoring with $\mathbb{C}$, to the space of weight two modular forms on $\Gamma_0(N)$ via integration. In particular, the ring generated by the Hecke operators acting on $H^1_{\mathrm{B}}(X_0(N); \{0,\infty\}; Z)^+$ is naturally identified with $\mathbb{T}(N)$.

The module $H^1_{\mathrm{B}}(X_0(N); \{0,\infty\}; Z)^+$ fits into the short exact sequence

$$0 \longrightarrow Z \xrightarrow{\partial^*} H^1_{\mathrm{B}}(X_0(N); \{0,\infty\}; Z)^+ \xrightarrow{i^*} H^1_{\mathrm{B}}(X_0(N), Z)^+ \longrightarrow 0 \tag{82}$$

of $\mathbb{T}(N)$-modules, where ∂^* is dual to the boundary homomorphism

$$\partial : H_{1,\mathrm{B}}(X_0(N); \{0,\infty\}; Z) \longrightarrow Z \cdot (0-\infty) = Z. \tag{83}$$

The relative cohomology group $H^1_{\mathrm{B}}(X_0(N); \{0,\infty\}; Z)$ can be described concretely in terms of Z-valued modular symbols: $\Gamma_0(N)$-invariant functions m from $\mathbb{P}_1(\mathbb{Q}) \times \mathbb{P}_1(\mathbb{Q})$ to Z which are *additive* in the sense that they satisfy

$$m\{a,b\} + m\{b,c\} = m\{a,c\} \quad \text{for all } a,b,c \in \mathbb{P}_1(\mathbb{Q}).$$

The image of the class $\partial^*(1)$ in $\mathbb{H}^+$, denoted by κ_0^+, is a distinguished Eisenstein element in $\mathbb{H}^+$, which corresponds to the *boundary symbol* sending (a,b) to $f_\infty(b) - f_\infty(a)$, where f_∞ is the unique $\Gamma_0(N)$-invariant function on $\mathbb{P}_1(\mathbb{Q})$ which sends ∞ to 1 and 0 to 0. Let

$$\bar{\kappa}_1^+ : \Gamma_0(N) \longrightarrow (\mathbb{Z}/p^t\mathbb{Z}), \qquad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \log(a).$$

Since it is trivial on parabolic elements, it can be viewed as an element of $H^1_{\mathrm{B}}(X_0(N), \mathbb{Z}/p^t\mathbb{Z})^+$. Let $\kappa_1^+ \in \mathbb{H}^+ \otimes (\mathbb{Z}/p^t\mathbb{Z})$ be the class obtained by choosing a preimage of $\bar{\kappa}_1^+$ under i^* in the exact sequence obtained from (82) by replacing Z with $(\mathbb{Z}/p^t\mathbb{Z})$ and projecting it to $\mathbb{H}^+$. This class depends on the choice

of preimage, but only up to the addition of a multiple of κ_0^+. Furthermore, it is annihilated by I_{Eis}^2, since $\bar{\kappa}_1^+$ is annihilated by I_{Eis}, and therefore, for all rational primes $\ell \neq N$, the class $(T_\ell - (\ell+1))\kappa_1^+$ is a multiple of the boundary symbol κ_0^+.

THEOREM 4.8. *The class κ_1^+ is the higher Eisenstein element in $\mathbb{H}^+ \otimes (\mathbb{Z}/p^t\mathbb{Z})$ attached to κ_0^+.*

Proof. The modular symbol attached to κ_1^+ admits an explicit description when restricted to $\Gamma_0(N)0 \times \Gamma_0(N)0$. Namely, if r/s and t/u (viewed as fractions in lowest terms, with the convention that $\infty = 1/0$, so that, in particular, s and u belong to $(\mathbb{Z}/N\mathbb{Z})^\times$) are elements of this $\Gamma_0(N)$-orbit, we have

$$\kappa_1^+(\{r/s, t/u\}) = \log(s/u).$$

This fact is proved by observing that the matrix

$$\gamma := \begin{pmatrix} u' & t \\ * & u \end{pmatrix} \begin{pmatrix} s & -r \\ * & s' \end{pmatrix} \in \Gamma_0(N), \qquad uu' \equiv ss' \equiv 1 \pmod{N}$$

sends r/s to t/u, and hence $\kappa_1^+(\{r/s, t/u\}) = \bar{\kappa}_1^+(\gamma) = \log(su')$. To calculate the constant of proportionality relating $(T_\ell - (\ell+1))\kappa_1^+$ and κ_0^+, we exploit the usual formula for the action of the Hecke operators on modular symbols (cf. [Maz77, Prop 18.9]):

$$\begin{aligned}(T_\ell - (\ell+1))\kappa_1^+(\{0,\infty\}) &= \kappa_1^+\left(\{0,\infty\} + \sum_{i=0}^{\ell-1}\{i/\ell, \infty\} - (\ell+1)\{0,\infty\}\right) \\ &= \sum_{i=1}^{\ell-1}\kappa_1^+(\{i/\ell, 0\}) = (\ell-1)\log(\ell) \\ &= (\ell-1)\log(\ell)\cdot\kappa_0^+(\{0,\infty\}).\end{aligned}$$

The result follows. □

4.4. *The Betti Cohomology of the Open Modular Curve*

Consider now the case where

$$\mathbb{X} = \mathbb{H}^- = H_{\mathrm{B}}^1(Y_0(N), Z)_{\mathfrak{m}}^-.$$

The exact sequence

$$0 \longrightarrow H_{\mathrm{B}}^1(X_0(N), Z)^- \longrightarrow H_{\mathrm{B}}^1(Y_0(N), \mathbb{Z})^- \longrightarrow Z \longrightarrow 0$$

produces an explicit rank one quotient of $H_{\mathrm{B}}^1(Y_0(N), \mathbb{Z})^-$ which is Eisenstein. The Eisenstein element κ_0^- in $\mathbb{H}^-$ is described by the Dedekind–Rademacher homomorphism on $\Gamma_0(N)$ described in [Maz79, §II.2]:

$$\kappa_0^-(\gamma) = \frac{1}{2\pi i}(\log(\Delta_N)(\gamma z) - \log(\Delta_N)(z)),\ \Delta_N(z) := \Delta(Nz)/\Delta(z),$$

which encodes the periods of the modular unit $\Delta_N \in \mathcal{O}^\times_{Y_0(N)}$. It is given by the formula

$$\kappa_0^- \begin{pmatrix} a & b \\ Nc & d \end{pmatrix} = \begin{cases} (N-1)b/d & \text{if } c = 0; \\ \frac{(N-1)(a+d)}{cN} + 12\,\mathrm{sign}(c) D^N(\frac{a}{N|c|}) & \text{if } c \neq 0, \end{cases}$$

where $\mathbf{D}^N(x) = \mathbf{D}(x) - \mathbf{D}(Nx)$ and $\mathbf{D}$ is the Dedekind sum

$$\mathbf{D}(a/m) = \sum_{j=1}^{m-1} B_1(j/m) B_1(aj/m) \quad \text{for } m > 0, \qquad \gcd(a, m) = 1.$$

The homomorphism κ_0^- can also be written as

$$\kappa_0^- \begin{pmatrix} a & b \\ Nc & d \end{pmatrix} = \varphi \begin{pmatrix} a & b \\ Nc & d \end{pmatrix} - \varphi \begin{pmatrix} a & Nb \\ c & d \end{pmatrix}, \tag{84}$$

where $\varphi : \mathrm{SL}_2(\mathbb{Z}) \longrightarrow \mathbb{Z}$ is the Rademacher φ-function given by

$$\varphi \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{cases} -b/d & \text{if } c = 0; \\ \frac{-(a+d)}{c} + 12\,\mathrm{sign}(c) \mathbf{D}(\frac{a}{|c|}) & \text{if } c \neq 0. \end{cases} \tag{85}$$

In [Lec], a formula for the higher Eisenstein element attached to κ_0^- is given, which we omit because it shall not be needed in this work.

4.5. The Dual of the Modular Forms

This section considers the case where $\mathbb{X} := \mathbb{M}^*$ is the completion of

$$M_2(N)^\vee = \hom(M_2(N), Z)$$

at the p-Eisenstein ideal. It is a free $\mathbb{T}$-module of rank one, and is also equipped with an Eisenstein element $\mathfrak{S}_0$ defined by

$$\mathfrak{S}_0(f) = a_0(f),$$

where $a_0(f)$ denotes the constant term of the modular form f at the cusp $\infty \in X_0(N)$. Let $\mathfrak{S}_1$ denote the higher Eisenstein element in $\bar{\mathbb{M}}^* := \mathbb{M}^* \otimes (\mathbb{Z}/p^t\mathbb{Z})$ attached to $\mathfrak{S}_0$. It turns out to be related to the *Shimura class* $\mathfrak{S}$ described in the Introduction.

More precisely, the inclusion $S_2(N) \hookrightarrow M_2(N)$ induces a surjection $\mathbb{M}^* \to \mathbb{S}^*$. Fix any lift of $\mathfrak{S}$ to $\bar{\mathbb{M}}^* = \mathbb{M}^* \otimes (\mathbb{Z}/p^t\mathbb{Z})$ via this surjection denoted by $\mathfrak{S}_1$. Note that $\mathfrak{S}_1$ is not completely well defined, but that any two choices of lift differ by a multiple of $\mathfrak{S}_0 \pmod{p^t}$.

THEOREM 4.9. *The class $\mathfrak{S}_1$ is the higher Eisenstein element in $\mathbb{M}^* \otimes (\mathbb{Z}/p^t\mathbb{Z})$ attached to the Eisenstein class $\mathfrak{S}_0$.*

Proof. The class $\mathfrak{S}_1$ arises from the $\bar{\kappa}_1^+$ described in the discussion preceeding Theorem 4.8 by means of the "étale to coherent" morphism $H^1_{\mathrm{et}}(X_0(N), \mathbb{Z}/p^t\mathbb{Z}) \longrightarrow H^1(X_0(N)_{/\mathbb{Z}/p^t\mathbb{Z}}, \mathbb{G}_a)$.

For reasons that will become clear in what follows, instead of working with $X_0(N)$ over the spectrum of $\mathbb{Z}_p$, we will use an unramified extension W of $\mathbb{Z}_p$ containing the Nth roots of unity. Clearly, it is enough to prove the claimed statement in $\mathbb{M}^* \otimes (W/p^tW)$ instead of $\mathbb{M}^* \otimes \mathbb{Z}/p^t$ since $\mathbb{Z}/p^t \hookrightarrow W/p^tW$.

Let $\iota : \text{cusps} \hookrightarrow X_0(N)$ be the inclusion of the cuspidal divisor, a relative divisor over Z. Let $j : Y_0(N) \to X_0(N)$ be the complementary open immersion. Now, there are compatible short exact sequences of étale sheaves on $X_0(N)_{W/p^t}$, the base change of $X_0(N)$ along $Z \to W/p^t$:

$$\begin{array}{ccc} j_!(\mathbb{Z}/p^t) & \longrightarrow & \mathcal{O}(-\text{cusps}) \\ \downarrow & & \downarrow \\ (\mathbb{Z}/p^t) & \longrightarrow & \mathcal{O} \\ \downarrow & & \downarrow \\ i_*(\mathbb{Z}/p^t) & \longrightarrow & \mathcal{O}_{\text{cusps}} \end{array} \tag{86}$$

Note that we are dealing here with étale sheaves whose order is not prime to the residual degrees, but all we are using is the existence of this diagram. Taking cohomology now gives the following commutative diagram which is compatible with Hecke operators:

$$\begin{array}{ccccc} H^0_{\text{et}}(\text{cusps}_W; \mathbb{Z}/p^t\mathbb{Z}) & \longrightarrow & H^0(\text{cusps}_{W/p^t}, \mathcal{O}) & & \\ \downarrow & & \downarrow & & \\ H^1_{\text{et}}(X_0(N)_W, \text{cusps}_W; \mathbb{Z}/p^t\mathbb{Z}) & \longrightarrow & H^1(X_0(N)_{W/p^t}, \mathcal{O}(-\text{cusps})) & \longrightarrow & \text{Hom}(M_2(N), W/p^t) \\ \downarrow & & \downarrow & & \downarrow \\ H^1_{\text{et}}(X_0(N)_W, \mathbb{Z}/p^t\mathbb{Z})^{(0)} & \longrightarrow & H^1(X_0(N)_{W/p^t}, \mathcal{O}) & \longrightarrow & \text{Hom}(S_2(N), W/p^t). \end{array} \tag{87}$$

Here, the groups in the middle column are Zariski cohomology groups; the map from left to middle column arises from, first of all, restricting to W/p^t, then using (86) and the fact that coherent sheaves have the same cohomology in Zariski and étale topology. The zero superscript in the bottom left of (87) refers to classes that are trivial when pulled back to the cusps. The maps from middle to right are induced by the Serre duality pairings as in (11).

The Shimura class $\mathfrak{S} \in H^1_{\text{et}}(X_0(N)_{\mathbb{Z}_p}, \mathbb{Z}/p^t)$ gives rise to a class in the group $H^1_{\text{et}}(X_0(N)_W, \mathbb{Z}/p^t)^{(0)}$ in the lower left of (87) (which we also denote by $\mathfrak{S}$), that is, $\mathfrak{S}$ becomes trivial when pulled back to the cusps—because the cusps are defined over W. Fix a lift

$$\tilde{\mathfrak{S}} \in H^1_{\text{et}}(X_0(N)_W, \text{cusps}_W; \mathbb{Z}/p^t\mathbb{Z})$$

to the middle left group in (87). Now this left-hand term can be compared with (82) via restriction to the geometric generic fiber, that is, the fiber over $\overline{\mathbb{Q}}_p$, and it

follows from Theorem 4.8 that

$$(T_\ell - \ell - 1)\tilde{\mathfrak{S}} = (\ell - 1)\log(\ell)\mathfrak{S}$$

holds after restriction to this geometric generic fiber.

We claim that "restriction to the geometric generic fiber" is injective on the group $H^1_{\text{et}}(X_0(N)_W, \text{cusps}_W; \mathbb{Z}/p^t)$. To see this, let $E = W \otimes \mathbb{Q}_p$ be the quotient field of W. In view of diagram (87), it is enough to check that the kernel of the map

$$q : H^1_{\text{et}}(X_0(N)_W, \mathbb{Z}/p^t) \to H^1_{\text{et}}(X_0(N)_{\overline{\mathbb{Q}}_p}, \mathbb{Z}/p^t)$$

is precisely the image of $H^1_{\text{et}}(\text{Spec } W, \mathbb{Z}/p^t)$ on the left.

A class in the kernel of q amounts to an étale $\mathbb{Z}/p^t$-cover of $X_0(N)_W$ which becomes trivial on the geometric generic fiber. This cover is uniquely determined by its restriction to $X_0(N)_E$ (see [SGA1, Théorème 3.8, Exposé X]) where it becomes trivial on passage to a finite field extension of E, that is, the cover on $X_0(N)_E$ necessarily arises from a character $\text{Gal}(\overline{\mathbb{Q}}_p/E) \to \mathbb{Z}/p^t$. For such a cover to extend over $X_0(N)_W$, the character χ must be unramified. (For instance, this can be seen by restricting to the cuspidal sections.) This implies the claim regarding $\ker(q)$ and concludes the proof. □

Remark 4.10. Theorem 4.9 implies Merel's theorem that $\langle \mathfrak{S}_1, E_2^{(N)} \rangle = \mathcal{M}$, where $\mathcal{M}$ is the Merel constant of (79), since, letting E' be the mod p^t modular form defined in Proposition 4.1, $\langle \mathfrak{S}_1, E_2^{(N)} \rangle = \langle \mathfrak{S}_0, E' \rangle = a_0(E') = \mathcal{M}$.

4.6. Supersingular Divisors and Modular Units

Recall from Section 2.2 the module $\text{Div}(\mathcal{E})$ of $\mathbb{Z}$-linear combinations of isomorphism classes of supersingular elliptic curves over $\overline{\mathbb{F}}_N$.

The Jacquet–Langlands correspondence shows that $\text{Div}(\mathcal{E}) \otimes \mathbb{C}$ is abstractly isomorphic to $M_2(N; \mathbb{C})$ as a module over the ring of Hecke operators, and in particular the Hecke ring for $\text{Div}(\mathcal{E})$ can be identified with $\mathbb{T}(N)$. In this section we consider the case where $\mathbb{X} := \mathbb{D}$ is the p-Eisenstein completion of $\text{Div}(\mathcal{E})$.

The vector (in the notation of Section 2.2)

$$\Sigma_0 := \sum_{i=1}^{n} \frac{e_i}{w_i} \in \mathbb{D} \tag{88}$$

satisfies $T_\ell \Sigma_0 = (\ell + 1)\Sigma_0$ for all $\ell \neq N$, and is thus an Eisenstein element in $\mathbb{D}$.

Let $\Sigma_1 \in \mathbb{D} \otimes (\mathbb{Z}/p^t\mathbb{Z})$ denote the higher Eisenstein element associated to Σ_0, as specified in Definition 4.6. The main goal of this section is to give an explicit construction of Σ_1 in terms of the restrictions of certain modular units to the supersingular locus. This construction is inspired from [Lec] and involves the Eisenstein series E_{N+1} of weight $N + 1$, and the cusp form Δ of weight 12, viewed as modular forms mod N of level 1.

Let $\mathcal{O}_N$ denote the ring of (meromorphic) modular functions on the modular curve of level one over $\text{Spec}(\mathbb{Z}/N\mathbb{Z})$ that are regular at its supersingular points.

Since p is odd and $p \nmid N+1$, the discrete logarithm log extends uniquely to the multiplicative group $\mathbb{F}_{N^2}^\times$, and can therefore be used to define a homomorphism

$$\mathrm{Log} : \mathcal{O}_N^\times \longrightarrow \mathrm{Div}(\mathcal{E}) \otimes (\mathbb{Z}/p^t\mathbb{Z}), \qquad \mathrm{Log}(U) := \sum_{i=1}^{n} \log(U(e_i)) \cdot \frac{e_i}{w_i}. \quad (89)$$

It shall be useful to introduce *multiplicative Hecke operators* acting on the multiplicative monoid in the graded ring of modular forms mod N. To describe these operators, we shall adopt Katz's point of view to describe modular forms over a ring. Recall that a *Katz test object* over $\mathbb{F}_N = \mathbb{Z}/N\mathbb{Z}$ is a pair $(A, \omega)_{/R}$, where

(i) A is an elliptic curve over an $\mathbb{F}_N$-algebra R;
(ii) ω in an R-module generator of $H^0(A, \Omega^1_A)$.

A *weakly holomorphic modular form of weight k and level* 1 *over* $\mathbb{F}_N$ is a rule f which to any such test object associates an invariant $f(A, \omega) \in R$, satisfying

(1) $f(A, \omega)$ depends only on the R-isomorphism class of (A, ω);
(2) f commutes with base change with respect to any homomorphism $R \to R'$ of $\mathbb{F}_N$-algebras, in the obvious sense;
(3) $f(A, u\omega) = u^{-k} f(A, \omega)$ for any $u \in R^\times$.

Let $(A_q, \omega_{\mathrm{can}})$ denote the "Tate test object" over $\mathbb{F}_N((q))$, whose points over this local field are identified with $\mathbb{F}_N((q))^\times/q^{\mathbb{Z}}$, equipped with its canonical differential $\omega_{\mathrm{can}} = dt/t$. If $f(A_q, \omega_{\mathrm{can}})$ lies in $\mathbb{F}_N[[q]]$ (resp. $q\mathbb{F}_N[[q]]$), then f is called a modular form (resp. a cusp form). The space of modular forms and cusp forms of weight k and level 1 over $\mathbb{F}_N$ shall simply be denoted by M_k and S_k respectively.

Let $\ell \neq N$ be a prime. The *multiplicative Hecke operator*

$$T_\ell^\times : M_k \longrightarrow M_{k(\ell+1)}$$

is defined by setting

$$(T_\ell^\times f)(A, \omega) = \prod_{\varphi} f(A', \omega'), \quad (90)$$

where the product is taken over the distinct isogenies $\varphi : A \to A'$ of degree ℓ, with ω' determined by $\omega := \varphi^*\omega'$. Up to language this is already in [Hur81]. One readily checks that $T_\ell^\times$ maps M_k to $M_{(\ell+1)k}$, as claimed. Of course, $T_\ell^\times$ is not additive but it is compatible with multiplication on the graded ring of modular forms over $\mathbb{F}_N$:

$$T_\ell^\times(fg) = T_\ell^\times(f) T_\ell^\times(g).$$

In particular, it induces homomorphisms $T_\ell^\times : \mathcal{O}_N^\times \longrightarrow \mathcal{O}_N^\times$ for which the diagram

$$\begin{array}{ccc} \mathcal{O}_N^\times & \xrightarrow{T_\ell^\times} & \mathcal{O}_N^\times \\ \downarrow \mathrm{Log} & & \downarrow \mathrm{Log} \\ \mathrm{Div}(\mathcal{E}) \otimes (\mathbb{Z}/p^t\mathbb{Z}) & \xrightarrow{T_\ell} & \mathrm{Div}(\mathcal{E}) \otimes (\mathbb{Z}/p^t\mathbb{Z}) \end{array} \tag{91}$$

commutes.

Consider the meromorphic modular function

$$\Sigma^\times := \frac{E_{N+1}^{12}}{\Delta^{N+1}} \tag{92}$$

of level one. By a result of Katz ([Kat, Theorem 3.1]), E_{N+1} has no common zero with the Hasse invariant. Since the Hasse invariant has simple zeroes at the supersingular points, it follows that $\Sigma^\times$ belongs to $\mathcal{O}_N^\times$ and therefore that the vector

$$\Sigma_1 := \frac{1}{12}\mathrm{Log}(\Sigma^\times) \in (\mathbb{Z}/p^t\mathbb{Z}) \otimes \mathrm{Div}(\mathcal{E}) \tag{93}$$

is well defined. Note that the class of Σ_1 mod $\mathbb{Z}/p^t\mathbb{Z} \cdot \Sigma_0$ does not depend on the way one normalizes the constant term of E_{N+1}.

THEOREM 4.11. *For all primes $\ell \neq N$,*

$$(T_\ell - (\ell+1))\Sigma_1 = (\ell-1)\log(\ell)\Sigma_0,$$

and Σ_1 is therefore equal to the higher Eisenstein element attached to $\Sigma_0 \in \mathbb{D}$.

Proof. While the Eisenstein series E_{N+1} presumably exhibits a complicated behavior under the multiplicative Hecke operators, a result of G. Robert ([Rob80, Théorème B]) asserts that if (A, ω) and (A', ω') are marked *supersingular* elliptic curves and $\varphi : A \longrightarrow A'$ is an isogeny of degree ℓ satisfying $\varphi^*(\omega') = \omega$, then

$$E_{N+1}(A', \omega') = \ell E_{N+1}(A, \omega) \quad \text{for all } A \in \mathcal{E}. \tag{94}$$

It follows that

$$T_\ell^\times E_{N+1} = \ell^{\ell+1} E_{N+1}^{\ell+1}. \tag{95}$$

In addition, for every prime $\ell \neq N$,

$$T_\ell^\times \Delta = \ell^{12} \Delta^{\ell+1}. \tag{96}$$

This follows by noting that

$$T_\ell^\times(\Delta)(E_q, \omega_{\mathrm{can}}) = \Delta(E_{q^\ell}, \ell^{-1}\omega_{\mathrm{can}}) \times \prod_{\zeta \in \mu_\ell} \Delta(E_{\zeta q^{1/\ell}}, \omega_{\mathrm{can}}) = \ell^{12}\Delta(q)^{\ell+1}.$$

Combining (95) and (96), we obtain

$$T_\ell^\times(\Sigma^\times) = \ell^{12(\ell-1)}(\Sigma^\times)^{\ell+1}.$$

It follows that

$$T_\ell(\mathrm{Log}(\Sigma^\times)) = 12(\ell-1)\log(\ell)\Sigma_0 + (\ell+1)\,\mathrm{Log}(\Sigma^\times),$$

as claimed. □

EXAMPLE 4.12. Take $N = 23$ and $p = 11$. The supersingular j-invariants mod N are $\{1, 728, 19, 0\}$, and we have $\Sigma_0 = (6, 1, 4)$ with respect to this basis. Normalize $\log : (\mathbb{Z}/N\mathbb{Z})^\times \longrightarrow \mathbb{Z}/p\mathbb{Z}$ by setting $\log(5) = 1$. Vector $\Sigma_1 = \frac{1}{12}\operatorname{Log}(\Sigma^*) = \operatorname{Log}(\frac{E_{24}}{\Delta^2}) \in \mathbb{F}_p e_{1,728} \oplus \mathbb{F}_p e_{19} \oplus \mathbb{F}_p e_0$ is then computed to be

$$\Sigma_1 = (-1, -1, -3).$$

This can readily be checked for instance by means of the identity

$$\frac{E_{24}}{\Delta^2} = (aj^2 + b(j^2 - 1{,}728\, j) + c(j - 1{,}728)^2)/d,$$

where

$$a = 49{,}679{,}091, \qquad b = 176{,}400{,}000,$$
$$c = 10{,}285{,}000, \qquad d = 236{,}364{,}091,$$

which follows by comparing the q-expansions of E_4, E_6, and E_{24}. A computation with Brandt matrices allows to verify numerically the identity of Theorem 4.11.

The description of Σ_1 given in Theorem 4.11 makes it possible to relate some of its pullbacks to modular units. More precisely, let $q \neq N$ be an auxiliary prime, let $\mathcal{E}^{(q)}$ denote the set of supersingular points of the modular curve $X_0(q)$ in characteristic N (i.e. over $\overline{\mathbb{F}_N}$), and let $\operatorname{Div}(\mathcal{E}^{(q)})$ and $\mathbb{D}^{(q)}$ denote (respectively) the space of Z- and $(\mathbb{Z}/p^t\mathbb{Z})$-linear combinations of elements of $\mathcal{E}^{(q)}$. Note that in carrying over constructions from $\mathcal{E}$ to $\mathcal{E}^{(q)}$ we must take account of the fact that the weights w_x for $x \in \mathcal{E}^{(q)}$ take into account the level structure and thus will not in general coincide with the weight $w_{\bar{x}}$ of the image $\bar{x} \in \mathcal{E}$.

The two degeneracy maps

$$\pi_1, \pi_2 : X_0(q) \longrightarrow X(1), \qquad \pi_1(A, C) = A, \qquad \pi_2(A) = A/C \tag{97}$$

induce maps $\pi_1, \pi_2 : \mathcal{E}^{(q)} \longrightarrow \mathcal{E}$ and correspondingly push-forward maps

$$\pi_{1*}, \pi_{2*} : \operatorname{Div}(\mathcal{E}^{(q)}) \longrightarrow \operatorname{Div}(\mathcal{E}).$$

The dual of these maps are pullback maps π_1^*, π_2^*, defined so as to satisfy

$$\langle \pi_j^* a, b\rangle_q = \langle a, \pi_{j*} b\rangle \quad \text{for all } a \in \operatorname{Div}(\mathcal{E}), b \in \operatorname{Div}(\mathcal{E}^{(q)}),$$

where $\langle -, -\rangle_q$ and $\langle -, -\rangle$ are the natural pairings (cf. (14)). In particular we get

$$\pi_1^*, \pi_2^* : \mathbb{D} \longrightarrow \mathbb{D}^{(q)},$$

which is, now, compatible with the corresponding pullback of functions on the ambient modular curves by means of map (89).

Just as in (89) we have a homomorphism

$$\operatorname{Log} : \mathcal{O}_{q,N}^\times \longrightarrow \operatorname{Div}(\mathcal{E}^{(q)}) \otimes (\mathbb{Z}/p^t\mathbb{Z}), \tag{98}$$

where now $\mathcal{O}_{q,N}^\times$ denotes the multiplicative group of (meromorphic) modular functions on $X_0(q)_{\mathbb{F}_N}$ regular at the supersingular points. This applies to the case where $f = \pi_1^*(\Delta)/\pi_2^*(\Delta) = \Delta(z)/\Delta(qz)$, which is a modular unit of level q.

THEOREM 4.13. *For any auxiliary prime $q \neq N$, denote by*

$$u_q := \Delta(z)/\Delta(qz) \tag{99}$$

the modular unit of level q, considered as an element of $\mathcal{O}^\times_{q,N}$ (see (98)). Then

$$\pi_1^*(\Sigma_1) - \pi_2^*(\Sigma_1) = -\frac{1}{6}\operatorname{Log}(u_q) \pmod{\Sigma_0^{(q)}},$$

where $\Sigma_0^{(q)} = \pi_1^*(\Sigma_0) = \pi_2^*(\Sigma_0)$ is an Eisenstein eigenvector on $\mathbb{D}^{(q)}$.

The use of the auxiliary prime q simplifies the situation: the map $(\pi_1^* - \pi_2^*)$ kills Σ_0; thus $(\pi_1^* - \pi_2^*)\Sigma_1$ is independent of the choice of Σ_1 and is *strictly* Eisenstein, rather than higher Eisenstein. In fact, in the case $q = 2$, this general idea appears in the work of Lecouturier; the role of the modular unit (99) is replaced in his work with the λ-invariant, see [Lec, Prop 3.25].

Proof. Equation (94) shows that $\pi_1^*(E_{N+1})/\pi_2^*(E_{N+1})$ is constant on $\mathcal{E}^{(q)}$, and hence

$$\operatorname{Log}(\pi_1^*(E_{N+1})/\pi_2^*(E_{N+1})) \sim \Sigma_0^{(q)},$$

where $\sim$ indicates that the two vectors are proportional to each other. It follows from definition (92) of $\Sigma^\times$ and $N \equiv 1$ modulo p^t that

$$\operatorname{Log}(\pi_1^*(\Sigma^\times)/\pi_2^*(\Sigma^\times)) = 2\operatorname{Log}(\Delta(qz)/\Delta(z)) \pmod{\Sigma_0^{(q)}},$$

and the claim follows from definition (93) of Σ_1. □

4.7. Tensor Products

Let M and N be any two free modules of rank one over $\mathbb{T}$. The tensor product $M \otimes_{\mathbb{T}} N$ is still free of rank one. If m_0 and m_1 (resp. n_0 and n_1) are Eisenstein and higher Eisenstein elements in M (resp. N), there seems to be no simple expression for the higher Eisenstein element in $M \otimes_{\mathbb{T}} N$ in terms of these elements. (For instance, the vector $m_0 \otimes n_0$ fails to generate the Eisenstein subspace in $M \otimes_{\mathbb{T}} N$ in general.)

Since $\mathbb{T}$ is Gorenstein, the $\mathbb{Z}_p$-dual $M^* = \operatorname{Hom}(M, \mathbb{Z}_p)$ is again a free $\mathbb{T}$-module of rank 1, and hence it makes sense to consider (higher) Eisenstein elements on it.

PROPOSITION 4.14. *If m_0^* and m_1^* (resp. n_0^* and n_1^*) are the Eisenstein and higher Eisenstein elements of M^* and N^* respectively, then*

(1) *The element $m_0^* \otimes n_0^*$ is an Eisenstein element of $(M \otimes_{\mathbb{T}} N)^*$.*
(2) *The element $m_0^* \otimes n_1^* + m_1^* \otimes n_0^*$ is the higher Eisenstein element of $(M \otimes_{\mathbb{T}} N)^*/p^t$ associated to $m_0^* \otimes n_0^*$.*

Note that there is a natural module homomorphism $M^* \otimes_{\mathbb{Z}_p} N^* \longrightarrow (M \otimes_{\mathbb{Z}_p} N)^*$ sending $m^* \otimes n^*$ to the functional defined by $(m^* \otimes n^*)(a \otimes b) = m^*(a)n^*(b)$. The meaning of the first statement is, then, that the displayed expressions in fact

belong to $(M \otimes_{\mathbb{T}} N)^* \subset (M \otimes_{\mathbb{Z}_p} N)^*$ and, moreover, are Eisenstein/higher Eisenstein considered in the former group. Similarly for the second statement (see what follows for details).

Proof. As for (1), we first check that $m_0^* \otimes n_0^*$ belongs to the submodule $(M \otimes_{\mathbb{T}} N)^*$ of $(M \otimes_{\mathbb{Z}_p} N)^*$. The kernel of the surjection $M \otimes_{\mathbb{Z}_p} N \longrightarrow M \otimes_{\mathbb{T}} N$ is generated by $(T \otimes 1 - 1 \otimes T)(M \otimes N)$ for $T \in \mathbb{T}$. Hence it suffices to verify that $(T \otimes 1 - 1 \otimes T)(m_0^* \otimes n_0^*) = 0$ for all $T \in \mathbb{T}$, and this follows because $\mathbb{T}$ is a simple algebra over $\mathbb{Z}_p$ generated by an element of I_{Eis}. Now (1) follows, as it is obvious that $m_0^* \otimes n_0^*$ is a generator of the $\mathbb{Z}_p$-module $(M \otimes_{\mathbb{T}} N)^*[I_{\mathrm{Eis}}]$.

As for (2), write $\bar{M} := M/p^t M$ and $\bar{N} := N/p^t N$. Note that $M^*/p^t \simeq \bar{M}^*$ where, on the right, $*$ denotes $\mathrm{Hom}(-, \mathbb{Z}/p^t)$. The expression $m_0^* \otimes n_1^* + m_1^* \otimes n_0^*$ lies in

$$(M^* \otimes_{\mathbb{Z}_p} N^*)/p^t = \bar{M}^* \otimes_{\mathbb{Z}/p^t} \bar{N}^*.$$

We argue as before that $m_0^* \otimes n_1^* + m_1^* \otimes n_0^*$ lies in $(\bar{M} \otimes_{\mathbb{T}} \bar{N})^*$. The $\mathbb{T}$-module structure is given by applying $T \in \mathbb{T}$ to either the first or second argument. Applying $T_\ell - \ell - 1$ to the first argument gives

$$\begin{aligned}
&(T_\ell - \ell - 1)[m_0^* \otimes n_1^* + m_1^* \otimes n_0^*] \\
&\quad = (T_\ell - \ell - 1)m_0^* \otimes n_1^* + (T_\ell - \ell - 1)m_1^* \otimes n_0^* \\
&\quad = (\ell - 1)\log(\ell) m_0^* \otimes n_0^*,
\end{aligned}$$

as desired. □

5. Proof of the Main Theorem

This section proves Conjecture 1.1 for dihedral modular forms.

5.1. *Elliptic Units*

We put ourselves in the situation of Sections 2.1 and 2.2 with $\psi_2 = \psi_1^{-1}$ and $\psi_2 \neq \psi_1$. In particular: K is an imaginary quadratic field of odd discriminant $D < 0$ and a ring of integers $\mathfrak{o}$; the level N is prime, $p > 3$ is a prime dividing $N - 1$, and $\psi_1 : \mathcal{C} \longrightarrow L^\times$ is a class group character into some cyclotomic field L. Let R be the ring of integers of L.

Finally, put

$$\psi = \psi_1/\psi_1' = \psi_1^2 : \mathcal{C} \to L^\times. \tag{100}$$

When N splits in K, Conjecture 1.1 reduces to the equality $0 = 0$, as explained in Section 1.3 of the Introduction. Hence it shall be assumed throughout that N is inert in K.

Let $\mathbb{F}_{N^2}$ be the quotient $\mathfrak{o}/N$, a finite field of size N^2, and fix an algebraic closure $\overline{\mathbb{F}}_N$ of $\mathbb{F}_{N^2}$.

In the current section only ψ will be relevant (and the discussion would be valid for an arbitrary character ψ, not just one of the form (100)). We will construct an elliptic unit u_ψ associated to ψ and explain how its discrete logarithm at

various primes is related to the geometry of supersingular points. We will use the setup of Section 2.1 regarding double coset spaces attached to definite quaternion algebras, but will now use the incarnation of these spaces in terms of supersingular elliptic curves.

More precisely, global class field theory identifies $\mathcal{C}$ with the Galois group of an abelian extension H of K: the Hilbert class field of K, generated over K by the j-invariants of elliptic curves over $\bar{K}$ with endomorphism ring equal to $\mathfrak{o}$. The set of all such elliptic curves up to $\bar{K}$-isomorphism, denoted by $\mathcal{E}_{\mathfrak{o}}$, is a principal transitive $\mathcal{C}$-set and the choice of a base point $A \in \mathcal{E}_{\mathfrak{o}}$ identifies the two sets

$$\mathfrak{a} \in \mathcal{C} \mapsto A_{\mathfrak{a}} \in \mathcal{E}_{\mathfrak{o}}$$

via tensoring with the inverse of $\mathfrak{a}$.

The prime N, which is inert in $K/\mathbb{Q}$, splits completely in H/K, and the choice of a prime $\mathfrak{N}$ of H above N determines the reduction maps

$$\iota : \mathcal{E}_{\mathfrak{o}} \longrightarrow \mathcal{E}, \qquad \iota : \mathrm{Pic}(\mathfrak{o}) \longrightarrow \mathcal{E},$$

where $\mathcal{E}$ is the set of isomorphism classes of supersingular curves over $\overline{\mathbb{F}}_N$. Since the end result we are proving is independent of the choice of $\mathfrak{N}$, we can and will choose $\mathfrak{N}$ in such a way that the reduction $\iota(A) \in \mathcal{E}$ matches one of the basepoints for $\mathcal{E}$ chosen before (13), that is, to reprise, the endomorphism ring of the reduction of A at $\mathfrak{N}$ should contain an order of the form $\mathfrak{o} \oplus \mathfrak{o}\, j$.

The map ι coincides with the map (13) after identifying $\mathcal{E}$ with maximal orders in the associated quaternion algebras, as specified prior to (13). As in (17), the image of ψ under the pushforward map $\iota_* : R[\mathrm{Pic}(\mathfrak{o})] \longrightarrow \mathrm{Div}(\mathcal{E}) \otimes R$ is denoted by $[\psi] := \iota_*(\psi) \in \mathrm{Div}(\mathcal{E}) \otimes R$.

Let q be an auxiliary rational prime which does not divide DN. A *Heegner point* on $X_0(q)(\bar{K})$ attached to $\mathfrak{o}$ is a pair (A, C) where A is an elliptic curve over $\bar{K}$ equipped with a cyclic subgroup $C \subset A$ of order q, for which both A and A/C belong to $\mathcal{E}_{\mathfrak{o}}$. The set $\mathcal{E}_{\mathfrak{o}}^{(q)}$ of Heegner points on $X_0(q)(\bar{K})$ is nonempty precisely when the prime $q \nmid D$ is split in $K/\mathbb{Q}$, that is, when $q = \mathfrak{q}\bar{\mathfrak{q}}$. It is then contained in $X_0(q)(H)$. Just as before, the choice of a prime $\mathfrak{N}$ of $\mathcal{O}_H$ induces reduction maps $\mathcal{E}_{\mathfrak{o}}^{(q)} \to \mathcal{E}^{(q)}$.

The set $\mathcal{E}_{\mathfrak{o}}^{(q)}$ is equipped with the two degeneracy maps

$$\pi_1, \pi_2 : \mathcal{E}_{\mathfrak{o}}^{(q)} \longrightarrow \mathcal{E}_{\mathfrak{o}}; \qquad \pi_1(A, C) = A, \qquad \pi_2(A, C) = A/C,$$

obtained by restricting the corresponding degeneracy maps $X_0(q) \to X(1)$. The choice of a prime divisor $\mathfrak{q}$ of q determines a section $\eta_{\mathfrak{q}} : \mathcal{E}_{\mathfrak{o}} \longrightarrow \mathcal{E}_{\mathfrak{o}}^{(q)}$ of π_1 by setting

$$\eta_{\mathfrak{q}}(A) = \tilde{A} := (A, A[\mathfrak{q}]).$$

Observe that the action of $\mathrm{Pic}(\mathfrak{o})$ on $\mathcal{E}_{\mathfrak{o}}$ satisfies

$$A_{\mathfrak{a}\mathfrak{q}} = \pi_2(\eta_{\mathfrak{q}}(A_{\mathfrak{a}})). \tag{101}$$

DEFINITION 5.1. The *elliptic unit* attached to ψ and $\mathfrak{q}$ is the element

$$u_{\psi,q} = \sum_{\mathfrak{a}\in \mathrm{Pic}(\mathfrak{o})} u_q(\eta_{\mathfrak{q}}(A_{\mathfrak{a}})) \otimes \psi(\mathfrak{a}) \in H^\times \otimes R, \tag{102}$$

with u_q the modular unit defined in (99).

If ψ is nontrivial, then $u_{\psi,q}$ belongs to $\mathcal{O}_H^\times \otimes R$ and more precisely to its ψ-isotypical component; that is to say:

$$g \cdot u_{\psi,q} = \psi^{-1}(g) u_{\psi,q} \quad \text{for all } g \in \mathrm{Gal}(H/K). \tag{103}$$

(Cf. [KL81, §11, Thms. 1.1. and 1.2].) Note that on the left-hand side of (103), g acts on H in the natural way. On the right-hand side, ψ is understood as a character of $\mathrm{Gal}(H/K)$ through the isomorphism $\mathrm{Gal}(H/K) \simeq \mathcal{C}$ through which this Galois group acts on $\mathcal{E}_{\mathfrak{o}}$, and $\psi^{-1}(g) \in R^\times$ acts by multiplication on the second factor in the tensor product $\mathcal{O}_H^\times \otimes R$. If $\psi = 1$ then $u_{\psi,q}$ may fail to be a unit at the primes above q, but this case will not arise.

The following proposition plays a key role in the proof of Conjecture 1.1 for CM forms described in the next section, since it is via this result that the relevant Stark unit makes its appearance.

PROPOSITION 5.2. *For all characters $\psi : \mathcal{C} \to R^\times$ and all split primes $q = \mathfrak{q}\bar{\mathfrak{q}}$ as given previously, we have an equality in R/p^t:*

$$(1 - \psi(\bar{\mathfrak{q}})) \times \langle \Sigma_1, [\psi] \rangle = -\frac{1}{6} \log(u_{\psi,\mathfrak{q}}),$$

where $\Sigma_1 \in \mathrm{Div}(\mathcal{E}) \otimes \mathbb{Z}/p^t\mathbb{Z}$ is the higher Eisenstein element of Theorem 4.11, and we wrote $\log : \mathcal{O}_H^\times \otimes R \longrightarrow R/p^t$ for the composition of the reduction map $\mathcal{O}_H^\times \to (\mathcal{O}_H/\mathfrak{N})^\times \simeq \mathbb{F}_{N^2}^\times$ with discrete logarithm fixed at the outset.[5]

Proof. Recall that A is a fixed basepoint for $\mathcal{E}_{\mathfrak{o}}$ and $[\psi] = \sum_{I\in\mathcal{C}} \psi(I) A_I$. We may write

$$\begin{aligned}(1 - \psi(\bar{\mathfrak{q}}))\langle \Sigma_1, [\psi] \rangle &= \sum_{I\in \mathrm{Pic}(\mathfrak{o})} (\psi(I) - \psi(I\bar{\mathfrak{q}}))\langle \Sigma_1, A_I \rangle \\ &= \sum_{I\in \mathrm{Pic}(\mathfrak{o})} \psi(I)\langle \Sigma_1, A_I - A_{I\mathfrak{q}} \rangle.\end{aligned}$$

Letting $\tilde{A}_I := \eta_{\mathfrak{q}}(A_I)$, we have, by (101),

$$A_I - A_{I\mathfrak{q}} = (\pi_1 - \pi_2)_*(\tilde{A}_I),$$

and hence, by invoking Theorem 4.13,

$$(1 - \psi(\bar{\mathfrak{q}}))\langle \Sigma_1, [\psi] \rangle = \sum_{I\in \mathrm{Pic}(\mathfrak{o})} \psi(I)\langle (\pi_1^* - \pi_2^*)\Sigma_1, \tilde{A}_I \rangle$$

[5] This discrete logarithm was defined on $(\mathbb{Z}/N\mathbb{Z})^\times$ but uniquely extends to $\mathbb{F}_{N^2}^\times$.

$$= -\frac{1}{6} \cdot \sum_{I \in \mathrm{Pic}(\mathfrak{o})} \psi(I) \langle \mathrm{Log}(u_q), \tilde{A}_I \rangle$$

with the pairings the natural ones on $\mathrm{Div}(\mathcal{E}^{(q)})$. The latter expression is equal to $-\frac{1}{6}\langle \mathrm{Log}(u_q), [\psi] \rangle = -\frac{1}{6}\log(u_{\psi,\mathfrak{q}})$, the equality taking place in R/p^t:

$$\begin{aligned} \langle \mathrm{Log}(u_q), [\psi] \rangle &\overset{(98)}{=} \sum_{I \in \mathcal{C}} \log u_q(\iota \circ \eta_{\mathfrak{q}}(A_I)) \psi(I) \\ &= \log\left(\sum_{I \in \mathcal{C}} u_q(\iota \circ \eta_{\mathfrak{q}}(A_I)) \otimes \psi(I) \right) \\ &= \log \mathrm{red}_{\mathfrak{N}} \sum_{I \in \mathcal{C}} u_q(\eta_{\mathfrak{q}}(A_I)) \otimes \psi(I) = \log(u_{\psi,\mathfrak{q}}). \end{aligned}$$

□

REMARK 5.3. One can replace the algebra $M_2(\mathbb{Q})$ with a nonsplit, indefinite quaternion algebra D_M over $\mathbb{Q}$, of discriminant $M > 1$ say, which is associated to a Shimura curve X_M arising from a co-compact subgroup of $\mathrm{SL}_2(\mathbb{R})$. Given a prime $N \nmid M$, the module $\mathcal{E}_{M,N}$ of supersingular points of X_M in characteristic N is identified with the space of functions on a finite double coset space attached to the definite quaternion algebra D_{MN} of discriminant MN. If ψ is a character of the class group of a quadratic imaginary field K in which all the primes dividing MN are inert, one can define an associated vector $[\psi] \in \mathcal{X}_{M,N}$ much as in the case where $M = 1$. The space $\mathcal{X}_{M,N}$ contains an Eisenstein eigenvector Σ_0, whose value on a double coset is equal to the cardinality of its stabilizer subgroup. Theorems 1.2 and 1.3 of [Yoo] show that the Hecke algebra $\mathbb{T}_{MN}$ acting on $\mathcal{X}_{M,N}$ is equipped with an Eisenstein homomorphism $\tilde{\varphi}_{\mathrm{Eis}}$ as in (80) with $\mathbb{T}$ replaced with $\mathbb{T}_{MN}$, and suggest that, if $p > 3$ is a prime with $p^t || N - 1$, then the module $\mathcal{X}_{M,N} \otimes (\mathbb{Z}/p^t\mathbb{Z})$ contains a generalized Eisenstein eigenvector Σ_1 attached to a choice of discrete logarithm $\log : \mathbb{F}_N^\times \longrightarrow \mathbb{Z}/p^t\mathbb{Z}$, satisfying

$$(T_\ell - (\ell + 1))\Sigma_1 = (\ell - 1)\log(\ell)\Sigma_0.$$

Does such Σ_1, when it exists, satisfy an analogue of Proposition 5.2 relating $\langle \Sigma_1, [\psi] \rangle$ to the discrete logarithm of the elliptic unit u_ψ, which does not depend on N? Such a relationship would be intriguing in light of the fact that the arithmetic subgroup of $\mathrm{SL}_2(\mathbb{R})$ defining X_M has no parabolic elements and hence there are no modular units on X_M that could be parlayed into a direct construction of Σ_1.

5.2. *Proof of Conjecture 1.1 for Definite Theta Series*

We now restrict to the case D prime; however, as we comment in the statements, the proofs verbatim give results for D odd under further restrictions on N.

We let $g = \theta_{\psi_1}$ be the associated θ series. It is a cusp form by virtue of the assumption that $\psi_1 \neq \psi_1^{-1}$. The Galois representation ρ_g is the induction to $G_{\mathbb{Q}}$ of the finite order character ψ_1. Let

$$G \in M_2(\Gamma_0(N)) = \mathrm{Tr}_N^{ND} g(z) g^*(Nz)$$

denote the modular form defined as the trace to the space of modular forms of weight 2 and level N of the product $g(z)g^*(Nz) = \theta_{\psi_1}(z)\theta_{\psi_1^{-1}}(Nz)$.

Recall from (15) the Θ-correspondence

$$\Theta : \mathrm{Div}(\mathcal{E}) \otimes_{\mathbb{T}(N)} \mathrm{Div}(\mathcal{E}) \to M_2(\Gamma_0(N)).$$

In particular, this induces a map on localizations at the Eisenstein ideal $\mathfrak{m}$, and it follows from [Eme02, Theorem 0.5] that the resulting map is an isomorphism of free $\mathbb{T} = \mathbb{T}(N)_{\mathfrak{m}}$-modules of rank one. Write

$$\overline{\mathbb{T}} = \mathbb{T}/p^t, \qquad \bar{\mathbb{D}} = \mathrm{Div}(\mathcal{E})_{\mathfrak{m}}/p^t, \qquad \bar{\mathbb{M}} = M_2(\Gamma_0(N)_{\mathfrak{m}}/p^t,$$
$$\bar{\mathbb{S}} = S_2(\Gamma_0(N))_{\mathfrak{m}}/p^t.$$

Then, reducing Θ modulo p^t, we obtain an isomorphism

$$\Theta : \bar{\mathbb{D}} \otimes_{\overline{\mathbb{T}}} \bar{\mathbb{D}} \simeq \bar{\mathbb{M}} \tag{104}$$

with associated adjoint

$$\Theta^* : \bar{\mathbb{M}}^* \simeq (\bar{\mathbb{D}} \otimes_{\overline{\mathbb{T}}} \bar{\mathbb{D}})^*. \tag{105}$$

Here $*$ denotes $\mathrm{Hom}(-, \mathbb{Z}/p^t)$.

The strategy of the proof of Conjecture 1.1, as outlined in Section 1.4, is to express the inner product $\langle G, \mathfrak{S}\rangle$ as an inner product on $\bar{\mathbb{D}} \otimes \bar{\mathbb{D}}$ via Θ. It follows from Theorem 2.2 that

$$\langle G, \mathfrak{S}\rangle = 4 \cdot \langle \Theta([1] \otimes [\psi]), \mathfrak{S}\rangle = 4\langle [1] \otimes [\psi], \Theta^*(\mathfrak{S})\rangle. \tag{106}$$

Here we regard the equality as occurring inside R/p^t, and we regard $\mathfrak{S} \in \bar{\mathbb{M}}^*$ and $[1] \otimes [\psi] \in \bar{\mathbb{D}} \otimes_{\overline{\mathbb{T}}} \bar{\mathbb{D}}$. We now need the following:

THEOREM 5.4. *Let $\mathfrak{S}_0$ and $\mathfrak{S}_1 \in \bar{\mathbb{M}}^*$ denote the Eisenstein and higher classes described in Section 4.5, and let Σ_0 and Σ_1 denote the analogous classes in $\bar{\mathbb{D}}$ described in Section 4.6. Then*

(1) $\Theta^*(\mathfrak{S}_0) = \frac{1}{2}\Sigma_0 \otimes \Sigma_0$;
(2) $\Theta^*(\mathfrak{S}_1) \equiv \frac{1}{2}(\Sigma_1 \otimes \Sigma_0 + \Sigma_0 \otimes \Sigma_1)$ *modulo* $\Sigma_0 \otimes \Sigma_0$.

Here we used the pairing $\langle , \rangle$ given in (14) to identify $\bar{\mathbb{D}} \simeq (\bar{\mathbb{D}})^*$; we also used the inclusion $(\bar{\mathbb{D}} \otimes_{\overline{\mathbb{T}}} \bar{\mathbb{D}})^* \subset (\bar{\mathbb{D}}^* \otimes_{\mathbb{Z}/p^t} \bar{\mathbb{D}}^*)$ to describe elements of the left-hand group, just as was done in Proposition 5.2.

Proof. The first part of the theorem follows directly from the definition of Θ given in (15). The second follows from the Hecke equivariance of Θ^*, in light of the fact that $\Sigma_1 \otimes \Sigma_0 + \Sigma_1 \otimes \Sigma_0$ is the higher Eisenstein element in $(\bar{\mathbb{D}} \otimes_{\mathbb{T}} \bar{\mathbb{D}})^*$ attached to $\Sigma_0 \otimes \Sigma_0$, by Proposition 4.14. □

We now choose an auxiliary prime ideal $\mathfrak{q}$ so that $\psi(\mathfrak{q})$ is a primitive root of unity of order equal to the order of ψ.

PROPOSITION 5.5. *There is an equality inside* R/p^t

$$(1-\psi(\bar{\mathfrak{q}}))\langle G,\mathfrak{S}\rangle = \frac{-h(\mathfrak{o})}{3}\log(u_{\psi,\mathfrak{q}}), \tag{107}$$

where $u_{\psi,\mathfrak{q}}$ *is the elliptic unit defined in* (5.1), *and* $h(\mathfrak{o})$ *is the order of the class group* $\mathcal{C}$.

Note that, for D odd but not assumed prime, the same conclusion holds true with the following caveats: we suppose not merely that N is inert in $\mathbb{Q}(\sqrt{-D})$, but that $-N$ is a square modulo D; and, owing to the denominators potentially introduced in Section 2.6, it is only valid for p sufficiently large in the sense of Theorem 2.2.

Proof. By (106) and part (2) of Theorem 5.4,

$$\langle G,\mathfrak{S}\rangle = 2\langle [1]\otimes[\psi],\,\Sigma_0\otimes\Sigma_1+\Sigma_1\otimes\Sigma_0\rangle = 2\langle\Sigma_0,[1]\rangle\langle\Sigma_1,[\psi]\rangle,$$

where we have used the fact that $\langle\Sigma_0,[\psi]\rangle = 0$ since ψ is nontrivial. Since $\langle\Sigma_0,[1]\rangle = h(\mathfrak{o})$ by definition, the theorem now follows from Proposition 5.2. □

To prove Theorem 1.2 of the Introduction for CM weight one forms, it remains to relate the right-hand side of (107) to the expression $\mathrm{red}_N(u_g)$ occurring in this theorem; this is done by the following lemma.

LEMMA 5.6. *Let* $U_g := (\mathcal{O}_H^\times\otimes \mathrm{Ad}^*(\rho_g)^\circ)^{G_\mathbb{Q}}$. *There exists* $u_g\in U_g$ *with the property that, for all* N *as before*,

$$\log(\mathrm{red}_N(u_g)) = 2\log(u_{\psi,\mathfrak{q}}).$$

This lemma concludes the proof of Theorem 1.2 after multiplying equality (107) by $\frac{-6n}{1-\psi(\bar{\mathfrak{q}})}\in R$ with n the norm of $1-\psi(\bar{\mathfrak{q}})$:

$$(-6n)\langle G,\mathfrak{S}\rangle = \log(u'_g), \qquad u'_g := \frac{-h(\mathfrak{o})n}{(1-\psi(\mathfrak{q}))}\cdot u_g,$$

where, in the last equality, we are implicitly using the R-module structure on U_g to form the product.

Proof. For typographical simplicity, we write just u_ψ instead of $u_{\psi,\mathfrak{q}}$.

Let e_1 be an eigenvector in V_g for the action of G_K, on which G_K acts via the character ψ_1. Since N is inert in K, the associated Frobenius automorphism $\sigma_N\in G_\mathbb{Q}$ sends e_1 to a complementary vector $e_2=\sigma_N(e_1)$, on which G_K acts via the character ψ_1'. Since σ_N has determinant -1, it then sends e_2 to e_1. Representing the elements of $\mathrm{Ad}(V_g)$ as matrices relative to the basis (e_1,e_2), so that

$$\rho_g(x) = \begin{pmatrix}\psi_1(x) & 0\\ 0 & \psi_1(x)^{-1}\end{pmatrix} \quad \text{for } x\in G_K \quad \text{and} \quad \rho_g(\sigma_N) = \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix},$$

and using the trace form to identify $\mathrm{Ad}(V_g)$ with its dual $\mathrm{Ad}^*(V_g)$, we define $u_g\in U_g$ via

$$u_g := u_\psi\otimes\begin{pmatrix}0 & 1\\ 0 & 0\end{pmatrix} + \sigma_N(u_\psi)\otimes\begin{pmatrix}0 & 0\\ 1 & 0\end{pmatrix}. \tag{108}$$

Note that the matrices do indeed define functionals on $\mathrm{Ad}(V_g)$ that send the image of $R[G_{\mathbb{Q}}]$ to R. We readily see that u_g is in fact $G_{\mathbb{Q}}$-invariant, for example, $\rho_g(G_K)$ acts on the u_ψ through ψ^{-1} and on the upper nilpotent matrix through $\psi = \psi_1^2$. We then compute an equality inside $\mathcal{O}_H^\times \otimes R$:

$$\mathrm{red}_N(u_g) = \langle u_g, \rho_g(\sigma_N)\rangle = \mathrm{Trace}\begin{pmatrix} u_\psi & 0 \\ 0 & \sigma_N(u_\psi)\end{pmatrix} = u_\psi + \sigma_N(u_\psi).$$

(The reader is cautioned that additive notation for the group law in $\mathcal{O}_H^\times \otimes R/p^t$ has been used in this last equation.) Since the discrete logarithm mod N is equivariant for the action of σ_N, which acts trivially on $(\mathbb{Z}/N\mathbb{Z})^\times$, we obtain the desired equality

$$\log(\mathrm{red}_N(u_g)) = \log(u_\psi + \sigma_N u_\psi) = 2\log(u_\psi).$$

□

5.3. *Proof of Conjecture 1.1 for Indefinite Theta Series*

We now turn to proving Conjecture 1.1 when g is an RM form. We will be in the situation of Section 3 with $\psi_2 = \psi_1^{-1}$. More precisely, let $\psi_1 : G_K \longrightarrow R^\times$ be the finite order character of mixed signature as in the beginning of Section 3, with values in the ring of integers of a finite extension L of $\mathbb{Q}$, such that $g = \theta_{\psi_1}$ is the theta series associated to ψ_1 as described in (22). Let N be an odd prime, and define $G \in S_2(\Gamma_0(N))$ as the trace to the space of modular forms of level N of $\theta_{\psi_1}(z)\theta_{\psi_1^{-1}}(Nz)$. As explained in the Introduction, *the conjecture we address in this note becomes trivial when N remains inert, and hence we assume throughout that it splits in K as $N = \mathfrak{N}\cdot\bar{\mathfrak{N}}$.*

The proof of Conjecture 1.1, which computes the pairing of G with the Shimura class, again relies crucially on the Θ-correspondence, namely the Hecke-equivariant map

$$\Theta : H_{1,\mathrm{B}}(X_0(N), \mathrm{cusps}; Z)^+ \otimes_{\mathbb{T}(N)} H_{1,\mathrm{B}}(Y_0(N), Z)^- \to M_2(N)$$

given by

$$\Theta(\gamma^+ \otimes \gamma^-) = \frac{-1}{24}\kappa_0^+(\gamma^+)\cdot\kappa_0^-(\gamma^-) + \sum_{m\geq 1}\langle T_m\gamma^+, \gamma^-\rangle q^m. \tag{109}$$

Here $\kappa_0^\pm$ are as defined in Sections 4.3 and 4.4. Note that the sign of $\frac{-1}{24}$ depends on orientation conventions implicit in the definition of the intersection pairing.

For the lack of a suitable reference, we sketch a proof. We identify the relative homology group $H_{1,\mathrm{B}}(X_0(N), \mathrm{cusps}; Z)^+$ with $H^1_{\mathrm{B}}(Y_0(N), Z)^-$, a free $\mathbb{T}(N)$-module of rank one, and thus with $\mathbb{T}(N)$ itself. We can similarly identify $H_{1,\mathrm{B}}(Y_0(N), Z)^-$ with its dual $M_2(N; Z)$. Adjusting these identifications if necessary, we can suppose that the Poincaré pairing $\langle -, -\rangle$ corresponds to the pairing on $\mathbb{T}(N) \times M_2(N; Z)$ given by $(T, f) \mapsto a_1(Tf)$, and Θ corresponds to $(T, f) \mapsto Tf$. Formula (109) follows from this up to the identification of the constant $\frac{-1}{24}$. To compute the constant, we take γ^+ the element represented by the

geodesic from 0 to ∞, and γ^- a small loop around ∞, and we fix orientations so that $\langle \gamma^+, \gamma^- \rangle = 1$. In particular,

$$\langle T_m \gamma^+, \gamma^- \rangle = \sum_{d|m,(d,N)=1} d, \qquad \kappa_0^+(\gamma^+) = 1, \qquad \kappa_0^-(\gamma^-) = N - 1.$$

The expansion on the right-hand side of (109) must represent $E_2^{(N)}$, and therefore this fixes the constant as $\frac{-1}{24}$.

We note in particular that κ_0^+ vanishes on the image of $H_{1,\mathrm{B}}(X_0(N))$, and so the formula above in fact matches with (45) used in an earlier section.

As in the CM setting, we can observe that—with $\mathfrak{m}$ the Eisenstein ideal as before—

- the modules $\mathbb{H}_+ := H_{1,\mathrm{B}}(X_0(N), \text{cusps}; \mathbb{Z})^+_{\mathfrak{m}}$ and $\mathbb{H}_- = H_{1,\mathrm{B}}(Y_0(N), \mathbb{Z})^-_{\mathfrak{m}}$, obtained from completing the singular homology of the complex modular curves, are again free $\mathbb{T}$-modules of rank 1.[6]
- the map $\Theta_{\mathfrak{m}}$ is an isomorphism: $(\mathbb{H}_+ \otimes_{\mathbb{T}} \mathbb{H}_-) \longrightarrow \mathbb{M}$, and so (cf. (104), (105)) we have adjoint maps

$$\Theta : \bar{\mathbb{H}}_+ \otimes_{\bar{\mathbb{T}}} \bar{\mathbb{H}}_- \simeq \bar{\mathbb{M}}, \qquad \Theta^* : \bar{\mathbb{M}}^* \simeq (\bar{\mathbb{H}}_+ \otimes_{\bar{\mathbb{T}}} \bar{\mathbb{H}}_-)^*. \tag{110}$$

Here bars denote tensoring with $\mathbb{Z}/p^t$ and $*$ denotes $\mathrm{Hom}(-, \mathbb{Z}/p^t)$.

The strategy of the proof of Conjecture 1.1 is, much as in the case of CM theta series, to express the inner product $\langle G, \mathfrak{S} \rangle$ as an inner product on $\mathbb{H}_+ \otimes_{\mathbb{T}} \mathbb{H}_-$ via Θ.

We will follow the notation of Section 3.2; in particular $\mathcal{C}$ is the narrow class group of K, and we have introduced Heegner cycles γ_I attached to $I \in \mathcal{C}$ as well as weighted combinations γ_ψ in (46). The following proposition plays a key role in the proof of Conjecture 1.1 for RM forms, since it is via this result that the relevant Stark unit—in this case, a fundamental unit of the real quadratic field—makes its appearance.

PROPOSITION 5.7. *For all even characters ψ of the narrow Picard group $\mathcal{C}$,*

$$\kappa_0^+(\gamma_\psi) = 0 \quad \textit{and} \quad \kappa_1^+(\gamma_\psi) = \begin{cases} -h \log(u_K) & \textit{if } \psi = 1, \\ 0 & \textit{if } \psi \neq 1, \end{cases}$$

where κ_0^+ and $\kappa_1^+ \in H^1_{\mathrm{B}}(X_0(N), \text{cusps}; \mathbb{Z})^+$ are the Eisenstein and higher Eisenstein elements described in Section 4.3, h is the order of the narrow class group $\mathcal{C}$, and $\log(u_K)$ refers to the logarithm of the reduction of u_K at the chosen divisor $\mathfrak{N}$ of N.[7]

[6] Note that we get, by duality, an isomorphism of these with the (sign-altered) cohomological analogues: $\mathbb{H}_+ \simeq \mathbb{H}^-$ and $\mathbb{H}_- \simeq \mathbb{H}^+$, so this result follows from its cohomological analogue.

[7] The definition of γ_ψ also depends on the choice of divisor of N, although this is not indicated in the notation. One checks that the identity remains valid upon replacing $\mathfrak{N}$ with $\mathfrak{N}'$ on both sides.

Proof. The assertion about κ_0^+ follows from the fact that the Heegner cycles γ_I, viewed as cycles in the integral homology of $X_0(N)$ relative to the cusps, are in the kernel of the boundary map ∂ of (83) and hence are orthogonal to κ_0.

To show the second assertion, recall that the class κ_1^+ was defined modulo p^t by choosing a discrete logarithm $\log : (\mathbb{Z}/N\mathbb{Z})^\times \longrightarrow \mathbb{Z}/p^t\mathbb{Z}$ and setting

$$\kappa_1^+ \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \log(a).$$

With this choice we have

$$\kappa_1^+(\gamma_I) = -\log(u_K), \tag{111}$$

where u_K is a fundamental unit of norm 1 of the real quadratic field K, $\log(u_K)$ refers to the logarithm of the reduction of u_K at $\mathfrak{N}$. This is because (notation of Section 3.2) the cycle γ_I arises from an embedding $\mathfrak{o} \to M_0(N)$ with respect to which the ring homomorphism sending a matrix in $M_0(N)$ to the mod N reduction of upper left-hand entry restricts to reduction modulo $\mathfrak{N}$ on $\mathfrak{o}$ (see the discussion before (43)); the sign arises for the orientation reason noted after (44). Equation (111) therefore implies that $\kappa_1^+(\gamma_\psi) = -(\sum_{\mathfrak{a}} \psi(\mathfrak{a})) \log(u_K)$, and the result follows. □

PROPOSITION 5.8. *For all totally odd ring class characters ψ,*

$$\kappa_0^-(\gamma_\psi) = (1 - \psi(\mathfrak{N}))L_{\mathrm{alg}}(\psi),$$

where $\kappa_0^- \in H^1_{\mathrm{B}}(Y_0(N), \mathbb{Z})^-$ is as defined in Section 4.4, and $L_{\mathrm{alg}}(\psi) \in R$ will be defined in (112) and is in particular independent of $\mathfrak{N}$.

Recall that κ_0^- arises from the Dedekind–Rademacher function φ of (85) which encodes the periods of the (complex!) logarithm of the modular unit $\Delta(Nz)/\Delta(z)$. The proposition shows that $\kappa_0^-(\gamma_\psi)$ exhibits a mild dependence on N through the factor $(1 - \psi(\mathfrak{N}))$.

Proof. The issue to be dealt with here is, essentially, passage from level 1 to level N. Let $I \in \mathcal{C}$. Choose a representative that is relatively prime to N and an oriented basis (e_1, e_2). The element

$$\eta_I = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \quad \text{where} \quad \begin{matrix} u_K e_1 = a e_1 + c e_2, \\ u_K e_2 = b e_1 + d e_2, \end{matrix}$$

has conjugacy class in $\mathrm{SL}_2(\mathbb{Z})$ that does not depend on the choice of oriented basis, and in particular $\varphi(\eta_{\mathfrak{a}})$ is well defined. Choose (e_1, e_2) so that e_2 belongs to $I \cap \mathfrak{N}$, and observe then that $(e_1', e_2') := (Ne_1, e_2)$ is an oriented basis for $I\mathfrak{N}$ and that u_K acts on this basis according to the rule $u_K e_1' = a e_1' + (cN) e_2'$ and $u_k e_2' = (b/N) e_1' + d e_2'$. By (84) as well as definition (42) of cycles γ_J, we get $\kappa_0^-(\gamma_{I\mathfrak{N}}) = \varphi(\eta_{I\mathfrak{N}}) - \varphi(\eta_I)$, and it follows that

$$\begin{aligned} \kappa_0^-(\gamma_\psi) &= \sum \psi(I\mathfrak{N})(\varphi(\eta_{I\mathfrak{N}}) - \varphi(\eta_I)) \\ &= (1 - \psi(\mathfrak{N})) \sum_I \psi(I)\varphi(\eta_I), \end{aligned}$$

and we obtain the result upon defining

$$L_{\mathrm{alg}}(\psi) := \sum_I \psi(I)^{-1}\varphi(\eta_I). \tag{112}$$

□

REMARK 5.9. As is implicit in the notation, $L_{\mathrm{alg}}(\psi)$ is closely related to the "algebraic part" of the L-series $L(\psi, s) = \sum_{\mathfrak{a}\lhd\mathfrak{o}_K} \psi(\mathfrak{a})(N\mathfrak{a})^{-s}$ attached to ψ at $s = 1$. The justification for this is given by Meyer's analogue of the Kronecker limit formula for real quadratic fields (cf. [Zag75, §4]) which asserts that, at least for all unramified, totally odd characters ψ of the narrow Hilbert class field of K, $L_{\mathrm{alg}}(\psi) = \frac{12\sqrt{D}}{\pi^2} L(\psi^{-1}, 1)$.

Note that if $x^2 - a_N(g) + \chi_K(N) = (x - \alpha_N)(x - \beta_N)$ is the Nth Hecke polynomial attached to g, then we may order α_N and β_N in such a way that

$$\alpha_N = \psi_1(\mathfrak{N}), \qquad \beta_N = \psi_1(\mathfrak{N}') \quad \text{and so} \quad \psi(\mathfrak{N}) = \psi_1(\mathfrak{N})/\psi_1'(\mathfrak{N}) = \alpha_N/\beta_N,$$

where we use definition (9). Proposition 5.8 can then be rewritten as

$$\kappa_0^-(\gamma_\psi) = (1 - \alpha_N/\beta_N) \times L_{\mathrm{alg}}(\psi). \tag{113}$$

Let $\mathfrak{S}_0$ and $\mathfrak{S} = \mathfrak{S}_1 \in \bar{\mathbb{M}}^*$ denote the Eisenstein and higher classes described in Section 4.5. It follows from Theorem 3.1 applied to the pair (ψ_1, ψ_1^{-1})—so by (41) $\psi_{12} = 1$ and $\psi_{12'} = \psi_1/\psi_1' = \psi$—that there exists $C_g \in R$ independent of N such that

$$\begin{aligned}\langle G, \mathfrak{S}\rangle &= \beta_N C_g \langle \Theta([\gamma_1] \otimes [\gamma_\psi]), \mathfrak{S}\rangle \\ &= \beta_N C_g \cdot \langle [\gamma_1] \otimes [\gamma_\psi], \Theta^*(\mathfrak{S})\rangle,\end{aligned} \tag{114}$$

where we understand $[\gamma_1] \otimes [\gamma_\psi]$ as an element of $(\bar{\mathbb{H}}_+ \otimes_{\bar{\mathbb{T}}} \bar{\mathbb{H}}_-)$ and $\Theta^*(\mathfrak{S})$ as an element of the $\mathbb{Z}/p^t$-dual, see (110). Here we regard Θ as normalized as in (109); the C_g that appears in the equation only agrees with that constant appearing in Theorem 3.1 up to sign, arising from the fact that the choice of orientation convention for (109) was not compared with the choice of orientation convention used in Theorem 3.1. This sign may be computed by the enthusiastic reader.

The next theorem, which determines the image of $\mathfrak{S}$ under Θ^*, plays exactly the same role in the RM proof as Theorem 5.4 in the CM setting.

THEOREM 5.10. *We have*

(1) $\Theta^*(\mathfrak{S}_0) = \frac{-1}{24}\kappa_0^+ \otimes \kappa_0^-$;

(2) $\Theta^*(\mathfrak{S}) \equiv \frac{-1}{24}(\kappa_1^+ \otimes \kappa_0^- + \kappa_0^+ \otimes \kappa_1^-)$ *modulo* $\kappa_0^+ \otimes \kappa_0^-$,

where κ^+ *are the Eisenstein classes of Section 4.3, or rather their image in* $(\mathbb{H}_+)^*$ *or* $(\overline{\mathbb{H}}_+)^*$, *and similarly* κ^- *are similarly defined from the Eisenstein classes of Section 4.4.*

The statements should be interpreted just as in Theorem 5.4: we use

$$(\overline{\mathbb{H}}_+ \otimes_{\overline{\mathbb{T}}} \overline{\mathbb{H}}_-)^* \subset (\overline{\mathbb{H}}_+ \otimes_{\mathbb{Z}/p^t} \overline{\mathbb{H}}_-)^* = (\overline{\mathbb{H}}_+)^* \otimes_{\mathbb{Z}/p^t} (\overline{\mathbb{H}}_-)^*,$$

where $*$ means $\mathrm{Hom}(-, \mathbb{Z}/p^t)$.

Proof. The first part of the theorem follows directly from the definition of Θ given in (109). The second follows from the Hecke equivariance of Θ^*, in light of the fact that $\kappa_1^+ \otimes \kappa_0^- + \kappa_1^+ \otimes \kappa_0^-$ is the higher Eisenstein element in $(\mathbb{H}^+ \otimes_{\mathbb{T}} \mathbb{H}^-)^\vee$ attached to $\kappa_0^+ \otimes \kappa_0^-$, by Proposition 4.14. □

We can now prove Conjecture 1.1 in the RM setting.

PROPOSITION 5.11. *We have*

$$\langle G, \mathfrak{S} \rangle = \frac{1}{24} h(\mathfrak{o}) C_g \cdot L_{\mathrm{alg}}(\psi) \cdot (\beta_N - \alpha_N) \cdot \log(u_K). \tag{115}$$

Proof. Applying (114) and part (2) of Theorem 5.10,

$$\begin{aligned} \langle G, \mathfrak{S} \rangle &= \frac{-\beta_N C_g}{24} \cdot \langle \gamma_1 \otimes \gamma_\psi, \kappa_0^+ \otimes \kappa_1^- + \kappa_1^+ \otimes \kappa_0^- \rangle \\ &= \frac{-\beta_N C_g}{24} \cdot \kappa_1^+(\gamma_1) \cdot \kappa_0^-(\gamma_\psi), \end{aligned}$$

where we have used the fact that $\kappa_0^+(\gamma_1) = 0$ to ignore the term arising from $\langle \gamma_1 \otimes \gamma_\psi, \kappa_0^+ \otimes \kappa_1^- \rangle$. The theorem now follows from Proposition 5.7 and (113), which imply that

$$\kappa_1^+(\gamma_1) = -h \log(u_K), \qquad \kappa_0^-(\gamma_\psi) = (1 - \alpha_N/\beta_N) \cdot L_{\mathrm{alg}}(\psi). \qquad \square$$

To prove Theorem 1.2 of the Introduction when K is a real quadratic field, it remains, as before, to relate the right-hand side of (115) to the expression $\mathrm{red}_N(u_g)$ occurring in this theorem.

LEMMA 5.12 (cf. Lemma 5.6). *Let $U_g := (\mathcal{O}_K^\times \otimes \mathrm{Ad}^*(\rho_g)^\circ)^{G_{\mathbb{Q}}}$. There exists $u_g \in U_g$ with the property that, for all N as before,*

$$\log(\mathrm{red}_N(u_g)) = (\alpha_N - \beta_N) \log(u_K).$$

As before, Theorem 1.2 will follow from this: we have

$$24 \langle G, \mathfrak{S} \rangle = \log(\mathrm{red}_N(u_g'))$$

with $u_g' = -h(\mathfrak{o}) L_{\mathrm{alg}}(\psi) C_g \cdot u_g$.

Proof. Let e_1 and e_2 be eigenvectors in V_g for the action of G_K, on which G_K acts via the characters ψ_1 and ψ_1' respectively. Since N is split in K, the associated Frobenius automorphism $\sigma_N \in G_{\mathbb{Q}}$ is a diagonal matrix with entries α_N and β_N. Representing the elements of $\mathrm{Ad}(V_g)$ as matrices relative to the basis (e_1, e_2), so that $\rho_g(\sigma_N) = \left(\begin{smallmatrix} \alpha_N & 0 \\ 0 & \beta_N \end{smallmatrix}\right)$, and using the trace form to identify $\mathrm{Ad}(V_g)$ with its dual $\mathrm{Ad}^*(V_g)$, we define

$$u_g := u_K \otimes \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

which is clearly $G_{\mathbb{Q}}$-invariant: it is fixed by G_K, and the nontrivial automorphism of K negates both factors. As after (108) this indeed defines an element of U_g.

One then finds

$$\begin{aligned}\mathrm{red}_N(u_g) &= \langle u_g, \rho_g(\sigma_N)\rangle = \mathrm{Trace}\begin{pmatrix} u_K \otimes \alpha_N & 0 \\ 0 & u_K \otimes (-\beta_N)\end{pmatrix} \\ &= u_K \otimes (\alpha_N - \beta_N).\end{aligned}$$

Therefore,

$$\log(\mathrm{red}_N(u_g)) = (\alpha_N - \beta_N)\log(u_K).$$

The lemma follows. □

ACKNOWLEDGMENTS. The authors are grateful to Jan Vonk for the valuable insights which guided their approach to proving the main theorem of Section 3. They also thank Frank Calegari, Hélène Esnault, and Alice Pozzi for stimulating discussions surrounding the topics of this paper.

The anonymous referee made a very careful reading of the paper and made several valuable corrections and suggestions. We thank her or him for their substantial effort, which has substantially improved the paper.

The authors are happy to express their appreciation to Gopal Prasad by dedicating this article to him. The second- and fourth-named authors would like to take this opportunity to add a few personal words:

M.H.: "I vividly remember Gopal's patient and enthusiastic explanation of his own work on arithmetic groups and his sincere interest in my work when we first met, just one year after my Ph.D. And I am grateful for Gopal's generosity and friendship at all our subsequent meetings on three continents over the following decades."

A.V.: "The clarity and beauty of Gopal's work on p-adic groups speak for themselves, and have influenced my work on too many occasions to readily enumerate. And it is with much warmth that I recall the kindness that Gopal has showed throughout my career; I still remember clearly that when I, as a graduate student, visited the University of Michigan, Gopal took the time to speak with me and encourage my work. It is therefore with the greatest pleasure that I dedicate this paper to him, with admiration for a great mathematical career and the best wishes for the future."

References

[Coh03] H. Cohn, *Advanced number theory,* Dover publ., 2003.

[Eme02] M. Emerton, *Supersingular elliptic curves, theta series and weight two modular forms,* J. Amer. Math. Soc. 15 (2002), no. 3, 671–714.

[GV18] S. Galatius and A. Venkatesh, *Derived Galois deformation rings,* Adv. Math. 327 (2018), 470–623.

[GH11] D. Goldfeld and J. Hundley, *Automorphic representations and L-functions for the general linear group,* Cambridge University Press, Cambridge, 2011.

[Gro87] B. H. Gross, *Heights and the special values of L-series, number theory,* Conf. Proc., Can. Math. Soc., 7, pp. 115–187, Am. Math. Soc., Providence, 1987.

[GZ86] B. H. Gross and D. B. Zagier, *Heegner points and derivatives of L-series,* Invent. Math. 84 (1986), no. 2, 225–320.

[HK91] M. Harris and S. Kudla, *The central critical value of a triple product L-function,* Ann. of Math. (2) 133 (1991), no. 3, 605–672.

[HV] M. Harris and A. Venkatesh, *Derived Hecke algebra for weight one forms,* Exp. Math. 28 (2019), 342–361.

[HIM86] T. Hiramatsu, N. Ishii, and Y. Mimura, *On indefinite modular forms of weight one,* J. Math. Soc. Japan 38 (1986), no. 1, 67–83.

[Hur81] A. Hurwitz, *Grundlagen einer independenten Theorie der elliptischen Modulfunctionen und Theorie der Multiplicatorgleichungen erster Stufe,* Math. Ann. 18 (1881), 528–592.

[JL70] H. Jacquet and R. P. Langlands, *Automorphic forms on* GL(2), Lecture Notes in Math., 114, Springer, Berlin, 1970.

[Kan12] E. Kani, *The space of binary theta series,* Ann. Sci. Math. Québec 36 (2012), 501–534.

[Kat] N. Katz, *On a question of Zannier,* unpublished, ⟨https://web.math.princeton.edu/~nmk/zannier8.pdf⟩.

[KL81] D. S. Kubert and S. Lang, *Modular units,* Grundlehren Math. Wiss., 244, Springer, New York-Berlin, 1981.

[Lec] E. Lecouturier, *Higher Eisenstein elements, higher Eichler formulas and ranks of Hecke algebras,* Invent. Math. 223 (2021), 485–595.

[Mar] D. Marcil, *Numerical verification of a conjecture of Harris and Venkatesh,* J. Number Theory 221 (2021), 484–495.

[Maz77] B. Mazur, *Modular curves and the Eisenstein ideal,* Publ. Math. Inst. Hautes Études Sci. 47 (1977), 33–186.

[Maz79] ———, *On the arithmetic of special values of L-functions,* Invent. Math. 55 (1979), 207–240.

[Mer96] L. Merel, *L'accouplement de Weil entre le sous-groupe de Shimura et le sous-groupe cuspidal de $J_0(p)$,* J. Reine Angew. Math. 477 (1996), 71–115.

[PV] K. Prasanna and A. Venkatesh, *Automorphic cohomology, motivic cohomology, and the adjoint L-function,* submitted for publication.

[Rob80] G. Robert, *Congruences entre séries d'Eisenstein, dans le cas supersingulier,* Invent. Math. 61 (1980), no. 2, 103–158.

[Sch02] R. Schmidt, *Some remarks on local newforms for $GL(2)$,* J. Ramanujan Math. Soc. 17 (2002), 115–147.

[SGA1] *Revêtements étales et groupe fondamental* (SGA 1). (French). Séminaire de géométrie algébrique du Bois Marie 1960–61. Directed by A. Grothendieck. With two papers by M. Raynaud. Updated and annotated reprint of the 1971 original [Lecture Notes in Math., 224, Springer, Berlin]. Documents Mathématiques (Paris) [Mathematical Documents (Paris)], 3. Société Mathématique de France, Paris, 2003.

[Ven] A. Venkatesh, *Derived Hecke algebra and cohomology of arithmetic groups,* Forum of Mathematics 7 (2019), e7.

[Vig80] M. F. Vignéras, *Arithmétique des algèbres de quaternions,* Lecture Notes in Math., 800, Springer, Berlin, 1980.

[Voi] J. Voight, *Quaternion algebras,* ⟨https://math.dartmouth.edu/~jvoight/quat-book.pdf⟩.

[Wei64] A. Weil, *Sur certains groupes d'opérateurs unitaires,* Acta Math. 111 (1964), 143–211.

[Yoo] H. Yoo, *Non-optimal levels of a reducible mod ℓ modular representation,* preprint.

[Zag75] D. Zagier, *A Kronecker limit formula for real quadratic fields,* Math. Ann. 213 (1975), 153–184.
[Zha] R. Zhang, Columbia Ph.D thesis, in progress.

H. Darmon
Department of Mathematics and Statistics
McGill University
Montreal
Canada

darmon@math.mcgill.ca

M. Harris
Department of Mathematics
Columbia University
New York, NY, 10027
USA

harris@math.columbia.edu

V. Rotger
IMTech
UPC and Centre de Recerca Matemàtiques
C. Jordi Girona 1-3, 08034 Barcelona
Spain

victor.rotger@upc.edu

A. Venkatesh
School of Mathematics
Institute for Advanced Study
Princeton, NJ, 08540
USA

akshay@ias.edu