CONGRUENCES BETWEEN MODULAR FORMS, CYCLIC ISOGENIES OF MODULAR ELLIPTIC CURVES, AND INTEGRALITY OF $p$-ADIC $L$-FUNCTIONS

SHU-LEUNG TANG

Abstract. Let $\Gamma$ be a congruence subgroup of type $(N_1, N_2)$ and of level $N$. We study congruences between weight 2 normalized newforms $f$ and Eisenstein series $E$ on $\Gamma$ modulo a prime $p$ above a rational prime $p$. Assume that $p \nmid 6N$, $E$ is a common eigenfunction for all Hecke operators and $f$ is ordinary at $p$. We show that the abelian variety associated to $f$ and the cuspidal subgroup associated to $E$ intersect non-trivially in their $p$-torsion points. Let $A$ be a modular elliptic curve over $\mathbb{Q}$ with good ordinary reduction at $p$. We apply the above result to show that an isogeny of degree divisible by $p$ from the optimal curve $A_1$ in the $\mathbb{Q}$-isogeny class of elliptic curves containing $A$ to $A$ extends to an étale morphism of Néron models over $\mathbb{Z}_p$ if $p > 7$. We use this to show that $p$-adic distributions associated to the $p$-adic $L$-functions of $A$ are $\mathbb{Z}_p$-valued.

Introduction

Let $A$ be a modular elliptic curve of conductor $N$ defined over $\mathbb{Q}$ and let $p > 2$ be a prime at which $A$ has good ordinary reduction. Let $\Delta$ be a positive integer prime to $p$. In [9], Mazur and Swinnerton-Dyer construct, using modular symbols, an $H_1(A, \mathbb{Z}) \otimes \mathbb{Q}_p$-valued measure $\mu_{A, \Delta}$ on $\mathbb{Z}_p^*$ associated to $A$, and define the $p$-adic $L$-function of $A$ to be the $p$-adic Mellin transform of $\mu_{A, \Delta}$ which interpolates the values of the complex $L$-functions $L(A, \chi, z)$ at $z = 1$ for Dirichlet characters $\chi$ of conductor $p^n\Delta$, $n \geq 0$. In the light of Iwasawa theory, one would expect $\mu_{A, \Delta}$ to be $H_1(A, \mathbb{Z}) \otimes \mathbb{Z}_p$-valued. This is known when $\Delta = 1$.

Let $\pi : X_0(N) \to A$ be a modular parametrization (i.e. a non-constant $\mathbb{Q}$-morphism) which sends the cusp $\infty$ to the origin of $A$. Let $\omega_A$ be a Néron differential on $A$. Then $\pi^*\omega_A = c(\pi)f(q)\frac{dq}{q}$, where $c(\pi) \in \mathbb{Q}^*$ and $f(q)\frac{dq}{q}$ is a normalized newform on $\Gamma_0(N)$. $c(\pi)$ is called the Manin constant of $\pi$ and is conjectured by Manin to be $\pm 1$ when $A$ is strong Weil [8]. Stevens in [23] studies parametrizations $\pi : X_1(N) \to A$ (which send the cusp $0 (= [0 : 1])$ to the origin) and refines Manin’s conjecture as follows.

Conjecture 0.1. ([23, Conj. I]) For every modular elliptic curve $A$ over $\mathbb{Q}$, there is a modular parametrization $X_1(N) \to A$ whose Manin constant is $\pm 1$. 

Received by the editors May 10, 1995 and, in revised form, September 21, 1995.

1991 Mathematics Subject Classification. Primary 11G05, 11G18; Secondary 11S40.

Key words and phrases. Modular forms, elliptic curves, $p$-adic $L$-functions.

©1997 American Mathematical Society
In [12], $p$-adic distributions on $\mathbb{Z}_p$, are constructed more generally for modular forms of weight $\geq 2$. In the case of $f$ arising from $A$ as above, the construction yields an $\mathcal{L}(A) \otimes \mathbb{Q}_p$-valued measure $\nu_{A,\Delta}$ where $\mathcal{L}(A)$ is the period lattice of $A$ with respect to $\omega_A$ (cf. [23, §4]). If $\Delta = 1$, $\mu_{A,\Delta}$ and $\nu_{A,\Delta}$ coincide (up to a $p$-adic unit) under the identification $H_1(A,\mathbb{Z}) \cong \mathcal{L}(A)$ but may differ in general (due to the $p$-adic “multiplier” [12, §14]). It is known ([23, Thms. 1.6, 4.6]) that $c(\pi) \in \mathbb{Z}$ and $c(\pi)\nu_{A,\Delta}$ is $\mathcal{L}(A) \otimes \mathbb{Z}_p$-valued for any modular parametrization $\pi : X_1(N) \to A$. Thus if Conjecture 0.1 is true, then $\nu_{A,\Delta}$ is $\mathcal{L}(A) \otimes \mathbb{Z}_p$-valued. We study in this paper the integrality of $\nu_{A,\Delta}$ and prove the following (cf. [23, §4, Conj. IV])

**Theorem 0.2.** With the above notation and assumptions, $\nu_{A,\Delta}$ is $\mathcal{L}(A) \otimes \mathbb{Z}_p$-valued for $p > 7$.

To prove Theorem 0.2, it suffices to show $p \nmid c(\pi)$ for some modular parametrization $\pi : X_1(N) \to A$. Let $A$ be the $\mathbb{Q}$-isogeny class of elliptic curves over $\mathbb{Q}$ containing $A$. Then there are a unique curve (up to $\mathbb{Q}$-isomorphism) $A_1$ in $A$ and a modular parametrization $\pi_1 : X_1(N) \to A_1$ such that if $\pi : X_1(N) \to A'$ is a modular parametrization of a curve $A' \in A$, then there is a $\mathbb{Q}$-isogeny $\beta : A_1 \to A'$ such that $\pi = \beta \circ \pi_1$. We call $A_1$ the optimal curve in $A$ and $\pi_1$ an optimal parametrization. By a result analogous to [11, Cor. 4.1], $c(\pi_1) \in \mathbb{Z}[1/n]^*$ where $n$ is the largest square dividing $N$. (Mazur proves this for $X_0(N)$-parametrizations of strong Weil curves, but his method works also for $X_1(N)$-parametrizations of optimal curves.) In particular, $p \nmid c(\pi_1)$. The next step is to look at $\mathbb{Q}$-isogenies between $A_1$ and $A$. In this direction, we prove

**Theorem 0.3.** Suppose $p > 7$. Let $\beta : A_1 \to A$ be a cyclic $\mathbb{Q}$-isogeny of degree divisible by $p$. Then $\beta$ is étale at $p$.

Here we say that an isogeny $\alpha : E_1 \to E_2$ of elliptic curves over $\mathbb{Q}$ is étale at $p$ if the morphism $\alpha : E_1/\mathbb{Z}_p \to E_2/\mathbb{Z}_p$ of Néron models over $\mathbb{Z}_p$ is étale. The proof of Theorem 0.3 relies on Theorem 0.4 below, which reflects a general principle in the theory of modular curves that whenever there is a congruence between two modular forms, there should be a fusion module which explains the congruence. Let $\Gamma$ be a congruence group of type $(N_1,N_2)$ and of level $N$ ([21, 1.1]). Let $f$ (resp. $E$) be a weight two normalized newform (resp. an Eisenstein series) on $\Gamma$. Assume that $E$ is a common eigenfunction for all Hecke operators and that there is a place $\mathfrak{p}$ of $\mathbb{Q}$ such that the Fourier coefficients of $f$ and $E$ are congruent mod $\mathfrak{p}$. We say that $\mathfrak{p}$ is an Eisenstein prime for $E$ and $f$. Let $A_f$ be the abelian subvariety over $\mathbb{Q}$ of the Jacobian $J_\Gamma$ of the modular curve associated to $\Gamma$ ([18, Thm. 7.14]) and $K_f$ the field generated over $\mathbb{Q}$ by the Fourier coefficients of $f$. There is an embedding of $K_f$ into $\text{End}(A_f) \otimes \mathbb{Q}$ (loc. cit.). Let $C_E$ be the cuspidal subgroup of $J_\Gamma$ associated to $E$ ([21, 1.8]). Let $\mathfrak{p}$ be the prime of $K_f$ below $\mathfrak{p}$. We say that $f$ is ordinary at $\mathfrak{p}$ if the $p$-th Fourier coefficient of $f$ is a unit mod $\mathfrak{p}$. By considering the $q$-expansions in characteristic $p$ of $A_f/\mathfrak{p}$ and $C_E/\mathfrak{p}$, we prove

**Theorem 0.4.** Let $\mathfrak{p}$ be an Eisenstein prime for $f$ and $E$. Assume that $\mathfrak{p} \nmid 6N$ and $f$ is ordinary at $\mathfrak{p}$. Then $A_f/\mathfrak{p} \cap C_E \neq 0$.

Returning to the proof of Theorem 0.3, we let $\beta : A_1 \to A$ be a cyclic isogeny of degree divisible by $p$. Assuming that the Galois character on the subgroup of order $p$ of $\ker \beta$ is not the trivial character or the Teichmüller character, we show that there is an Eisenstein series $E$ on $\Gamma_1(N)$ arising from the Galois representation on
the $p$-torsion points of $A_1$ whose Fourier coefficients are congruent mod $\mathfrak{P}$ to those of $f$ (Prop. 2.6). Theorem 0.4 shows that $A_1$ and the cuspidal subgroup of the Jacobian of $X_1(N)$ associated to $E$ intersect non-trivially in their $p$-torsion points. Using the classification theorem of rational cyclic isogenies of elliptic curves over $\mathbb{Q}$ ([11], [7]), we deduce that $p \leq 7$ ($\S$2.3).

We prove Theorems 0.4, 0.3 and 0.2 in Sections 1, 2 and 3 respectively. For a field $K$, we write $\overline{K}$ for an algebraic closure of $K$, $K_s$ for the separable closure of $K$ in $\overline{K}$ and $G_K$ for $\text{Gal}(K_s/K)$. Throughout the paper, we fix a place $\mathfrak{P}$ of $\overline{\mathbb{Q}}$ above $p$ and identify the residue field of the valuation ring of $\overline{\mathbb{Q}}$ at $\mathfrak{P}$ as an algebraic closure $\mathbb{F}_p$ of $\mathbb{F}_p$. Also fix an embedding of $\overline{\mathbb{Q}}$ into $\mathbb{C}$ so that $\mathfrak{P}$ is the place induced by it. For a prime $l$, $D_l$ will denote a decomposition group in $G_Q$ for $l$ and $I_l$ its inertia subgroup. For a commutative group scheme $G$ and $\alpha$ an endomorphism of $G$, $G[\alpha]$ will denote the kernel of $\alpha$ and $G[\alpha^\infty] = \bigcup_{n \geq 0} G[\alpha^n]$. If $a$ is a set of endomorphisms of $G$, then $G[a]$ will denote $\bigcap_{a \in a} G[\alpha]$. When $G = \mathbb{G}_m$ is the multiplicative group, we write $\mu_n$ for $\mathbb{G}_m[n]$. We shall use the following notation for cusps: if $\Gamma$ is a congruence subgroup of level $N$ and $a$, $b \in \mathbb{Z}$ are such that $(a, b, N) = 1$, then $[a/b] = [a/b]_\Gamma$ will denote the $\Gamma$-equivalence class of the cusp $a/b$.

Acknowledgments. This work was done while the author was a post-doctoral fellow at McMaster University. Their support is gratefully acknowledged. I also thank the referee for suggestions which led to an improvement of Theorem 0.4.

1. Fusion module of an Eisenstein prime

In this section, we prove Theorem 0.4. Let $\Gamma$ be a congruence subgroup of type $(N_1, N_2)$ and of level $N$. Let $f$ (resp. $E$) be a weight two normalized newform (resp. an Eisenstein series) on $\Gamma$. Suppose that $E$ is a common eigenfunction for all Hecke operators. Let $a_n$ ($n \geq 0$) (resp. $b_n$ ($n \geq 0$)) be the Fourier coefficients of $f$ (resp. $E$). (We take $a_0 = 0$.) Assume that $\mathfrak{P}$ is an Eisenstein prime associated to $f$ and $E$, i.e. $a_n = b_n \pmod{\mathfrak{P}}$ for all $n \geq 0$. We write $f \equiv E \pmod{\mathfrak{P}}$. Assume further that $\mathfrak{P} \nmid 6N$ and $f$ is ordinary at $p$. We first review some properties of regular differentials on modular curves and their $q$-expansions ($\S$1.2) and the $q$-expansions of the $p$-torsion points of the Jacobian of a curve over $\mathbb{F}_p$ ($\S$1.3). We show that the $q$-expansions in characteristic $p$ of $A_f[p]$ and the cuspidal subgroup $C_E[p]$ coincide. This enables us to conclude that $A_f[p]$ and $C_E$ intersect non-trivially.

1.1. Modular curves and Hecke operators. Let $\mathfrak{H}$ be the upper half plane and $\mathfrak{H}^* = \mathfrak{H} \cup \mathbb{P}^1(\mathbb{Q})$. The quotient $\mathfrak{H}/\Gamma$ is an open Riemann surface which can be compactified to a projective algebraic curve $X_{\Gamma/C} = \mathfrak{H}/\Gamma$ over $\mathbb{C}$ by the addition of cusps. By Shimura [18, §6.7], $X_{\Gamma/C}$ has a canonical model $X_{\Gamma}$ over $\mathbb{Q}$. The moduli interpretation of $X_{\Gamma}$ is that it is the coarse moduli scheme of the functor associating to each $\mathbb{Q}$-scheme $S$ the $S$-isomorphism classes of generalized elliptic curves over $S$ with an $H$-orbit of level $N$-structures where $H$ is the image of $\Gamma$ under the natural map $\Gamma \to \text{GL}_2(\mathbb{Z}/N\mathbb{Z})$. Write $X(N), X_0(N), X_1(N)$ for $\Gamma = \Gamma(N), \Gamma_0(N), \Gamma_1(N)$ respectively.

Let $T_l$ ($l \nmid N$) and $U_l$ ($|l| N$) be the usual Hecke correspondences on $X_{\Gamma}$ (see for example [18, Chap. 7]). For $m \in (\mathbb{Z}/N\mathbb{Z})^*$, let $\sigma_m \in \text{SL}_2(\mathbb{Z})$ be such that

$$\sigma_m \equiv \begin{pmatrix} * & 0 \\ 0 & m \end{pmatrix} \pmod{N}$$
and write $\langle m \rangle$ for the Hecke correspondence corresponding to $\sigma_m$. Let $J_\Gamma$ be the Jacobian of $X_\Gamma$ and $T \subset \text{End}(J_\Gamma) \otimes \mathbb{Q}$ the Hecke algebra generated by the images of $T_l$ ($l \nmid N$), $U_l$ ($l \mid N$) and $\langle m \rangle$, $m \in (\mathbb{Z}/N\mathbb{Z})^\times$. Denote the images of $T_l$, $U_l$ and $\langle m \rangle$ in $T$ by the same symbols. For brevity, we shall sometimes write $T_l$ for $U_l$ when $l\mid N$ below.

1.2. **Regular differentials and their $q$-expansions.** Let $\zeta_N$ be a primitive $N$-th root of unity. Let $O$ be the completion of $\mathbb{Z}[\zeta_N]$ at the prime below $\mathfrak{q}$, and $K$ the field of fractions of $O$. Fix an embedding of $K$ in $\mathbb{C}$. Let $X_{\Gamma/O}$ be the normalization of the $j$-line $\mathbb{P}^1_{/\mathcal{O}}$ in the function field of $Y_{\Gamma/K}$, where the morphism $Y_{\Gamma/K} \to \mathbb{P}^1_{/\mathcal{O}}$ is defined on points by sending an elliptic curve $E$ with level $H$-structure to the $j$-invariant of $E$. Then $X_{\Gamma/O}$ is smooth. For any ring $R$ over $O$, let $\Omega_{\Gamma/R} = \Omega_{X_{\Gamma/R}}$, $\Omega_{\Gamma/cusps} = \Omega_{X_{\Gamma/R}(\text{cusps})}$ the sheaf which, when restricted to the complement of the cuspidal sections, is the sheaf of regular differentials and whose sections in a neighborhood of the cuspidal sections are meromorphic differentials with at worst simple poles along those sections ([10, II 3]). We consider only rings $R$ which are flat over $O$ or $O/p^nO$ for some $n$.

**Proposition 1.1.** ([24, Prop. 6.1], [6, Prop. 5.1]) Let $R \to R'$ be a morphism of rings which are flat over $O$ or $O/p^nO$ for some $n$. Then,

$$H^0(X_{\Gamma/R}, \Omega_{\Gamma/R}) \otimes_R R' \cong H^0(X_{\Gamma/R'}, \Omega_{\Gamma/R'}),$$

$$H^0(X_{\Gamma/R}, \Omega_{\Gamma/R}(\text{cusps})) \otimes_R R' \cong H^0(X_{\Gamma/R'}, \Omega_{\Gamma/R'}(\text{cusps})).$$

We consider the $q$-expansions of regular differentials. Since $H^0(X_{\Gamma/R}, \Omega_{\Gamma/R}) = H^0(X(N)_{/R}, \Omega_{N/R})^H$ by [5, VII 3.3], we can restrict ourselves to the case $\Gamma = \Gamma(N)$. Let $\text{Tate}(q)$ be the Tate curve with $N$-sides over $O[q^{1/N}]$. $\text{Tate}(q)$ with Drinfeld basis $(\zeta_N, q^{\frac{1}{N}})$ defines a point on $X_{\Gamma/O}$, and the corresponding morphism

$$\tau_{/O} : \text{Spec } O[q^{1/N}] \to X_{\Gamma/O}$$

can be identified with the formal completion of $X_{\Gamma/O}$ along the section corresponding to the cusp $\infty$ ($= [1:0]$) ([5, VII 2.4]). For any $R$ as above, we then have a morphism

$$\tau_{/R} : \text{Spec } R[q^{1/N}] \to X_{\Gamma/R}.$$ 

For any $\omega \in H^0(X_{\Gamma/R}, \Omega_{\Gamma/R})$, we define the $q$-expansion of $\omega$ at $\infty$ to be the element $\varphi_R(\omega) \in R[q^{1/N}]$ such that

$$\tau_{/R}^* \omega = \varphi_R(\omega) dq^{1/N}/q^{1/N}.$$ 

This defines the $q$-expansion morphism $\varphi_R : H^0(X_{\Gamma/R}, \Omega_{\Gamma/R}) \to R[q^{1/N}]$. Similarly, there is a $q$-expansion map $\varphi_R : H^0(X_{\Gamma/R}, \Omega_{\Gamma/R}(\text{cusps})) \to R[q^{1/N}]$. Let $B^0(O)$ (resp. $B(O)$) be the submodule of $O[q^{1/N}]$ consisting of the $q$-expansions at $\infty$ of cusp forms (resp. holomorphic modular forms) of weight $2$ on $\Gamma$ with coefficients in $O$. For any $R$ as above, let $B^0(R) = B^0(O) \otimes R$ and $B(R) = B(O) \otimes R$. One can show, using Prop. 1.1, that $\varphi_R(H^0(X_{\Gamma/R}, \Omega_{\Gamma/R})) \subset B^0(R)$ ([24, Prop. 6.2]). Similarly, we have $\varphi_R(H^0(X_{\Gamma/R}, \Omega_{\Gamma/R}(\text{cusps}))) \subset B(R)$. So we have maps

(1.1) $\varphi_R : H^0(X_{\Gamma/R}, \Omega_{\Gamma/R}) \to B^0(R),$

(1.2) $\varphi_R : H^0(X_{\Gamma/R}, \Omega_{\Gamma/R}(\text{cusps})) \to B(R).$
One can define an action of $\mathbb{T}$ on $H^0(X_{\Gamma/R}, \Omega_{/R}^{1}(\text{cusps}))$ using the definition of Hecke correspondences, and one on $B(R)$ by its action on the $q$-expansions of classical modular forms. With these actions, (1.1) and (1.2) are then $\mathbb{T}$-morphisms.

Furthermore, if $g \in R[q^\mathbb{Z}]$ with zero constant term is a common eigenvector for $T_i$ ($i \nmid N$) and $U_i$ ($i|N$) with eigenvalues $c_i$, then the usual recursive relations ([18, (3.5.12)]) show that $g$ is determined by the $c_i$ up to multiplication by a constant.

1.3. $q$-expansions of $p$-torsion points. Let $X$ be a smooth projective curve defined over $\mathbb{F}_p$ and let $J$ be its Jacobian. Let $\Omega^1_X$ be the canonical sheaf of differentials on $X$ and let $\mathcal{C}$ be the Cartier operator on $H^0(X, \Omega^1_X)$ ([3]). There is a canonical isomorphism (cf. [15, §11, Prop. 10])

$$
\delta : J[p] \rightarrow H^0(X, \Omega^1_X)^C
$$

where $J[p] = \{x \in J(F_p) : px = 0\}$ and $H^0(X, \Omega^1_X)^C = \{\omega \in H^0(X, \Omega^1_X) : C\omega = \omega\}$. The definition of $\delta$ is as follows: if $x$ in the domain is represented by a divisor $D$ on $X/\mathbb{F}_p$ such that $pD = (g)$ where $(g)$ is the divisor of $g$, then $\delta(x) = dg/g$.

**Proposition 1.2.** ([24, Prop. 6.5], [6, Prop. 5.2]) Let $J$ be the Jacobian of $X = X_{\Gamma/R}$ and let $\varphi_{\mathbb{F}_p}$ be as in (1.1). Then $\varphi_{\mathbb{F}_p} \circ (\delta \otimes 1)$ induces an injection $\varphi : J[p] \otimes_{\mathbb{F}_p} \mathbb{F}_p \hookrightarrow B^0(\mathbb{F}_p)$ such that $\varphi \circ T_n = T_n \circ \varphi$ for all $n \geq 1$ where $T_n$ is the $n$-th Hecke operator and $T_n^*$ is the dual of the endomorphism of $J$ which $T_n$ induces by Pic functoriality.

We call $\varphi$ in Proposition 1.2 the $q$-expansion map of the $p$-torsion points of $J$.

Let $A_f$ be the abelian subvariety over $\mathbb{Q}$ of the Jacobian $J_\Gamma$ of $X_\Gamma$ associated to $f$ ([18, Thm. 7.14]). Let $K_f$ be the field generated over $\mathbb{Q}$ by the $a_n$ and $\iota$ the embedding $K_f \hookrightarrow \text{End}(J_\Gamma) \otimes_{\mathbb{Z}} \mathbb{Q}$ from the construction of $A_f$ (loc. cit.). Let $p$ be the prime of $K_f$ below $\mathfrak{p}$.

**Proposition 1.3.** Assume that $p \nmid N$ and $f$ is ordinary at $p$. Then the image of $A_f[p]/\mathfrak{p}(\mathbb{F}_p) \otimes_{\mathbb{F}_p} \mathbb{F}_p$ under $\varphi$ is the $\mathbb{F}_p$-module generated by the reduction $\overline{f}$ of $f(q)$ in $B^0(\mathbb{F}_p)$.

**Proof.** By [18, Thm. 7.14], $A_f$ is stable under subrings of $\text{End}_\mathbb{Q}(J_\Gamma) = \text{End}(J_\Gamma) \otimes_{\mathbb{Z}} \mathbb{Q}$ induced by the Hecke correspondences $T_n$ via Albanese functoriality and Pic functoriality which are related as follows. The endomorphism of $J_\Gamma$ which $T_n$ induces by Albanese functoriality is the endomorphism denoted $\xi_n$ in [18, Chap. 7]. Its dual is the endomorphism of $J_\Gamma$ which $T_n$ induces by Pic functoriality. (For more details, see [14, p. 444].) By [18, Thm. 7.14(b)], $\xi_n x = \iota(a_n)x$ for all $x \in A_f$ and all $n$. Since $J_\Gamma$ has good reduction at $p$, the morphism $A_f[\mathfrak{p}] \rightarrow J_{\Gamma/\mathfrak{p}}$ is a closed immersion ([11, Prop. 1.2]), hence $A_f[p]/\mathfrak{p} \hookrightarrow J_{\Gamma}[p]/\mathfrak{p}$. Since $f$ is ordinary at $p$, $A_f[p]/\mathfrak{p}(\mathbb{F}_p)$ is a one-dimensional vector space over the residue field of $p$ (cf. [25, Thm. 2.2]). The action of $\iota(a_n)$ on $A_f[p]/\mathfrak{p}(\mathbb{F}_p)$ is given by multiplication by $a_n$ mod $p$. For any $x \in A_f[p]/\mathfrak{p}(\mathbb{F}_p)$ and $n \geq 1$, it follows from Prop. 1.2 and the above discussion that $T_n \varphi(x \otimes 1) = \varphi(T_n x \otimes 1) = \varphi(\iota(a_n)x \otimes 1) = a_n \varphi(x \otimes 1)$.

Now $\overline{f}$ is a common eigenvector for all $T_n$ with eigenvalues $a_n$ mod $p$. Thus $\varphi(x \otimes 1)$ is an eigenvector of $T_n$ for all $n$ with the same eigenvalues. (Note that $B^0(\mathbb{F}_p) \subset q\mathbb{F}_p[[q]]$.) So $\varphi(x \otimes 1) = c\overline{f}$ for some $c \in \mathbb{F}_p$. This proves the proposition. $\square$
Remark 1.4. Let $\sigma : K_f \hookrightarrow \mathbb{C}$ be an embedding. Let $f^{\sigma}$ be the cusp form obtained by applying $\sigma$ to the coefficients of $f$ (cf. [18, Thm. 7.14]), $A_f^\sigma$ the abelian subvariety of $J_f$ associated to $f^{\sigma}$ and $p^\sigma$ the $\sigma$-conjugate of $p$. Then $\sigma_p^\sigma$ is a unit mod $p^\sigma$, so $f^{\sigma}$ is ordinary at $p^\sigma$. If $\sigma$ extends to an element in the decomposition group $D_{p^\sigma}$ for $\mathfrak{P}$ (we view $K_f$ as a subfield of $\overline{\mathbb{Q}}$), then the same arguments as in Proposition 1.3 show that $\varphi \left( A_f^\sigma[p^\sigma]/\mathbb{F}_p, \mathbb{F}_p \right) = \overline{\mathbb{F}}_p$. 

1.4. Cuspidal subgroups associated to Eisenstein series. We recall some results in [21] and [22] which we need below (Props. 1.5, 1.6 and 1.7). Let $E_\Gamma$ be the space of weight 2 Eisenstein series on $\Gamma$. For any $E \in \mathcal{E}_\Gamma$, let $\omega_E$ be the differential form on $\mathcal{H}/\Gamma$ whose pull-back to $\mathcal{H}$ is $E(z)dz$. Let $\mathcal{P}(E)$ be the image of

$$H_1(\mathfrak{H}/\Gamma, \mathbb{Z}) \to \mathbb{C}, \quad \gamma \mapsto \int_1^{\gamma} \omega_E.$$ 

For any $\mathbb{Z}$-module $M \subset \mathbb{C}$, let $\mathcal{E}_\Gamma(M) = \{ E \in \mathcal{E}_\Gamma : \mathcal{P}(E) \subset M \}$. We then have

**Proposition 1.5.** ([22, Prop. 1.1(a)]) For any $\mathbb{Z}$-module $M \subset \mathbb{C}$, the natural map $\mathcal{E}_\Gamma(\mathbb{Z}) \otimes_\mathbb{Z} M \to \mathcal{E}_\Gamma(M)$ is an isomorphism.

In [21, §1.8], Stevens showed how one can associate to an arbitrary $E \in \mathcal{E}_\Gamma$ a subgroup $C_E$ of the cuspidal group $C_\Gamma$ of $J_\mathfrak{P}$. The construction of $C_E$ is as follows. Let $\text{cusps} = \text{cusps}(\Gamma)$ denote the set of cusps on $X_\Gamma$ and $\text{Div}^0(\text{cusps})$ the group of divisors of degree zero supported on the cusps. For any $\mathbb{Z}$-module $M$, define $\text{Div}^0(\text{cusps}; M) = \text{Div}^0(\text{cusps}) \otimes_\mathbb{Z} M$. Let

$$\delta_\Gamma(E) = \sum_{x \in \text{cusps}} r_x(E) \cdot x \quad \in \text{Div}^0(\text{cusps}; \mathbb{C})$$

where $r_x(E) = 2\pi i \text{res}_x(\omega_E)$ and $\text{res}_x(\omega_E)$ is the residue of $\omega_E$ at the cusp $x$. We note that by [22, Thm. 1.3(a)],

$$r_{[\gamma]}(E) = e([\gamma]) \cdot a_0(E|_I\gamma_{[\gamma]})\label{eq:1.4}$$

where $e([\gamma])$ is the ramification index of $[\gamma]$ over $X(1)$, $\gamma_{[\gamma]} \in \text{SL}_2(\mathbb{Z})$ is such that $\gamma_{[\gamma]} \cdot \infty$ represents $[\gamma]$ and $a_0(E|_I\gamma_{[\gamma]})$ is the constant term of the Fourier expansion of $E|_I\gamma_{[\gamma]}$. Let $R(E)$ be the $\mathbb{Z}$-submodule of $C_{\Gamma}$ generated by the coefficients of $\delta_\Gamma(E)$ and let

$$R(E)^* = \{ \eta \in \text{Hom}_\mathbb{Q}(R(E) \otimes_\mathbb{Z} \mathbb{Q}, \mathbb{Q}) : \eta(R(E)) \subset \mathbb{Z} \}.$$ 

The subgroup $C_E$ of $C_\Gamma$ associated to $E$ is by definition the image of the composition

$$\begin{array}{ccl}
R(E)^* & \longrightarrow & \text{Div}^0(\text{cusps}) \\
\eta & \mapsto & \theta(\delta_\Gamma(E)),
\end{array}\label{eq:1.5}$$

where $\theta$ sends a divisor to its divisor class. Note that since $r_x(E)$ is the integral of $\omega_E$ along some cycle around $x$, $R(E) \subset \mathcal{P}(E)$. Let $A_E = \mathcal{P}(E)/R(E)$. 

**Proposition 1.6.** ([22, Thm. 1.2(a)]) For any $E \in \mathcal{E}_\Gamma$, there is a perfect duality $C_E \times A_E \to \mathbb{Q}/\mathbb{Z}$.

Suppose $E \in \mathcal{E}_\Gamma$ is a common eigenfunction for all $T_l$ and $\langle l \rangle$, $l \nmid N$. Then there are Dirichlet characters $\epsilon_1$ and $\epsilon_2$ modulo $N$ such that $E|T_l = (\epsilon_1(l) + l\epsilon_2(l))E$ for each prime $l \nmid N$ ([21, 3.2.2, (3.2.3)]). We say that $E$ has signature $\epsilon_1$, $\epsilon_2$. Let $\mathbb{Z}[\epsilon_1, \epsilon_2]$ (resp. $\mathbb{Q}[\epsilon_1, \epsilon_2]$) be the ring generated by the values of $\epsilon_1$ and $\epsilon_2$ over $\mathbb{Z}$ (resp. $\mathbb{Q}$). By [21, 3.2.1, 3.2.2], $\mathcal{P}(E)$ and $R(E)$ are fractional ideals of...
Let \( \sigma = \mathbb{Z}[1/2, \epsilon_1, \epsilon_2] \), \( a = \sigma + \sigma \mathcal{R}(E) \) and \( b \) the \( \sigma \)-module generated by \( \{1, B_{1, \epsilon^{-1}}, B_{1, \epsilon}, S(\epsilon_1)B_{2, \epsilon}, s(\epsilon_2)B_{2, \epsilon^{-1}}\} \), where for \( i = 1, 2, B_{i,-} \) are the generalized Bernoulli numbers and
\[
S(\epsilon_i) = \begin{cases} 
\phi(N_i) & \text{if } \epsilon_i = 1, \\
0 & \text{otherwise}, 
\end{cases}
\]
and \( \phi \) is the Euler function.

**Proposition 1.7.** ([21, Thm. 3.6.1]) Let \( E \in \mathcal{E}_1 \) have signature \( \epsilon_1, \epsilon_2 \). Then \( a \subset \sigma \mathcal{P}(E) \subset b \).

We next give a set of generators of the space over \( \mathbb{Q} \) of weight 2 Eisenstein series \( E \) of level \( N \) with \( \mathcal{R}(E) \subset \mathbb{Q} \). For fractional ideals \( a_1 \) and \( a_2 \) of \( \mathbb{Q} \) and \( a_1, a_2 \in \mathbb{Q} \), define
\[
E(z, s) = E(z, s; a_1, a_2; a_1, a_2)
\]
for \( z \in \mathbb{H}, s \in \mathbb{C} \) with \( \text{Re} s > 2 \), where the sum is over all pairs \((m_1, m_2) \in \mathbb{Q}^2 - (0, 0)\) such that \( m_i \equiv a_i \pmod{a_i}, i = 1, 2 \). For fixed \( z, E(z, s) \) may be continued analytically to a meromorphic function in the \( s \)-plane which is holomorphic at \( s = 0 \) (cf. [19, §3]). Define
\[
E(z) = E(z; a_1, a_2; a_1, a_2) = E(z, 0; a_1, a_2; a_1, a_2).
\]

The Fourier expansion of \( E(z) \) at \( \infty \) is given by
\[
-\delta(a_1, a_1)(2\pi)^{-2}N(a_2) \sum_{0 \neq d | a_2} |d|^{-2} \sum_{c \equiv a_1 \pmod{a_2}, bc > 0} \sum_{e \equiv a_1} |b|e^{2\pi i (bcz + ba_2)}
\]
where \( \delta(a_1, a_1) = 1 \) or 0 according as \( a_1 \in a_1 \) or not (cf. [19, (3.6)]). For any \((x, y) \in (N^{-1}\mathbb{Z}/\mathbb{Z})^2 \), let
\[
\phi(x, y)(z) = N^{-2} \sum_{(a_1, a_2) \in (N^{-1}\mathbb{Z}/\mathbb{Z})^2} e^{2\pi i (a_2x_1 - a_1x_2)} E(z; a_1, a_2; \mathbb{Z}, \mathbb{Z}).
\]

By Hecke (cf. [21, pp. 59-60]), \( \{\phi(x, y) \mid (x, y) \in (N^{-1}\mathbb{Z}/\mathbb{Z})^2 - (0, 0)\} \) spans the space of weight 2 Eisenstein series \( E \) of level \( N \) with \( \mathcal{R}(E) \subset \mathbb{Q} \) over \( \mathbb{Q} \). Another fact we need is that if \( U_1 \) is the group of meromorphic functions on \( \mathbb{X}_1/\mathbb{C} \) whose divisors are supported on the cusps, then logarithmic differentiation gives an isomorphism
\[
U_1/\mathbb{C}^* \longrightarrow \mathcal{E}_1(\mathbb{Z}), \quad g \mapsto \frac{1}{2\pi i} \frac{g'(z)}{g(z)},
\]
and if \( E(z) = (2\pi i)^{-1}g'(z)/g(z) \), then \( \delta_1(E) = (g) \) (cf. [22, §1]).

**Lemma 1.8.** For any \( E \in \mathcal{E}_1(\mathbb{Z}) \), the Fourier coefficients of \( E \) at each cusp are in \( (12N^2)^{-1}\mathbb{Z} \).

**Proof.** By (1.9) and a theorem of Kubert (cf. [22, §3]), \( 2E \) is a \( \mathbb{Z} \)-linear combination of the \( \phi(x, y) \) with \((x, y) \in (N^{-1}\mathbb{Z}/\mathbb{Z})^2 - (0, 0)\). For any \( \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}_2(\mathbb{Z}) \), we have \( \phi(x, y)^{\gamma} = \phi(x, y)^{\gamma} \), where \((x, y)^{\gamma} = (ax + cy, bx + dy) \) (cf. [21, 2.4.1(a)]). From [21, 2.4.2(a)], we see that the Fourier coefficients of \( \phi(x, y) \), \((x, y) \in (N^{-1}\mathbb{Z}/\mathbb{Z})^2 - (0, 0)\), at \( \infty \) are in \( (12N^2)^{-1}\mathbb{Z} \). \( \square \)
Suppose now $E$ is a common eigenfunction for $T_l$ for all $l$ and $\langle l \rangle$, $l \mid N$, such that $\mathfrak{P}$ is an Eisenstein prime associated to $f$ and $E$ as at the beginning of §1.

**Proposition 1.9.** Assume that $p \nmid 6N$ and $f$ is ordinary at $p$. Then $p$ divides the order of $C_E$.

*Proof.* Let $\mathfrak{o}_1 = \mathbb{Z}[\epsilon_0, \epsilon_0^{-1}]$ and $\mathfrak{o} = \mathfrak{o}_1[1/2]$. By Prop. 1.7, $N \cdot \mathcal{P}(E) \subset \mathfrak{o}$, so $E \in \mathcal{E}_N(N^{-1} \mathfrak{o})$. By Prop. 1.5, there exist $\lambda_i \in N^{-1} \mathfrak{o}$, $E_i \in \mathcal{E}_N(\mathbb{Z})$ such that $E = \sum \lambda_i E_i$. Since $\mathfrak{b} \subset N^{-1} \mathfrak{o}$, Prop. 1.7 shows that the non-integral part of $\mathfrak{b} \mathcal{P}(E)$ is prime to $p$. (By the integral (resp. non-integral) part of a fractional ideal, we mean the product of the factors in its prime decomposition which occur to a positive (resp. negative) exponent.) Since $\mathfrak{o} \mathcal{R}(E) \subset \mathfrak{o} \mathcal{P}(E)$, the non-integral part of $\mathfrak{o} \mathcal{R}(E)$ is prime to $p$ also. We suppose $p \nmid \#C_E$ and derive a contradiction. By Prop. 1.6, $p \nmid \#(\mathcal{P}(E)/\mathcal{R}(E))$, so $p \nmid \#(\mathfrak{o} \mathcal{R}(E)/\mathfrak{o} \mathcal{R}(E))$. Since $\mathfrak{a} \subset \mathfrak{o} \mathcal{P}(E)$ by Prop. 1.7, $p \nmid \#(\mathfrak{o} + \mathfrak{o} \mathcal{R}(E))/\mathfrak{o} \mathcal{R}(E) = \#(\mathfrak{o} \cap \mathfrak{o} \mathcal{R}(E))$. This implies that the integral part of $\mathfrak{o} \mathcal{R}(E)$ is prime to $p$. Hence $\mathfrak{o} \mathcal{R}(E)$ is prime to $p$.

Let $\wp = \mathfrak{P} \cap \mathfrak{o}_1$ and let $\eta_0$ be the composite homomorphism $\mathfrak{o}_1 \rightarrow \mathfrak{o}_1/\wp \rightarrow \wp_p$ where $\operatorname{tr}$ is the trace map from $\wp := \mathfrak{o}_1/\wp$ to $\wp_p$. Since $\mathfrak{o}_1$ is projective over $\mathbb{Z}$, we can lift $\eta_0$ to a surjective homomorphism $\eta_0 : \mathfrak{o}_1 \rightarrow \mathbb{Z}$. Extend $\eta_0$ $\mathbb{Q}$-linearly to a map $\mathcal{R}(E) \otimes \mathbb{Q} \to \mathbb{Q}$, denoted $\eta_0$ again. Since $\mathcal{R}(E)$ is prime to $p$, there exists $a \in \mathbb{Z}$, $(a, p) = 1$, such that $a \mathcal{R}(E) \subset \mathfrak{o}_1$. Since $a \mathcal{R}(E)$ is prime to $p$, $\eta_0(a \mathcal{R}(E)) = m \mathbb{Z}$ for some $m \in \mathbb{Z}$ prime to $p$. Let $\eta = \frac{a}{m} \eta_0$. Then $\eta \in \mathcal{R}(E)^*$. Hence $\eta_0(\mathcal{R}(E)) = \mathbb{Z}$, $\eta(\mathfrak{o}) = \frac{a}{m} \mathbb{Z}[1/2]$ and $\eta(\wp) \subset \frac{p}{m} \mathbb{Z}$. So $\eta(N^{-1} \mathfrak{o}) = \frac{a}{mN} \mathbb{Z}[1/2]$, and we can choose $n \in \mathbb{Z}$, $p \nmid n$, such that $n_i = n \eta(\lambda_i) \in \mathbb{Z}$ for all $i$. Let

$$\eta(E) = \sum \eta(\lambda_i) E_i.$$ 

Then

$$\eta(E)(q) = \sum \eta(\lambda_i) E_i(q) = \eta(\sum \lambda_i E_i(q)) = \eta(E(q)),$$

where $\eta(E(q))$ is the $q$-series obtained by applying $\eta$ to the coefficients of $E(q)$. Since $f \equiv E$ (mod $\mathfrak{P}$),

$$\eta(E)(q) \equiv \operatorname{Tr}_{\wp/\wp_p}(E(q)) \equiv \operatorname{Tr}_{\wp/\wp_p}(f(q)) \pmod{p \mathbb{Z}(p)},$$

where $\operatorname{Tr}_{\wp/\wp_p}(E(q))$ is the $q$-series obtained by reducing the coefficients of $E(q)$ mod $\wp$ and taking the trace from $\wp$ to $\wp_p$, and similarly for $\operatorname{Tr}_{\wp/\wp_p}(f(q))$, and $\mathbb{Z}(p)$ is the localization of $\mathbb{Z}$ at $p$. By (1.9), there exist $g_i \in U_{T_l}$ such that $(2\pi i)^{-1} g_i'(z)/g_i(z) = E_i(z)$ for all $i$. Let $g = \prod g_i^{n_i}$ and $\omega = dg/g$. Then $\eta(E)(q)$ is the $q$-expansion of $\omega$ at $\infty$ and $(g) = \delta_{T}(\mathbb{M}(E))$. In particular, $g$ is non-constant. Since $\eta(E) = \sum \eta(\lambda_i) E_i$ with $E_i \in \mathcal{E}_N(\mathbb{Z})$ and $\eta(\lambda_i) \in \mathbb{Z}(p)$ for all $i$, Lemma 1.8 gives that $\eta(E)$ has $p$-integral Fourier coefficients at each cusp for $p \nmid 6N$. It follows from [5, VII 3.9(ii)] that $\eta(E)$ is a modular form with coefficients in $\mathcal{O}$. (Recall $\mathcal{O}$ was the completion of $\mathbb{Z}[\mathfrak{n}]$ at the prime below $\mathfrak{P}$.) Hence $\omega$ arises by extension of scalars to $\mathbb{C}$ from an element (denoted $\omega$ again) in $H^0(X_1(N)/\mathcal{O}, \mathcal{O}(\mathfrak{c}(\text{cusps})))$ with $\varphi_{\mathcal{O}}(\omega) = n \eta(E)(q)$.

Write $X$ for $X_\mathfrak{P}$. Let $\mathcal{O}^*(\mathfrak{c}(\text{cusps}))$ denote the sheaf on $X_\mathfrak{O}$ which when restricted to the complement of the cuspidal divisors is the sheaf of invertible elements of $\mathcal{O}_X$ and whose sections in a neighborhood of the cuspidal divisors consist of functions with divisors supported on those divisors. We see from the exact sequence

$$0 \to \mathcal{O}^* \to H^0(X_\mathfrak{O}, \mathcal{O}^*(\mathfrak{c}(\text{cusps}))) \xrightarrow{d\log} H^0(X_\mathfrak{O}, \mathcal{O}(\mathfrak{c}(\text{cusps})))$$
that $g$ comes from a function (denoted $g$ again) in $H^0(X/\mathcal{O}, \mathcal{O}^*(\text{cusps}))$ up to an element in $\mathcal{O}^*$. Let $g_0$ be the function on $X_{/\mathbb{F}_p}$ obtained from $g$ by the base change $\text{Spec}(\overline{\mathbb{F}}_p) \to \text{Spec}(\mathcal{O})$. Then $g_0$ is a non-constant function. Since $X/\mathcal{O}$ is smooth over $\text{Spec}(\mathcal{O})$, $(g_0) = \delta_\tau(n\eta(E))/\mathcal{P}_p$, by [17, Thm. 20], where $\delta_\tau(n\eta(E))/\mathcal{P}_p$ is the pull-back of $b_\tau(n\eta(E))$ to $X_{/\mathbb{F}_p}$. The cuspidal sections of $X_{/\mathbb{Z}[1/N, \zeta_N]}$ are all disjoint over $\text{Spec}\mathbb{Z}[1/N, \zeta_N]$, cf. [5, VII §2.2]. Let $\omega/\mathcal{P}_p$ be the image of $\omega$ in $H^0(X_{/\mathbb{F}_p}, \Omega^1_{\mathcal{P}_p})$. By (1.10), $\varphi_{\mathcal{P}_p}(\omega/\mathcal{P}_p) = \text{Tr}_{\mathbb{F}_p/\mathbb{F}_p}(f(q))$. For each $\tau \in \text{Gal}(\mathbb{F}/\mathcal{P}_p)$, fix a lift $\sigma_\tau$ of $\tau$ in the decomposition group $D_\mathcal{P}$ of $G_\mathbb{Q}$ for $\mathcal{P}_p$, and let $x_\sigma \otimes c_\tau \in \mathcal{A}_\omega^s[p^s\sigma]/\mathcal{P}_p(\mathbb{F}_p) \otimes \mathbb{F}_p$ be such that $\varphi(x_\sigma \otimes c_\tau) = \mathcal{F}_\sigma \tau$ (cf. Prop. 1.3, Remark 1.4).

Then

$$\varphi_{\mathcal{P}_p}(\omega/\mathcal{P}_p) = n \sum \mathcal{F}_\sigma \tau = n \cdot \varphi \left( \sum \tau x_\tau \otimes c_\tau \right) \in \varphi \left( J_\tau[p]/\mathcal{P}_p(\mathbb{F}_p) \otimes \mathbb{F}_p \right)$$

and so $\omega/\mathcal{P}_p \in H^0(X_{/\mathbb{F}_p}, \Omega^1_{\mathcal{P}_p}) \otimes \mathbb{F}_p$. Since $\omega/\mathcal{P}_p$ is of the form $dg_0/g_0$, $\omega/\mathcal{P}_p \in H^0(X_{/\mathbb{F}_p}, \Omega^1_{\mathcal{P}_p})$ by [3, Thm. 2]. Hence there exists $x \in A_f[p]/\mathcal{P}_p(\mathbb{F}_p)$ such that $\delta(x) = \omega/\mathcal{P}_p$, by (1.3). If $x$ is represented by a divisor $D$ on $X_{/\mathbb{F}_p}$, then $p|D = (g_0)$ (mod $p\text{Div}^0(X_{/\mathbb{F}_p}))$, where $\text{Div}^0(X_{/\mathbb{F}_p})$ is the group of divisors of degree 0 on $X_{/\mathbb{F}_p}$. Since $p \nmid n$ and $\delta_\tau(n\eta(E)) = n\delta_\tau(\eta(E))$, $pD \equiv \delta_\tau(\eta(E))/\mathcal{P}_p$ (mod $p\text{Div}^0(X_{/\mathbb{F}_p})$). Hence the coefficients of $\delta_\tau(\eta(E))/\mathcal{P}_p$ are all divisible by $p$. But this contradicts the fact that $\eta(\mathcal{R}(E)) = \mathbb{Z}$. Hence $p \nmid \mathcal{C}_E$. This proves Proposition 1.9.

Let $J_{(\overline{\mathbb{F}_p}/\mathcal{P}_p)}$ be the Néron model of $J_{(\overline{\mathcal{P}_p})}$, resp. $C_E(\mathcal{P}_p)$ the scheme-theoretic closure of $C_{(\overline{\mathcal{P}_p})}$ in $J_{(\overline{\mathcal{P}_p})}$.

**Corollary 1.10.** With notation as above, $C_E[p]/\mathcal{P}_p(\mathbb{F}_p) \neq 0$.

**Proof.** Since the cusps of $X_1(N)$ are rational over $\mathbb{Q}(\zeta_N)$ and $p \nmid N$, $C_E$ is unramified at $p$. Thus $C_E[z_{\mathcal{P}_p}]$ is a Néron model of $C_E/\mathbb{Q}_p$ ([1, 7.1, Cor. 6]). By Prop. 1.9, there exists $x \in C_E[z_{\mathcal{P}_p}]$ of exact order $p$, where $K$ is the field of fractions of $\mathcal{O}$. Let $\tilde{x} \in C_E[z_{\mathcal{P}_p}](\mathcal{O})$ be the $\mathcal{O}$-valued point corresponding to $x$. Since $C_E[p]/\mathcal{P}_p$ is finite flat, the specialization lemma in [11, §1] shows that the specialization of $\tilde{x}$ to the special fiber has order $p$, so $C_E[p]/\mathcal{P}_p(\mathbb{F}_p) \neq 0$.

Next we determine the image of $C_E[p]/\mathcal{P}_p(\mathbb{F}_p)$ under $\varphi$.

**Lemma 1.11.** For any prime $l$ and any $E \in \mathcal{E}_1$, we have

$$T_l^*(\delta_1(E)) = \delta_1(E|T_l)$$

where $T_l^*$ acts on $\delta_1(E)$ via its action on the cusps.

**Proof.** Let $\pi : X(N) \to X_1(N)$ be the natural projection. The induced map

$$\pi^* : \text{Div}^0(\text{cusps}(\Gamma)) \longrightarrow \text{Div}^0(\text{cusps}(\Gamma(N)))$$

is injective. It is easy to check that $\pi^*$ commutes with the actions of $T_l^*$. Thus it is enough to prove the lemma with $\Gamma = \Gamma(N)$. As $\{\phi(x,y) : (x,y) \in (\mathbb{N}^{-1}\mathbb{Z}/\mathbb{Z})^2 - (0,0)\}$ spans the weight 2 Eisenstein series $E$ of level $N$ with $\mathcal{R}(E) \subset \mathbb{Q}$ over $\mathbb{Q}$, it suffices by Prop. 1.5 to prove the lemma for $E = \phi(x,y), (x,y) \in (\mathbb{N}^{-1}\mathbb{Z}/\mathbb{Z})^2 - (0,0)$, and all primes $l$. For $l \nmid N$, the lemma follows from [21, 1.3.2, 2.4.7, 3.2.1].
Suppose now \( l|N \). We have the double coset decomposition:

\[
\Gamma \left( \begin{array}{cc} l & 0 \\ 0 & 1 \end{array} \right) \Gamma = \bigcup_{k=0}^{l-1} \left( \begin{array}{cc} l & 0 \\ Nk & 1 \end{array} \right) \Gamma.
\]

So

\[
T_l^r \delta_{\Gamma}(\phi(x, y)) = \sum_{[r']} \left( \sum_{s \in \text{cusps}} r_{(s)}^{[r']} (\phi(x, y)) \right) \cdot \sum_{k=0}^{l-1} \left[ \frac{lr}{Nkr + s} \right]
\]

\[
= \sum_{[r']} \left( \sum_{s \in \text{cusps}} r_{(s)}^{[r']} (\phi(x, y)) \right) \left[ \frac{r}{s} \right]
\]

\[
= \sum_{[r']} \sum_{k=0}^{l-1} r_{[r + Nkr]}^{[r']} (\phi(x, y)) \left[ \frac{r}{s} \right],
\]

(1.11)

where the unindexed sum is over all \([r'] \in \text{cusps} = \text{cusps}(\Gamma(N))\) such that \([r']_{Nkr'+s'} = [r]_s\) for some \(0 \leq k \leq l - 1\). Let \( S = \{[r] \in \text{cusps} : l \nmid r \} \) and \( S' = \text{cusps} - S \). We split the sum over \([r]\) in (1.11) into two sums \(\Sigma_1\) and \(\Sigma_2\) over \(S\) and \(S'\) respectively. By [21, Props. 2.4.1(a), 2.4.2(a)], \(a_0(\phi(x, y)|\gamma_{[r]}) = \frac{1}{2}B_2(rx + sy)\), where \(B_2(t)\) is the second Bernoulli function. We remark that \(B_2(t)\) is periodic with period 1. So from (1.4),

\[
r_{[r]}^{[r]}(\phi(x, y)) = \frac{1}{2}B_2(rx + sy).
\]

(1.12)

For \([r] \in S\) we have \([r+Nkr]_{ls} = [r]_{ls}\), so

\[
r_{[r+Nkr]}^{[r]}(\phi(x, y)) = r_{[r]}^{[r]}(\phi(x, y)) = \frac{1}{2}r^{[r]}l^2 e([r]_{ls})B_2(rx + lsy) = \frac{1}{l}e([r]_{s})a_0(\phi(x, ty)|\gamma_{[r]})
\]

\[
= \frac{1}{l}r_{[r]}^{[r]}(\phi(x, ty))
\]

since \(e([r]_{ls}) = e([r]_{s})/l\) for \(l|N\) and since \(l \nmid r\). Hence

\[
\Sigma_1 = \sum_{[r] \in S} r_{[r]}^{[r]}(\phi(x, ty)) \left[ \frac{r}{s} \right].
\]

(1.13)

For \([r] \in S'\) we have \([r+Nkr]_{ls} = [r/l+Nks/l]_{s}\), so by (1.12)

\[
\Sigma_2 = l \sum_{[r] \in S'} \sum_{k=0}^{l-1} e([r]_{s}) \frac{1}{2}B_2(rx/l + Nks/l + sy) \left[ \frac{r}{s} \right].
\]

(1.14)

Write \(x = a/N_2\) with \(N_2|N\) and \((a, N_2) = 1\). We now divide into two subcases according as \(l\) divides \(N/N_2\) or not. Suppose first \(l \nmid (N/N_2)\). Then \(l \nmid a\), so

\[
\phi(x, y)|T_l = \phi(x, ty) = \sum_{k=0}^{l-1} \sum_{j=0}^{l-1} \phi((x+j)/l, y+k/l).
\]

(1.15)
For $[\gamma] \in S'$, $0 \leq k \leq l-1$ and $0 \leq j \leq l-1$, we have

$$r_{[\gamma]}(\phi((x+j)/l, y+k/l)) = e(\frac{r}{s}) \frac{1}{2} B_2 \left( \frac{x+j}{l} r + \left( y + \frac{k}{l} \right) s \right)$$

$$= e(\frac{r}{s}) \frac{1}{2} B_2 \left( \frac{xr}{l} + ys + \frac{ks}{l} \right).$$

(1.17)

Putting (1.11), (1.13), (1.15)-(1.17) together, we have $T_i^* \delta_T(\phi_{(x,y)}) = \delta_T(\phi_{(x,y)}|T_l)$ for $l \mid (N/N_2)$.

Suppose now $l|(N/N_2)$. The proof of [21, Prop. 2.4.7] shows that

$$\phi_{(x,y)}|T_l = l \sum_{k=0}^{l-1} \phi_{((x+k)/l, y)}.$$  

(1.18)

By (1.13), [21, Prop. 2.4.2(b)] and (1.12), we have

$$\Sigma_1 = \sum_{[\gamma] \in S} \sum_{k=0}^{l-1} \sum_{j=0}^{l-1} r_{[\gamma]}(\phi((x+k)/l, y+j/l)) \left[ \frac{r}{s} \right]$$

$$= \sum_{[\gamma] \in S} e(\frac{r}{s}) \sum_{k=0}^{l-1} \sum_{j=0}^{l-1} \frac{1}{2} B_2 (rx/l + sy + kr/l + sj/l).$$

(1.19)

As $k$ and $j$ run through $\{0, 1, \ldots, l-1\}$, $kr + sj \pmod{l}$ runs through $\{0, 1, \ldots, l-1\}$ $l$ times. Thus (1.19) and (1.12) give

$$\Sigma_1 = l \sum_{[\gamma] \in S} e(\frac{r}{s}) \sum_{k=0}^{l-1} \frac{1}{2} B_2 (rx/l + k/l + sy) \left[ \frac{r}{s} \right]$$

$$= l \sum_{[\gamma] \in S} \left[ \sum_{k=0}^{l-1} r_{[\gamma]}(\phi((x+k)/l, y)) \right] \left[ \frac{r}{s} \right].$$

(1.20)

On the other hand, (1.14) and (1.12) give

$$\Sigma_2 = l^2 \sum_{[\gamma] \in S'} e(\frac{r}{s}) \sum_{k=0}^{l-1} \frac{1}{2} B_2 (rx/l + sy) \left[ \frac{r}{s} \right]$$

$$= l \sum_{k=0}^{l-1} \sum_{[\gamma] \in S'} r_{[\gamma]}(\phi((x+k)/l, y)) \left[ \frac{r}{s} \right].$$

(1.21)

Combining (1.18), (1.20) and (1.21) gives $T_i^* \delta_T(\phi_{(x,y)}) = \delta_T(\phi_{(x,y)}|T_l)$. This proves Lemma 1.11.

Observe that since $\mathcal{P}(E)$ and $\mathcal{R}(E)$ are fractional ideals of $\mathbb{Q}[e_1, e_2]$, $A_E$ and by duality $C_E$ have natural $\mathbb{Z}[e_1, e_2]$-module structures. The composite map (1.5) is a $\mathbb{Z}[e_1, e_2]$-module map with respect to these structures. If $x \in C_E$ is represented by $\eta(\delta_T(E))$ with $\eta \in \mathcal{R}(E)^*$, then Lemma 1.11 shows that $T_i^* x$ is represented by $\eta(\delta_T(E|T_l)) = \eta(b_i \delta_T(E))$, where $b_i$ is the eigenvalue of $T_i$ on $E$. Hence $T_i^*$ acts by multiplication by $b_i$ on $C_E$. 

\[ \square \]
Proposition 1.12. Under the same assumptions as in Proposition 1.9, the image of $C_E[p]_{\mathbb{Z}_p}(\mathbb{F}_p) \otimes_{\mathbb{F}_p} \mathbb{F}_p$ under $\varphi$ is the $\mathbb{F}_p$-module generated by $\overline{f}$.

Proof. Let $\eta \in \mathcal{R}(E)^*$. Choose $r \in \mathbb{Z}$ such that $r(\overline{\theta}(\eta(\delta_T(E))))$ is of order dividing $p$. Here $\overline{\theta}(\cdot)$ means the specialization to the special fiber of the $\mathcal{O}$-valued point of $C_E/\mathbb{Z}_p$ corresponding to $\theta(\cdot)$. By Prop. 1.2 and Lemma 1.11, we have for each prime $l$,

$$
\varphi(r\overline{\theta}(\eta(\delta_T(E))))|_{\mathbb{T}_l} = \varphi(r\overline{\theta}(\eta(\delta_T(E)))) = b_l\varphi(r\overline{\theta}(\eta(\delta_T(E)))) = a_l\varphi(r\overline{\theta}(\eta(\delta_T(E)))).
$$

It follows that $\varphi(r\overline{\theta}(\eta(\delta_T(E)))) = \epsilon \cdot \overline{f}$ for some $\epsilon \in \mathbb{F}_p$. Since $C_E[p]_{\mathbb{Z}_p}(\mathbb{F}_p) \neq 0$ by Cor. 1.10 and $\eta \in \mathcal{R}(E)^*$ was arbitrary, $\varphi \left( C_E[p]_{\mathbb{Z}_p}(\mathbb{F}_p) \otimes \mathbb{F}_p \right) = \mathbb{F}_p \cdot \overline{f}$. \qed

We can now complete the proof of Theorem 0.4. By Propositions 1.3, 1.12 and the injectivity of $\varphi$, we have $A_f[p]_{\mathbb{Z}_p}(\mathbb{F}_p) \otimes \mathbb{F}_p = C_E[p]_{\mathbb{Z}_p}(\mathbb{F}_p) \otimes \mathbb{F}_p$, hence $A_f[p]_{\mathbb{Z}_p}(\mathbb{F}_p) = C_E[p]_{\mathbb{Z}_p}(\mathbb{F}_p)$. Since the special fiber of $(A_f[p] \cap C_E)/\mathbb{Z}_p$ is $A_f[p]_{\mathbb{Z}_p} \cap C_E/\mathbb{Z}_p$, it follows that $A_f[p] \cap C_E \neq 0$. This proves Theorem 0.4.

2. Cyclic isogenies of modular elliptic curves

In this section, we prove Theorem 0.3. Let $A_1$ be an optimal curve over $\mathbb{Q}$ of conductor $N$. Let $p > 2$ be a prime where $A_1$ has good ordinary reduction and let $\beta : A_1 \to A$ be a cyclic $\mathbb{Q}$-isogeny of degree divisible by $p$. Let $\epsilon : G_Q \to \text{Aut}(\ker(\beta[p]))$ be the character giving the action of $G_Q$ on $\ker(\beta[p])$ and $\chi$ the Teichmüller character giving the action of $G_Q$ on $\mu_p$. Consider the following three cases:

1. $\epsilon = 1$,
2. $\epsilon = \chi$,
3. $\epsilon \neq 1, \chi$.

We shall show that if $p > 7$, the first two cases do not occur and $\beta$ is étale at $p$ in the last case.

2.1. Reduction to $\epsilon \neq 1, \chi$. If $\epsilon = 1$, then $\ker(\beta[p]) \subset A(\mathbb{Q})_{\text{tors}}$. By Mazur’s classification theorem [11, Thm. 2], this implies $p \leq 7$. Thus if $p > 7$, this case cannot occur.

Suppose next $\epsilon = \chi$, so $\ker(\beta[p]) \cong \mu_p$. Let $A' = A_1/\ker(\beta[p])$ and let $\beta' : A_1 \to A'$ be the natural isogeny. By [13, §15, Thm. 1], the kernel of the dual isogeny $\beta' : A' \to A_1$ is the Cartier dual of $\ker(\beta[p])$ and so is isomorphic to $\mathbb{Z}/p\mathbb{Z}$ as $G_Q$-module. This implies that $p \mid \#A'(\mathbb{Q})_{\text{tors}}$. By Mazur’s classification theorem again, this cannot happen if $p > 7$.

We assume, henceforth, $\epsilon \neq 1, \chi$. Let $\rho : G_Q \to \text{Aut}(A_1[p]) \cong \text{GL}_2(\mathbb{F}_p)$ be the Galois representation on the $p$-torsion points of $A_1$. Then with respect to a suitable basis, we have

$$
\rho \sim \begin{pmatrix} \epsilon & * \\ 0 & \epsilon' \end{pmatrix}
$$

for some character $\epsilon' : G_Q \to \mathbb{F}_p^*$. The Weil pairing shows that $\det(\rho(\text{Frob}_l)) \equiv l \pmod{p}$ for any prime $l \nmid Np$, where $\text{Frob}_l$ is a Frobenius element of $G_Q$ for $l$. It
follows from our assumption $\epsilon \neq 1, \chi$ that $\epsilon' \neq 1$. Since $A_1$ is ordinary at $p$, there is an exact sequence of finite flat group schemes over $\mathbb{Z}_p$

$$0 \to A_1[p]_0^0 \to A_1[p]_{/\mathbb{Z}_p} \to A_1[p]_0^\text{ét}_{/\mathbb{Z}_p} \to 0,$$

where the flanking terms are each of order $p$ such that the inertia group $I_p$ acts via $\chi$ on the $G_{\mathbb{Q}_p}$-module associated to $A_1[p]_0^0$ and acts trivially on that associated to $A_1[p]_0^\text{ét}_{/\mathbb{Z}_p}$. It follows that exactly one of $\epsilon$ and $\epsilon'$ is unramified at $p$. The next two lemmas show that we may assume $\epsilon'$ is unramified at $p$.

**Lemma 2.1.** Let $\beta : A \to A'$ be a cyclic $\mathbb{Q}$-isogeny of elliptic curves over $\mathbb{Q}$. Suppose $A$ has good reduction at $p$ and $\ker \beta[p^\infty](\overline{\mathbb{Q}})$ is unramified at $p$. Then $\beta$ is étale at $p$.

**Proof.** Let $\beta_p : A_{/\mathbb{Z}_p} \to A'_{/\mathbb{Z}_p}$ be the extension of $\beta$ to Néron models over $\mathbb{Z}_p$. To show that $\beta_p$ is étale, we have to show that it is flat and unramified. Note that $\beta_p$ is quasi-finite and flat [1, 7.3, Lemmas 1, 2]. We check that it is unramified at points of residue characteristic $p$. The kernel $\ker \beta_p$ of $\beta_p$ is a finite flat group scheme over $\mathbb{Z}_p$. Let $K$ be the extension of $\mathbb{Q}_p$ cut out by $\ker \beta_p(\overline{\mathbb{Q}_p})$ and let $\mathcal{O}$ denote its ring of integers. Since $A$ has good reduction at $p$, $A[m]$ is unramified at $p$ for all $m$ prime to $p$ by the Néron-Ogg-Shafarevich criterion. By the assumption on $\ker \beta[p^\infty](\overline{\mathbb{Q}})$, $\ker \beta(\overline{\mathbb{Q}_p})$ is unramified as $G_{\mathbb{Q}_p}$-module. Thus $\ker \beta_p$ is a Néron model of $\ker \beta_p(\mathbb{Q}_p)$ ([1, 7.1, Cor. 6]). Let $x \in \ker \beta_p(\mathcal{O})$ be the $\mathcal{O}$-valued point corresponding to a generator of $\ker \beta_p(K)$. By the specialization lemma in [11, §1], the order of the specialization of $x$ to the residue field of $\mathcal{O}$ equals the order of $x$. So if $\overline{\beta}_p$ is the reduction of $\beta_p$ mod $p$, then

$$\# \ker \overline{\beta}_p = \# \ker \beta = \deg \beta = \deg \overline{\beta}_p.$$ 

By [20, 4.10(a)], $\# \ker \overline{\beta}_p$ equals the degree of separability $\deg_s \overline{\beta}_p$ of $\overline{\beta}_p$. So $\deg_s \overline{\beta}_p = \deg \overline{\beta}_p$; hence $\overline{\beta}_p$ is separable and unramified by [20, 4.10(c)]. This proves that $\beta_p$ is étale. $\square$

**Lemma 2.2.** Let $\beta : A \to A'$ be a cyclic $\mathbb{Q}$-isogeny of degree $d$ divisible by $p$. Suppose $A$ has good ordinary reduction at $p$ and $\ker \beta[p]$ is unramified at $p$. Then $\ker \beta[p^\infty]$ is unramified at $p$.

**Proof.** Let $\epsilon_1$ be the Galois character on $\ker \beta[p^\infty]$. Write $\epsilon_1 \oplus \epsilon_2$ for the semi-simplification of the Galois representation $\rho : G_{\mathbb{Q}} \to \text{Aut}(A[p^r])$, where $\epsilon_2$ is some Galois character and $p^r \| d$. Since $p$ is ordinary, one of the characters $\epsilon_1$ and $\epsilon_2$ is unramified at $p$ and the other when restricted to $I_p$ is the cyclotomic character on $\mu_{p^r}$. By our assumption, $\epsilon_1$ (mod $p$) is unramified at $p$. Since $p > 2$, $\epsilon_1$ is unramified at $p$. This proves the lemma. $\square$

If $\epsilon$ is unramified at $p$, then by Lemma 2.2, $\ker \beta[p^\infty]$ is unramified at $p$. Thus $\beta$ is étale at $p$ by Lemma 2.1, hence Theorem 0.3. So we assume, from now on,

$$\epsilon$$

is ramified at $p$.

Let $\pi : X_1(N) \to A_1$ be a modular parametrization and let $f$ be the associated weight 2 normalized newform on $\Gamma_1(N)$. Write

$$f(z) = \sum_{n=1}^{\infty} a_n q^n, \quad q = e^{2\pi iz}, \quad z \in \mathfrak{H}$$

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use
for the $q$-expansion of $f$ at the cusp $\infty$. We show that there is a weight 2 Eisenstein series $E$ on $\Gamma_1(N)$ associated to $\rho$ such that $\Psi$ is an Eisenstein prime for $E$ and $f$ (Prop. 2.6). Applying Theorem 0.4 and the classification theorem of rational cyclic isogenies of elliptic curves over $\mathbb{Q}$, we deduce that $p \leq 5$ (§2.3).

2.2. **Eisenstein series associated to** $\rho$. Let $\chi_1$ and $\chi_2$ be two Dirichlet characters, not necessarily primitive, modulo $N_1$ and $N_2$ respectively. Put

$$G(a_1, a_2; a_1, a_2) = \frac{1}{N_2} \sum_{t \in N_2^{-1}Z/Z} e^{2\pi i (-ta_2)} E(z; a_1, t; a_1, a_2^{-1})$$

and

$$(2.4) \quad E(\chi_1, \chi_2) = \frac{1}{2} \sum_{a_1=0}^{N_1-1} \sum_{a_2=0}^{N_2-1} \chi_1(a_1) \chi_2(a_2) G(a_1, a_2; N_1Z, Z)$$

where $E(z; a_1, a_2; a_1, a_2)$ is as in (1.7).

**Proposition 2.3.** Notation being as above, assume that not both $\chi_1$ and $\chi_2$ are the trivial character of any conductor. Then

(a) $E(\chi_1, \chi_2)$ is a weight 2 Eisenstein series on $\Gamma_0(N_1N_2)$ of character $(\chi_1\chi_2)^{-1}$.

(b) The Dirichlet series $L(E, s) := \sum_{n=1}^{\infty} b_n n^{-s}$ of $E(\chi_1, \chi_2)$ is

$$L(\chi_1, s)L(\chi_2, s - 1),$$

where $b_n$ is the $n$-th Fourier coefficient of $E(\chi_1, \chi_2)$ at $\infty$.

(c) If $\chi_1 \neq 1$, then the constant term of the Fourier expansion of $E(\chi_1, \chi_2)$ at $\infty$ is 0.

**Proof.** (a) and (b) follow from [19, Prop. 3.4] for Artin characters of degree 1 of totally real number fields of degree $> 1$. But, as remarked in [25, §1.5], the same result holds for $\mathbb{Q}$ if $\chi_1$ and $\chi_2$ are not both the trivial character of any conductor. (c) follows from the Fourier expansion of $E(z; a_1, a_2; N_1Z, Z)$ in (1.8), the definition of $E(\chi_1, \chi_2)$ in (2.4), and the assumption that $\chi_1 \neq 1$.

**Remark 2.4.** Using (1.8), we find that the Fourier expansion of $E(\chi_1, \chi_2)$ at $\infty$ is

$$(2.5) \quad E(\chi_1, \chi_2)(z) = \sum_{c=1}^{\infty} \sum_{b=1}^{\infty} \chi_1(c) \chi_2(b) e^{2\pi i (bcz)}.$$

From this, we can deduce Prop. 2.3(b) in a similar fashion to [21, Prop. 3.4.2(b)].

We want to apply Prop. 2.3 to certain Dirichlet characters associated to $\epsilon$ and $\epsilon'$ in (2.1) to get an Eisenstein series with suitable properties. For this, we consider the ramification behavior of the primes dividing $N$ in $\mathbb{Q}(A_1[p])/\mathbb{Q}$. For each prime $q$, let $T_q$ be the $q$-adic Tate module of $A_1$ and $V_q = T_q \otimes_{Z_q} \mathbb{Q}_q$. Let $H_q = H^1_{\text{et}}(A_1 \times \mathbb{Q} \leftarrow \mathbb{Q}_q)$. Then $V_q = H_q \otimes_{\mathbb{Q}_q} \mathbb{Q}_q(1)$, and the collection $\{H_q\}_q$ forms a compatible system $V$ of $q$-adic representations of $G_{\mathbb{Q}}$ whose $L$-function $L(V, s)$ is defined by an Euler product (for $\text{Re} \ s > \frac{3}{2}$):

$$L(V, s) = \prod_l L_l(V, s) = \prod_l \det(1 - \text{Frob}_l^{-1} l^{-s} (H_q)_l)^{-1},$$

where for each $l$, $q$ is a prime $\neq l$ and $(H_q)_l$ is the maximal subspace of $H_q$ on which $I_l$ acts trivially.
Let \( l \) be a prime dividing \( N \). Suppose \( l \| N \). Then \( A_1 \) has multiplicative reduction at \( l \). By [16, §1.12], there is an unramified extension \( K_l/Q_l \) of degree \( \leq 2 \) such that \( A_1 \) is isomorphic over \( K_l \) to the Tate curve \( E_q = \mathbb{G}_m/q^2 \) for some \( q \in \mathbb{Z}_l \) determined by the \( j \)-invariant of \( A_1 \). We have an exact sequence of \( G_{K_1} \)-modules for each \( n \):

\[
0 \to \mu_{p^n} \to A_1[p^n] \to \mathbb{Z}/p^n\mathbb{Z} \to 0.
\]

As \( p \) is given by (2.1), both \( \epsilon \) and \( \epsilon' \) are unramified at \( l \). On taking inverse limit over \( n \) and then tensoring with \( \mathbb{Q}_p \), (2.6) gives a (non-split) exact sequence of \( G_{K_1} \)-modules:

\[
0 \to \mathbb{Q}_p(1) \to V_p \to \mathbb{Q}_p \to 0.
\]

Thus \( G_{Q_l} \) acts via some character \( \psi_l \) of \( \text{Gal}(K_l/Q_l) \) on \( (V_p)_\text{f} \) (= the maximal quotient of \( V_p \) on which \( I_l \) acts trivially). From (2.1), \( \psi_l \equiv \epsilon|G_{Q_l} \) (mod \( p \)) or \( \psi_l \equiv \epsilon'|G_{Q_l} \) (mod \( p \)). Let \( S_1 = \{ l : l \| N, \psi_l \equiv \epsilon|G_{Q_l} \) (mod \( p \)) \} and \( S_2 = \{ l : l \| N, l \not\in S_1 \} \).

Suppose now \( l^2|N \). Then \( A_1 \) has additive reduction at \( l \). By [16, §5.6 Prop. 23b], the images of \( I_l \) under \( \epsilon \) and \( \epsilon' \) are cyclic of order 2, 3, 4 or 6. In particular, \( \epsilon \) and \( \epsilon' \) are ramified at \( l \).

Let \( f_{\epsilon_0,\text{prim}} \) and \( f_{\epsilon_0',\text{prim}} \) be the conductors of the primitive Dirichlet characters \( \epsilon_{0,\text{prim}} \) and \( \epsilon'_{0,\text{prim}} \) associated to \( \epsilon \) and \( \epsilon' \) respectively. Let \( \epsilon_{0,\text{prim}} \epsilon^{-1} \) be the primitive Dirichlet character such that \( \epsilon_{0,\text{prim}} = \epsilon_{0,\text{prim}} \epsilon^{-1} \cdot \chi \). Here we view \( \chi \) as both a character of \( G_{Q_l} \) and a Dirichlet character. Since \( \epsilon' \) is unramified at \( p \) (cf. (2.2)) and \( \epsilon(l) \epsilon'(l) \equiv 1 \) (mod \( p \)) for any \( l \nmid Np \), the conductor \( f_{\epsilon_{0,\text{prim}},\epsilon^{-1}} \) of \( \epsilon_{0,\text{prim}} \epsilon^{-1} \) is prime to \( p \). Now let \( \epsilon_0 \epsilon^{-1} \) (resp. \( \epsilon_0', \epsilon' \) ) be the Dirichlet character modulo \( f_{\epsilon_{0,\text{prim}},\epsilon^{-1}} \cdot \prod_{l \in S_2} l \) (resp. \( f_{\epsilon_{0,\text{prim}}'} = f_{\epsilon_{0,\text{prim}}'} = f_{\epsilon_{0,\text{prim}}'} \cdot \prod_{l \in S_1} l \) whose primitive character is \( \epsilon_{0,\text{prim}} \epsilon^{-1} \) (resp. \( \epsilon_{0,\text{prim}}', \epsilon'_{0,\text{prim}} \)). (For a Dirichlet character \( \psi \) modulo \( m \), we set \( \psi(n) = 0 \) if \( (n, m) \neq 1 \).)

**Lemma 2.5.**

(a) \( f_{\epsilon_{0,\epsilon^{-1}}}, f_{\epsilon'_{0,\epsilon'}}, f_{\epsilon_{0,\epsilon^{-1}}}, f_{\epsilon'_{0,\epsilon'}} \) divides \( N \).

(b) \( f_{\epsilon_{0,\epsilon^{-1}}} f_{\epsilon'_{0,\epsilon'}} \) and \( N \) have the same prime divisors.

**Proof.** (a) By a result of Carayol [2, 0.8], the level \( N \) of \( f \) is equal to the conductor of the \( p \)-adic representation \( V_p \). (For the definition of the latter, see for example [4, §1.1].) Put \( \Phi = \ker \beta[p] \) and \( \Phi' = A_1[p]/\Phi \). For any prime \( l \neq p \), we have

\[
dim_{\mathbb{F}_p} A_1[p]^{G_l} = \dim_{\mathbb{F}_p} \Phi^{G_l} + \dim_{\mathbb{F}_p} \Phi'^{G_l},
\]

where \( G_0 \supset G_1 \supset \cdots \) is the series of ramification groups in \( \text{Gal}(Q_l(A_1[p])/Q_l) \). Since \( \sum_{l=0}^{\infty}(G_0 : G_l)^{-1} \dim_{\mathbb{F}_p}(\Phi/\Phi^{G_l}) = \) the \( l \)-part of \( f_{\epsilon_{0,\text{prim}}} \) and similarly for \( \Phi' \) and \( \epsilon' \), the \( l \)-part of \( f_{\epsilon_{0,\text{prim}}} f_{\epsilon'_{0,\text{prim}}} \) divides \( N \). To see that the \( l \)-part of \( f_{\epsilon_{0,\epsilon^{-1}}} f_{\epsilon'_{0,\epsilon'}} \) divides \( N \), we need only consider the case \( l \| N \). In this case \( l \nmid f_{\epsilon_{0,\text{prim}}}, f_{\epsilon'_{0,\text{prim}}} \), so by the definition of \( f_{\epsilon_{0,\epsilon^{-1}}} f_{\epsilon'_{0,\epsilon'}} \) we have \( l \| f_{\epsilon_{0,\epsilon^{-1}}} f_{\epsilon'_{0,\epsilon'}} \). Hence \( f_{\epsilon_{0,\epsilon^{-1}}} f_{\epsilon'_{0,\epsilon'}} \) divides \( N \). This proves (a).

(b) Let \( l \) be a prime. If \( l \| N \), then \( l \| f_{\epsilon_{0,\epsilon^{-1}}} f_{\epsilon'_{0,\epsilon'}} \). If \( l^2 \| N \), then \( \epsilon \) and \( \epsilon' \) are both ramified at \( l \), so \( l \| f_{\epsilon_{0,\epsilon^{-1}}} f_{\epsilon'_{0,\epsilon'}} \). This proves (b). \( \square \)

We now apply Prop. 2.3 to \( \chi_1 = \epsilon_0 \) and \( \chi_2 = \epsilon_0 \epsilon^{-1} \) to get an Eisenstein series \( E = E(\epsilon_0, \epsilon_0 \epsilon^{-1}) \). (Recall that, under our assumption (2.2), \( \epsilon_0 \) and \( \epsilon_0 \epsilon^{-1} \) are both non-trivial.)
Proposition 2.6. The Fourier coefficients of the $q$-expansions of $E$ and $f$ at $\infty$ are congruent mod $\mathfrak{P}$:

$$E(q) \equiv f(q) \pmod{\mathfrak{P}}.$$  

Proof. By Prop. 2.3(b), the Euler factor $L_i(E, s)$ of $L(E, s)$ at a prime $l$ is $(1 - \epsilon_0'(l)l^{-s})^{-1}(1 - \epsilon_0\chi^{-1}(l)l^{1-s})^{-1}$. We have a formal Euler product for the Dirichlet series $L(f, s)$ of $f$:

$$L(f, s) = \prod_{l \mid N} L_l(f, s) = \prod_{l \mid N}(1 - a_l l^{-s})^{-1} \prod_{l \not\mid N}(1 - a_l l^{-s} + l^{1-2s})^{-1},$$  

where $a_l$ is the $l$-th Fourier coefficient of $f$ in (2.3). By [2], $L(f, s) = L(V, s)$.

For $l \nmid Np$, we have $\ell_0 l^{\epsilon_0'(l) - 1} = \ell_0 l^{\epsilon_0\chi^{-1}(l)} = L_l(E, s)$ (mod $\mathfrak{P}$).

Let $l \mid N$. Then $L_l(f, s) = (1 - a_l l^{-s})^{-1}$. Suppose $l \not\mid N$. Then $\ell_0 = 0$ and $L_l = 1$. Since $\epsilon_0'(l) = \epsilon_0\chi^{-1}(l) = 0$, $L_l(E, s) = 1$.

Finally, suppose $l = p$. Since $A_1$ is ordinary at $p$, $a_p$ is congruent mod $\mathfrak{P}$ to the eigenvalue of Frobenius on the $p$-adic Tate module of $A_1/\mathfrak{P}$. So we have

$$(1 - a_l l^{-s})^{-1} \equiv (1 - \epsilon^*(l) l^{-s})^{-1} \equiv L_l(E, s) \pmod{\mathfrak{P}},$$

where $\epsilon^* = \epsilon_0$ or $\epsilon_0'$ according as $l \in S_1$ or $l \in S_2$. Next suppose $l^2 \mid N$. Then $\ell_0 = 0$ and $L_l = 1$. Since $\epsilon_0'(l) = \epsilon_0\chi^{-1}(l) = 0$, $L_l(E, s) = 1$.

Hence $L_l(f, s)$ is congruent mod $\mathfrak{P}$ to $L_l(E, s)$ for each $l$. This shows that $a_n \equiv b_n$ (mod $\mathfrak{P}$) for each $n \geq 1$ and, together with Prop. 2.3(c), proves the proposition. 

We show that $E = E(\epsilon_0, \epsilon_0\chi^{-1})$ is a common eigenfunction for all $T_l$ and $(l)$.

Lemma 2.7. For any prime $l$, we have

(a) $E(l) = E$ if $l \nmid N$;
(b) $E(T_l) = (\epsilon_0'(l) l^{\epsilon_0\chi^{-1}(l)}) E$.

Proof. (a) Since $\epsilon_0'(l) l^{\epsilon_0\chi^{-1}(l)} = 1$ for all $l \nmid N$, $E$ is modular on $\Gamma_0(N)$ by Prop. 2.3(a). Hence $E(l) = E_{\mid\Gamma_0(N)}$.

(b) We use the $q$-expansion of $E$ at $\infty$ given by (2.5):

$$E(z) = \sum_{c=1}^{\infty} \sum_{b=1}^{\infty} \epsilon_0'(c) \epsilon_0\chi^{-1}(b) b y^{b c}, \quad q = e^{2\pi iz},$$

$$= \sum_{n=1}^{\infty} \sum_{c=1}^{\infty} \epsilon_0'(c) \epsilon_0\chi^{-1}(b) b y^n,$$

where $b_n = \sum_{bb=nn} \epsilon_0'(c) \epsilon_0\chi^{-1}(b) b$ for each $n \geq 1$. 


By Prop. 2.3(a), the level of $E$ divides $f_{\epsilon_0\chi^{-1}}f_\epsilon$, which has the same prime divisors as $N$ by Lemma 2.5. The action of $T_l$ on $E$ is then given by ([18, (3.5.12)]):

\begin{equation}
E|T_l = \sum_{n=1}^{\infty} b_{ln} q^n + l \sum_{n=1}^{\infty} b_n q^n, \quad l \nmid N,
\end{equation}

\begin{equation}
E|T_l = \sum_{n=1}^{\infty} b_{ln} q^n, \quad l|N.
\end{equation}

Suppose first $l \nmid N$. Then

\begin{equation}
b_{ln} = \sum_{bc=ln}^{b \mid l} e'_0(c) e_0 \chi^{-1}(b) b
\end{equation}

\begin{equation}
= \frac{1}{l} \sum_{bc=ln}^{b \mid l} e'_0(c) e_0 \chi^{-1}(b) b + l \sum_{bc=ln}^{b \mid l} e'_0(c) e_0 \chi^{-1}(b) b
\end{equation}

\begin{equation}
= e'_0(l) \sum_{bc=ln}^{b \mid l} e'_0(c') e_0 \chi^{-1}(b') b' + l e_0 \chi^{-1}(l) \sum_{b' c=ln}^{b' \mid l} e'_0(c) e_0 \chi^{-1}(b') b'.
\end{equation}

Since $e'_0(l) e_0(l) = \chi(l)$ for all $l \nmid N p$ and $p \nmid f_{\epsilon_0} f_{\epsilon_0\chi^{-1}}$, it follows that $e'_0(l) = e_0 \chi^{-1}(l^{-1})$ for all $l \nmid N$. So

\begin{equation}
b_{ln} = \frac{1}{l} \sum_{bc=ln}^{b \mid l} e'_0(c) e_0 \chi^{-1}(b) b
\end{equation}

\begin{equation}
= e_0 \chi^{-1}(l^{-1}) \sum_{bc=ln}^{b \mid l} e'_0(c) e_0 \chi^{-1}(b) b
\end{equation}

\begin{equation}
= e'_0(l) \sum_{bc=ln}^{b \mid l} e'_0(c) e_0 \chi^{-1}(b) b.
\end{equation}

(b) follows from (2.7), (2.9) and (2.10) for $l \nmid N$. For $l|N$, we have

\begin{equation}
b_{ln} = \begin{cases} 
\frac{l e_0 \chi^{-1}(l)}{2} b_n, & \text{if } l \nmid f_{\epsilon_0'}, \text{ and } l \nmid f_{\epsilon_0\chi^{-1}}, \\
\epsilon_0(l) b_n, & \text{if } l \mid f_{\epsilon_0\chi^{-1}}, \text{ and } l \nmid f_{\epsilon_0'}, \\
0, & \text{otherwise},
\end{cases}
\end{equation}

and (b) follows from (2.8).

\begin{flushright}
\hfill \Box
\end{flushright}

2.3. Completion of proof of Theorem 0.3 in the case $\epsilon \neq 1, \chi$. We can now complete the proof of Theorem 0.3 in this case, assuming (2.2). Applying Theorem 0.4 to $f$ and $E$, we have $A_1[p] \cap C_E \neq 0$. By [21, Thm. 3.2.4], $C_E$ is stable under the action of $G_Q$, which is given by $e'$. Since $\epsilon$ (resp. $e'$) is ramified (resp. unramified) at $p$, it follows that $\ker \beta[p]$ and $A_1[p] \cap C_E$ are two independent cyclic subgroups of order $p$ defined over $\mathbb{Q}$. Hence $A_1/\ker \beta[p]$ is an elliptic curve over $\mathbb{Q}$ which has a cyclic subgroup of order $p^2$ defined over $\mathbb{Q}$. Kenku [7, Thm. 1] has shown that the table in the introduction of [11] is a complete list of $d$ for which there is a rational cyclic $d$-isogeny of elliptic curves over $\mathbb{Q}$. This implies that $p \leq 5$. Thus if $p > 7$, $\epsilon$ is unramified at $p$. This completes the proof of Theorem 0.3.
3. Integrality of \( \mathbb{p} \)-adic \( L \)-functions

We now apply Theorem 0.3 to establish Theorem 0.2. We shall use the following result of Stevens.

**Theorem 3.1.** ([23, Thm. 4.6]) Suppose \( p > 2 \). Let \( \pi : X_1(N) \to A \) be a modular parametrization and \( c(\pi) \) the Manin constant of \( \pi \). Then \( c(\pi)\nu_{A,\Delta} \) takes values in \( \mathcal{L}(A) \otimes \mathbb{Z}_p \).

To prove Theorem 0.2, it suffices by Theorem 3.1 to show that there is a modular parametrization \( \pi : X_1(N) \to A \) such that \( c(\pi) \) is a \( p \)-unit. Let \( A \) be the \( \mathbb{Q} \)-isogeny class of elliptic curves over \( \mathbb{Q} \) containing \( A \). Let \( A_1 \) be the optimal curve in \( A \) and \( \pi_1 : X_1(N) \to A_1 \) an optimal parametrization (cf. the introduction). Let \( n \) be the largest square dividing \( N \).

**Proposition 3.2.** With notation as above, \( c(\pi_1) \in \mathbb{Z}[1/2n]^* \).

**Proof.** The analogous result for a strong parametrization \( \pi_0 : X_0(N) \to A_0 \) (which takes the cusp \( \infty \) to the origin of \( A_0 \)) of the strong Weil curve \( A_0 \in A \) has been proved in [11, Cor. 4.1] by showing that \( \pi_0 : X_0(N)^{\text{smooth}}/\mathbb{Z}[\pi_1] \to A_0/\mathbb{Z}[\pi_1] \) is a formal immersion along the \( \infty \)-section, where \( X_0(N)^{\text{smooth}}/\mathbb{Z}[\pi_1] \) is the smooth locus of \( X_0(N)/\mathbb{Z}[\pi_1] \to \text{Spec} \mathbb{Z} \). An analysis of the arguments used there shows that for an optimal parametrization \( \pi_1 : X_1(N) \to A_1 \) which takes the cusp \( 0 \) to the origin of \( A_1 \), \( \pi_1 : X_1(N)^{\text{smooth}}/\mathbb{Z}[\pi_1] \to A_1/\mathbb{Z}[\pi_1] \) is a formal immersion along the \( 0 \)-section. Since \( X_1(N)/\mathbb{Z}[\pi_1] \) is irreducible if \( l \nmid N \) and since the Atkin-Lehner involution \( w_N \) interchanges the two irreducible components of \( X_1(N)/\mathbb{Z}[\pi_1] \) if \( l \mid N \), we have \( c(\pi_1) \in \mathbb{Z}[1/\pi_1]^* \). \( \square \)

**Lemma 3.3.** Let \( X \xrightarrow{f} Y, Y \xrightarrow{g} Z \) be morphisms of schemes. Suppose that \( f \) is smooth. Then there is an exact sequence of \( \mathcal{O}_X \)-modules

\[
0 \to f^*\Omega^1_{Y/Z} \to \Omega^1_{X/Z} \to \Omega^1_{X/Y} \to 0,
\]

where \( \Omega^1_{X/Y} \) is the sheaf of relative differentials of degree 1 of \( X \) over \( Y \) and similarly for \( \Omega^1_{Y/Z} \) and \( \Omega^1_{X/Z} \), and \( X \) is considered as a \( Z \)-scheme via \( g \circ f \).

**Proof.** See [1, 2.2 Prop. 5(b)] and the remark after it. \( \square \)

**Corollary 3.4.** Let \( \beta : A \to A' \) be a \( \mathbb{Q} \)-isogeny of elliptic curves over \( \mathbb{Q} \) \( \text{étale at } p \). Let \( \Omega^1_{A/\mathbb{Z}_p} \) and \( \Omega^1_{A'/\mathbb{Z}_p} \) be the sheaves of Néron differentials on \( A/\mathbb{Z}_p \) and \( A'/\mathbb{Z}_p \) respectively. Then \( \beta \) induces an isomorphism

\[
\beta^* : H^0(A'/\mathbb{Z}_p, \Omega^1_{A'/\mathbb{Z}_p}) \cong H^0(A/\mathbb{Z}_p, \Omega^1_{A/\mathbb{Z}_p}).
\]

**Proof.** Since \( \beta \) is \( \text{étale at } p \), \( \beta/\mathbb{Z}_p \) is smooth and \( \Omega^1_{A/\mathbb{Z}_p}/\mathbb{Z}_p \) is smooth. So the exact sequence in Lemma 3.3 gives \( \beta^*\Omega^1_{A'/\mathbb{Z}_p} \cong \Omega^1_{A/\mathbb{Z}_p} \). Hence \( H^0(A'/\mathbb{Z}_p, \Omega^1_{A'/\mathbb{Z}_p}) \cong H^0(A/\mathbb{Z}_p, \Omega^1_{A/\mathbb{Z}_p}) \). \( \square \)

We can now prove Theorem 0.2. As remarked above, it suffices to show that there is a modular parametrization \( \pi : X_1(N) \to A \) such that \( c(\pi) \) is a \( p \)-unit. We show that a modular parametrization \( \pi : X_1(N) \to A \) of minimal degree meets this requirement. By the definition of optimality, there is a \( \mathbb{Q} \)-isogeny \( \beta : A_1 \to A \)
such that \( \pi = \beta \circ \eta_1 \). We have \( \deg \pi = \deg \beta \deg \eta_1 \). It follows that \( \deg \beta \) is
minimal among all isogenies from \( A_1 \) to \( A \). Thus \( \beta \) must be cyclic. Let \( \omega_A \) and
\( \omega_A \) be Néron differentials on \( A_1 \) and \( A \) respectively, and let \( c(\beta) \in \mathbb{Z} \) be such that
\( \beta^* \omega_A = c(\beta) \omega_A \). If \( p \nmid \deg \beta \), then \( p \nmid c(\beta) \). If \( p | \deg \beta \), then \( \beta \) is étale at \( p \) by
Theorem 0.3, and so \( p | c(\beta) \) by Corollary 3.4. Since \( c(\pi) = c(\beta)c(\eta_1) \) and \( c(\eta_1) \) is
a \( p \)-unit by Prop. 3.2, \( c(\pi) \) is a \( p \)-unit. This completes the proof of Theorem 0.2.

References

1. S. Bosch, W. Lütkebohmert and M. Raynaud, Néron Models, Ergeb. der Math. und ihrer
2. H. Carayol, Sur les représentations l-adiques associées aux formes modulaires de Hilbert,
3. P. Cartier, Une nouvelle opération sur les formes différentielles, C. R. Acad. Sc. Paris 244
(1957), 426-428. MR 18:708b
4. J. Coates and C.-G. Schmidt, Iwasawa theory for the symmetric square of an elliptic curve,
5. P. Deligne and M. Rapoport, Les schémas de modules de courbes elliptiques, Lecture Notes
6. H. Hida, On congruence divisors of cusp forms as factors of the special values of their zeta
functions, Invent. Math. 64 (1981), 221-262. MR 83h:10066
7. M.A. Kenku, On the number of \( \mathbb{Q} \)-isomorphism classes of elliptic curves in each \( \mathbb{Q} \)-isogeny
Mat. 36 (1972), 19-65 (Russian); English transl. in Math. USSR-Izv. 6 (1972), 19-64. MR 47:3396
MR 50:7152
(1977), 33-186. MR 80c:14015
12. B. Mazur, J. Tate and J. Teitelbaum, On \( p \)-adic analogues of the conjectures of Birch and
Math. 100 (1990), 431-476. MR 91g:11066
Topología Algebraica, Universidad Nacional Autónoma de México, 1958, pp. 24-53. MR 20:4559
15 (1972), 259-331. MR 52:8126
17. G. Shimura, Reduction of algebraic varieties with respect to a discrete valuation ring of the
basic field, Amer. J. Math. 77 (1955), 134-176. MR 16:616d
18. G. Shimura, Introduction to the Arithmetic Theory of Automorphic Functions, Iwanami
19. G. Shimura, The special values of the zeta functions associated with Hilbert modular forms,
MR 87b:10050
291 (1985), 519-550. MR 87a:11056
23. G. Stevens, Stickelberger elements and modular parametrizations of elliptic curves, Invent.
Math. 98 (1989), 75-106. MR 90m:11089
24. A. Wiles, Modular curves and the class group of \( \mathbb{Q}(\zeta_p) \), Invent. Math. 58 (1980), 1-35. MR 82j:12009


Department of Mathematics and Statistics, McMaster University, Hamilton, Ontario, Canada L8S 4K1

Current address: Department of Mathematics, The University of Hong Kong, Pokfulam Road, Hong Kong