NONVANISHING OF L-VALUES

HARUZO HIDA

Contents

This series of two lecture is an introductory discussion of problems concerning nonvanishing of L-values modulo p. Nonvanishing result has seen powerful applications in divisibility problems of class numbers (see [W1], [FW] and [ICF] Chapter 7) and in many proofs of the main conjectures in Iwasawa's theory. Recently, new methods of proving nonvanishing emerged in the work of Vatsal, Finis and myself. In these two lectures, we describe a geometric method, which was stared by Sinnott in [Si] and [Si1] and has been generalized in [H04], [H06a] and [H06b] via the theory of Shimura varieties.

Date: June 24, 2006.

Two lectures at Columbia university 6/17-18/2006; the author is partially supported by the following NSF grant: DMS 9988043 and DMS 0244401.

1. Dirichlet L-values modulo p

1.1. **Statement of the theorem for Dirichlet L-values.** We consider the group scheme $\mathbb{G}_m = Spec(\mathbb{Z}[t, t^{-1}])$. We fix a Dirichlet character λ of $(\mathbb{Z}/N\mathbb{Z})^\times$ with $\lambda(-1) = -1$ and two embeddings $\mathbb{C} \overset{i_\infty}{\hookleftarrow} \overline{\mathbb{Q}} \overset{i_p}{\hookrightarrow} \overline{\mathbb{Q}}_p$. We regard λ to have values in any one of the three fields. Consider a rational function:

$$\Phi(t) = \Phi_\lambda(t) = \sum_{n=1}^{\infty} \lambda(n)t^n = \frac{\sum_{a=1}^{N} \lambda(a)t^a}{1 - t^N} \in \mathbb{Z}[t, t^{-1}]_{(p,t-1)} = \mathcal{O}_{\mathbb{G}_m,1}.$$

Since the numerator $\sum_{a=1}^{N} \lambda(a)t^a$ is divisible by $(t-1)$, the rational function Φ is finite at $t = 1$. As Euler discovered in 1735,

$$\Phi(1) = L(0, \lambda) \in \overline{\mathbb{Q}}.$$

Thus $L(0, \lambda)$ is a p–adic integer in the ring $\mathbb{Z}_p[\lambda]$ generated by the values of λ. Writing $\mathfrak{P}$ for the maximal ideal of the p–adic valuation ring of $\overline{\mathbb{Q}}_p$, the theorem of Washington can be stated as follows:

Theorem 1.1. *For almost all characters $\chi : \mathbb{Z}_\ell{}^\times \to \mu_{\ell^\infty}$, $L(0, \lambda\chi) \not\equiv 0 \mod \mathfrak{P}$.*

By Kummer's class number formula, we can relate this statement to the statement on the ℓ-power cyclotomic class number.

The automorphic proof of this theorem has several steps.

(Step1) *Hecke operators*: Introduction of Hecke operators $U(\ell)$ acting on rational functions on $\mathbb{G}_{m/\overline{\mathbb{F}}_p}$ and functions on μ_{ℓ^∞}.

(Step2) *Measure associated to $U(\ell)$-eigenforms*: Choose a sequence of generators ζ_n in μ_{ℓ^n} so that $\zeta_n^\ell = \zeta_{n-1}$ (for example, $\zeta_n = \exp\left(\frac{2\pi i}{\ell^n}\right)$). Fix an isomorphism $\mathbb{Z}_\ell \cong \mathbb{Z}_\ell(1) = \varprojlim_n \mu_{\ell^n}$ given by $\mu_{\ell^n} \ni \zeta_n^a \mapsto a \in \mathbb{Z}/\ell^n\mathbb{Z}$. For an eigenform $\phi|U(\ell) = a\phi$ with unit eigenvalue $a \in \overline{\mathbb{F}}_p^\times$, construction of a measure $d\mu_\phi$ on $\mathbb{Z}_\ell^\times$ with $\int_{a+\ell^n\mathbb{Z}_\ell} d\mu_\phi \doteqdot \phi(\zeta_n^a)$ for the image ζ_n^a of ζ^a in μ_{ℓ^n}. Here a measure μ on $\mathbb{Z}_\ell$ with values in $\overline{\mathbb{F}}_p$ is a $\overline{\mathbb{F}}_p$-linear functional defined on a space $\mathcal{C}(\mathbb{Z}_\ell; \overline{\mathbb{F}}_p)$ of continuous functions: $\mathbb{Z}_\ell \to \overline{\mathbb{F}}_p$. Thus $\mu : \mathcal{C}(\mathbb{Z}_\ell; \overline{\mathbb{F}}_p) \to \overline{\mathbb{F}}_p$ is an $\overline{\mathbb{F}}_p$-linear map.

(Step3) *Evaluation formula*: For a character $\chi : \Gamma = \mathbb{Z}_\ell^\times/\mu_{\ell-1} \to \overline{\mathbb{F}}_p^\times$:

$$L(0, \lambda\chi^{-1}) \doteqdot \int_{\mathbb{Z}_\ell^\times} \chi d\mu_\Phi = \int_\Gamma \chi d\mu_\Psi$$

for $\Psi(\zeta) = \sum_{\varepsilon \in \mu_{\ell-1}} \Phi(\zeta^\varepsilon)$ (not ζ^ε is defined only for $\zeta \in \mu_{\ell^\infty}$).

(Step4) *Zariski density*: Regard Ψ as induced from the rational function $\widetilde{\Psi}(t_\varepsilon) = \sum_{\varepsilon\in\mu_{\ell-1}/\{\pm1\}} (\Phi(t_\varepsilon) + \Phi(t_\varepsilon^{-1}))$ on $G = \mathbb{G}_m^{\mu_{\ell-1}/\{\pm1\}}$ by pull-back under the embedding $i : \mu_{\ell^\infty} \hookrightarrow G$ given by $\zeta \mapsto (\zeta^\varepsilon)$. The Zariski density of $i(\mu_{\ell^\infty})$ in a big subvariety in G defined by the equations of $\varepsilon \in \mu_{\ell-1}$ (for example, if $\ell = 5$, $-\varepsilon = \varepsilon^2 = -1$ for $\varepsilon = \sqrt{-1}$ gives $t_{\varepsilon^2}t_1 = 1$) implies the constancy of $\widetilde{\Psi}$ and hence of Φ (a contradiction) if $\int_{\mathbb{Z}_\ell^\times} \chi d\mu_\Phi = 0$ for infinitely many characters. The Zariski density is the idea of Sinnott [Si1].

We are going to describe each step.

1.2. **Hecke operators.** A little more generally, we start with μ_{ℓ^∞} over an integral domain B whose quotient field is K. Take an algebraic closure $\overline{K}$ of K. We suppose that ℓ is invertible in B and all ℓ-power roots of are in B. Fix a prime ℓ prime to p. Define a Hecke operator $U(\ell)$ acting on functions ϕ on μ_{ℓ^∞} by

$$\phi|U(\ell)(t) = \frac{1}{\ell}\sum_{\zeta\in\mu_\ell} \phi(\zeta t^{1/\ell}) = \frac{1}{\ell}\sum_{T^\ell=t} \phi(T).$$

Exercise 1.2. *Prove*

(1) $U(\ell^h) = U(\ell)^h$ *for* $h = 1, 2, \dots,$
(2) $a(n, \phi|U(\ell)) = a(n\ell, \phi)$ *if* $\phi(t) = \sum_{n\gg-\infty} a(n, \phi)t^n$ *is a rational function on* $\mathbb{G}_m$.

From this we conclude $\Phi|U(\ell) = \lambda(\ell)\Phi$. Hence Φ is a Hecke eigen function in

$$\mathcal{O}_{\mathbb{G}_m,1} = \{\phi \in \overline{\mathbb{F}}_p(\mathbb{G}_m)|\phi \text{ is finite at } 1\} \quad (\text{the stalk of } \mathcal{O}_{\mathbb{G}_m} \text{ at } 1).$$

1.3. **Measure associated to a $U(\ell)$-eigen function.** Since $\mathbb{Z}_\ell(1)$ is compact, any continuous function $f : \mathbb{Z}_\ell(1) \to \overline{\mathbb{F}}_p$ is a locally constant function. For a measure $\mu : \mathcal{C}(\mathbb{Z}_\ell(1); \overline{\mathbb{F}}_p) \to \overline{\mathbb{F}}_p$, we often write $\int_U f\chi_U d\mu$ for $\mu(f\chi_U)$ for the characteristic function χ_U of an open set $U \subset \mathbb{Z}_\ell(1)$.

Fix an identification $\mathbb{Z}_\ell(1) \cong \mathbb{Z}_\ell$, which is equivalent to choose a primitive ℓ^n-th root ζ_n so that $\zeta_{n+1}^\ell = \zeta_n$. Fix a positive integer h. We have a coset decomposition

$$\mathbb{Z}_\ell(1) = \bigsqcup_{z \mod \ell^{hn}} \zeta_{hn}^z \mathbb{Z}_\ell(1)^{\ell^{hn}} = \bigsqcup_{z \mod \ell^{hn}} (z + \ell^{hn}\mathbb{Z}_\ell)$$

for every n. The measure μ is determined by assigning the value $\Phi(\zeta_{hn}^z) = \int_{\zeta_{hn}^z\mathbb{Z}_\ell(1)^{\ell^{hn}}} d\mu$ to $\zeta_{hn}^z\mathbb{Z}_\ell(1)^{\ell^{hn}}$. To be well defined, these values have to satisfy the following distribution relation for $n = 1, 2, \dots, \infty$:

(Dist1)

$$\Phi(\zeta_{hn}^w) = \int_{\zeta_{hn}^w \mathbb{Z}_\ell(1)^{\ell^{hn}}} d\mu = \sum_{z \equiv w \mod \ell^{h(n+1)}, z \in \mathbb{Z}/\ell^{h(n+1)}\mathbb{Z}} \int_{\zeta_n^z \mathbb{Z}_\ell(1)^{\ell^{h(n+1)}}} d\mu$$

$$= \sum_{z \equiv w \mod \ell^{h(n+1)}} \Phi(\zeta_{h(n+1)}^z) = \sum_{\zeta \in \mu_{\ell^{h(n+1)}}, \zeta^{\ell^h} = \zeta_{hn}^w} \Phi(\zeta) = \ell^h \Phi | U(\ell^h)(\zeta_{hn}^w).$$

In other words, if $\phi | U(\ell^h) = a\phi$ with $a \neq 0$, we can take $\Phi(\zeta_{nh}^z) = \ell^{-nh} a^{-h} \phi(\zeta_{nh}^z)$, and get a measure μ_ϕ.

Let $B = \overline{\mathbb{F}}_p$ or $\overline{\mathbb{Q}}_p$. Let $\mathcal{O}_{\mathbb{G}_m, 1/B} = \{\phi \in B(\mathbb{G}_m) | \phi \text{ is finite at } t = 1\}$. Formally, adding the variable t, we may define a measure with variable

$$(\ell a)^{nh} \int f d\mu_\phi(t) = \sum_{x \in \mathbb{Z}/\ell^{nh}\mathbb{Z}} f(x) \phi(\zeta_{nh}^x t) \in \mathcal{O}_{\mathbb{G}_m, 1/B},$$

and then, $\int f d\mu_\phi$ is its evaluation at $t = 1$: $\int f d\mu_\phi(1)$. We then have for a primitive Dirichlet character $\chi : (\mathbb{Z}/\ell^{nh}\mathbb{Z})^\times \to B^\times$

$$(\ell a)^{nh} \int \chi d\phi(t) = \sum_x \sum_m \chi(x) a(m, \phi) (\zeta_{nh}^x t)^m$$

$$= \sum_m \left(\sum_{x \in \mathbb{Z}/\ell^{nh}\mathbb{Z}} \chi(x) \zeta_{nh}^{mx} \right) t^m = G(\chi) \sum_m \chi^{-1}(m) a(m, \phi) t^m,$$

where $G(\chi)$ is the Gauss sum: $G(\chi) = \sum_{x \in \mathbb{Z}/\ell^n\mathbb{Z}} \chi(x) \zeta^x \neq 0$.

1.4. **Evaluation formula.** Applying the computation in the previous section to $\phi = \Phi_\lambda = \sum_{m=0}^\infty \lambda(m) t^m$ and evaluating the result at $t = 1$, we find

$$\int \chi d\mu_\Phi = (\ell\lambda(\ell))^{-n} G(\chi) \Phi_{\chi^{-1}\lambda}(1) = (\ell\lambda(\ell))^{-n} G(\chi) L(0, \chi^{-1}\lambda).$$

Since $\chi \neq 1$ is supported on $\mathbb{Z}_\ell{}^\times$, we may restrict $d\mu_\Phi$ to $\mathbb{Z}_\ell{}^\times$.

Since any character $\chi : \mathbb{Z}_\ell{}^\times \to \mu_{\ell^\infty}$ factors through $\Gamma = \mathbb{Z}_\ell{}^\times / \mu_{\ell-1}$, we want to have a measure φ supported on $\Gamma = \mathbb{Z}_\ell{}^\times / \mu_{\ell-1}$ so that we have

$$\int_\Gamma \chi d\varphi = \int_{\mathbb{Z}_\ell{}^\times} \chi d\mu_\Phi \quad \text{for all character } \chi \text{ of } \Gamma.$$

The measure φ is not associated to a rational function like Φ, but if we allow functions on μ_{ℓ^∞}, φ is associated to a function Ψ close to Φ.

Noting that $\mu_{\ell-1} \subset \mathbb{Z}_\ell$ acts such functions by $\phi(\zeta) \mapsto \phi(\zeta^s)$ $(s \in \mathbb{Z}_\ell)$, we find that $\varphi = d\mu_\Psi$ for Ψ given by

$$\Psi(\zeta) = \sum_{\varepsilon \in \mu_{\ell-1}} \Phi(\zeta^\varepsilon) = \sum_{\varepsilon \in \mu_{\ell-1}/\{\pm 1\}} (\Phi(\zeta^\varepsilon) + \Phi(\zeta^{-\varepsilon})) \text{ if } \ell \nmid N.$$

1.5. **Zariski density.** We now assume that $B = \overline{\mathbb{F}}_p$. We admit the following result in [Si1]:

Theorem 1.3 (Sinnott). *Let $\Xi \subset \mu_{\ell^\infty}(\overline{\mathbb{F}}_p)$ be an infinite set. Let $\mathcal{F}$ be the $\overline{\mathbb{F}}_p$-algebra of functions on Ξ with values in $\overline{\mathbb{F}}_p$, and define an integral domain $\mathcal{F}_0 = \mathcal{F}/\mathcal{N}$ for the prime ideal $\mathcal{N}$ formed by functions vanishing at almost all $\zeta \in \Xi$ (except finitely many ζ). If $a_1, \dots, a_r \in \mathbb{Z}_\ell$ are linearly independent over $\mathbb{Z}$, the algebra homomorphism from the affine ring $R_0 = \overline{\mathbb{F}}_p[y_1, y_1^{-1} \dots, y_r, y_r^{-1}]$ of $\mathbb{G}_m^r$ into $\mathcal{F}_0$ sending y_j to an element of $\mathcal{F}_0$ given by $\zeta \mapsto \zeta^{a_j}$ for $j = 1, 2, \dots, r$ is injective.*

To conclude the assertion of (Step4), we need to make the following variable change: Let A be the additive subgroup of $\mathbb{Z}_\ell$ generated by $\mu_{\ell-1}$ and take an $\mathbb{Z}$-basis $I = \{a_1, \dots, a_r\}$ of A. Take a complete set of representative $\varepsilon_1, \dots, \varepsilon_n$ of $\mu_{\ell-1}/\{\pm 1\}$ and write $\varepsilon_j = \sum_i c_{ij} a_i$. Write $\mathbb{G}_m^{\mu_{\ell-1}/\{\pm 1\}} = \mathrm{Spec}(R)$ for $R = \overline{\mathbb{F}}_p[t_1, t_1^{-1}, \dots, t_n, t_n^{-1}]$ (t_j corresponds to the component indexed by ε_j). Consider the ring homomorphism $R \to R_0$ sending t_j to $\prod_i y_i^{c_{ij}}$. This induces a morphism $\iota : Y = \mathbb{G}_m^I \to \mathbb{G}_m^{\mu_{\ell-1}/\{\pm 1\}}$ of algebraic groups, and for an infinite subset $\Xi \subset \mu_{\ell^\infty}$, $\widetilde{\Xi} = \{(\zeta^{\varepsilon_1}, \dots, \zeta^{\varepsilon_n}) | \zeta \in \Xi\}$ is the image of $\{(\zeta^{a_1}, \dots, \zeta^{a_n}) | \zeta \in \Xi\} \subset Y$ which is dense in Y by the above theorem. Then in the following section, we conclude the assertion of (Step4) from

Lemma 1.4. *Let the notation be as above. Then a relation of the form:*

$$(*) \qquad (P_1(t_1) + \cdots + P_n(t_n)) \circ \iota = 0$$

in R for $P_j(z) \in \overline{\mathbb{F}}_p[z, z^{-1}]$ can only occur if $P_j(z) \in \overline{\mathbb{F}}_p$ for all j.

Proof. Let $R_0 = \overline{\mathbb{F}}_p[y_1, y_1^{-1}, \dots, y_r, y_r^{-1}]$. Restrict $P_1(t_1) + \cdots + P_n(t_n)$ to Y and look at $\sum_i P_i \circ \iota \in R_0$. Since a_j is a basis of A, $P_i \circ \iota(y)$ and $P_j \circ \iota(y)$ for $i \neq j$ do not contain common monomials of y_j. Since monomials of y_j are all linearly independent over $\overline{\mathbb{F}}_p$, we find that the relation $(*)$ implies $P_i(z) \in \overline{\mathbb{F}}_p$ for all i. $\square$

1.6. **Application of Zariski density.** We first assume that $\int_\Gamma \chi d\varphi = 0$ (that is, $L(0, \chi^{-1}\lambda) \equiv 0 \mod \mathfrak{P}$) for all $\chi : \Gamma \to \mu_{\ell^\infty}$. Then by orthogonality relation of characters, we find $\Psi(\zeta) = 0$ for all $\zeta \in \mu_{\ell^\infty}$. Thus we find that $\Phi(t^\varepsilon) + \Phi(t^{-\varepsilon}) \in \overline{\mathbb{F}}_p$, which is impossible by the t-expansion of Φ.

Now we assume a weaker condition that we have an infinite sequence of characters $\{\chi_j\}_j$ of order ℓ^{n_j} with $\int_\Gamma \chi_j d\varphi = 0$, which implies by variable change: $\int_\Gamma \chi_j(x)d\varphi(ax) = 0$.

Exercise 1.5. *For any field k of characteristic different from ℓ, prove the following formula for a primitive ℓ^n-th root of unity ζ_n with $n \geq 2$ not in k:* $\mathrm{Tr}_{k[\zeta_n]/k}(\zeta_n^x) \neq 0 \Leftrightarrow \zeta_n^x \in k$.

We assume that λ has values in $\mathbb{F}_q^\times$ ($q = p^f$). Then applying the Frobenius automorphism $F(x) = x^q$, we find for $\chi = \chi_j$ and $n = n_j$

$$0 = \left(\int_\Gamma \chi(x)d\varphi(ax)\right)^{q^n} = \left(\sum_u \chi(u)\Psi(\zeta_n^{au})\right)^{q^n}$$
$$= \sum_u \chi^{q^n}(u)\Psi(\zeta_n^{auq^n}) = \chi^{q^n}(q^n)^{-1}\int_\Gamma \chi^{q^n} d\varphi(ax)$$

for all n. Thus taking the trace of $\int_\Gamma \chi(x)d\varphi(ax)$ from the field $\mathbb{F}_q[\chi_j]$ generated by the values of χ_j to $\mathbb{F}_q[\mu_\ell]$, we find that

$$\sum_{u\in\chi_j^{-1}(\mathbb{F}_q[\mu_\ell])} \chi_j(u)\Psi(\zeta_{n_j}^{au}) = 0$$

for all $a \in \Gamma/\Gamma^{\ell^{n_j}}$. Writing the order of the ℓ–primary part of $(\mathbb{F}_q[\mu_\ell])^\times$ as ℓ^m, note that the above sum only involves $u \in \Gamma^{\ell^{n_j-m}}/\Gamma^{\ell^{n_j}}$. Taking n_j so that $n_j \geq 2m$, we can identify the multiplicative group $\Gamma^{\ell^{n_j-m}}/\Gamma^{\ell^{n_j}}$ with the additive one $\mathbb{Z}/\ell^m\mathbb{Z}$ by $\mathbb{Z}/\ell^m\mathbb{Z} \ni v \mapsto 1+\ell^{n_j-m}v = u$. We can then write $\chi_j(u) = \zeta_m^{b_j v}$ for $b_j \in (\mathbb{Z}/\ell^m\mathbb{Z})^\times$ and $\zeta_n^{au} = \zeta_n^a\zeta_m^v$. Since $\{\chi_j\}$ is infinite, we may assume that b_j is a constant b. We have for any $a \in \mathbb{Z}_\ell^\times$

$$\sum_{v \mod \ell^m} \zeta_m^{bv}\Psi(\zeta_{n_j}^a\zeta_m^v) = \sum_{v \mod \ell^m} \zeta_m^{bv}\Psi|\zeta_m^v(\zeta_{n_j}^a) = 0,$$

where for $f \in \overline{\mathbb{F}}_p(\mathbb{G}_m)$, $f|x \in \overline{\mathbb{F}}_p(\mathbb{G}_m)$ is defined by $f|x(t) = f(tx)$ for $x \in \mathbb{G}_m(\overline{\mathbb{F}}_p)$. Since $\pi(\Xi)$ for $\Xi = \bigcup_j \mu_{\ell^{n_j}}^\times$ is still dense in Y, applying Lemma 1.4 to $P_j(z) = \Phi'_j(z)+\Phi'_j(\frac{1}{z})$ for $\Phi'_j(z) = \sum_{v \mod \ell^{n_0}} \zeta_{n_0}^{av}\Phi|\zeta_{n_0}(z)$ on $\mathbb{G}_m = \mathrm{Spec}(\overline{\mathbb{F}}_p[z, z^{-1}])$, we conclude $P_j(z) \in \overline{\mathbb{F}}_p$, whose Taylor expansion at $z = 1$ can be easily seen to be nonconstant by computation.

2. Modular Curves

We create a circumstance very similar to the pair $(\mathbb{G}_m, \mu_{\ell^\infty})$ replacing $\mathbb{G}_m$ by modular curves and μ_{ℓ^∞} by CM-points of modular curves. This new setting allows us to prove nonvanishing modulo p of Hecke L-values in the following sections. We write $G(A) = GL_2(A)$.

2.1. **A sketch of the theory of modular curves.** We study classification problem of elliptic curves $E_{/A}$ over a ring A (which is an algebra over a base ring B). The abelian group E has the identity section $\mathbf{0}_E : \mathrm{Spec}(A) \hookrightarrow E$, and $\Omega_{E/A}$ is a locally free sheaf of rank 1. In particular, if it is free, we have a unique generator $\omega \in H^0(E, \Omega_{E/A})$ such that $\Omega_{E/A} = \mathcal{O}_E\omega$. Since E is projective, $H^0(E, \mathcal{O}_E) = A$, ω is uniquely determined up to multiplication by units in $A^\times$.

We consider the following moduli functor of level $\Gamma(N)$,

$$\mathcal{E}_{\Gamma(N),\zeta}(A) = \left[(E, \phi_N : (\mathbb{Z}/N\mathbb{Z})^2 \cong E[N])\middle|\langle\phi_N(1,0), \phi_N(0,1)\rangle = \zeta\right],$$

for all $\mathbb{Z}[\frac{1}{N}, \zeta]$-algebras A, where ζ is a generator of μ_N. Here $\langle\cdot,\cdot\rangle$ is the Weil pairing. We know classically $\mathcal{E}_{\Gamma(N),\zeta}(\mathbb{C}) \cong \Gamma(N)\backslash\mathfrak{H}$. If we remove the contribution upon ζ and consider the functors $\mathcal{P}_{\Gamma(N)}(A) = \left[(E, \omega, \phi_N)_{/A}\right]$ and $\mathcal{E}_{\Gamma(N)}(A) = \left[(E, \phi_N)_{/A}\right]$ defined on the category of $\mathbb{Z}[\frac{1}{N}]$-algebras, we have $\mathcal{P}_{\Gamma(N)} = \bigsqcup_\zeta \mathcal{P}_{\Gamma(N),\zeta}$ and $\mathcal{E}_{\Gamma(N)} = \bigsqcup_\zeta \mathcal{E}_{\Gamma(N),\zeta}$, and these functors are represented by a geometrically non-connected scheme $\mathcal{M}_{\Gamma(N)}$ and $Y(N)$ defined over $\mathbb{Z}[\frac{1}{N}]$ if $N \geq 3$. Note that $Y(N)_{/\mathbb{Z}[\frac{1}{N},\zeta_N]} = \bigsqcup_{\zeta\in\mu_N^\times} Y_\zeta(N)$ with $Y_\zeta(N)(\mathbb{C}) \cong \Gamma(N)\backslash\mathfrak{H}$.

We can let a constant group $\alpha \in SL_2(\mathbb{Z}/N\mathbb{Z})$ act on $Y_\zeta(N)$ (and hence on $X_\zeta(N)$) by $(E, \phi) \mapsto (E, \phi\circ\alpha)$. Since $\langle\phi\circ\alpha(1,0), \phi\circ\alpha(0,1)\rangle = \zeta_N^{\det(\alpha)}$, the same action of $\alpha \in G(\mathbb{Z}/N\mathbb{Z})$ induces an automorphism of $Y(N)$ (and $X(N)$) regarded as schemes over $\mathbb{Z}[\frac{1}{N}]$ (not over $\mathbb{Z}[\frac{1}{N}, \zeta_N]$), which coincides with the Galois action $\zeta_N \mapsto \zeta_N^{\det(\alpha)}$ on $\mathbb{Z}[\zeta_N]$. By taking the limit $Y = \varprojlim_N Y(N)$ (which is a pro-scheme defined over $\mathbb{Q}$). $G(\widehat{\mathbb{Z}}) = \varprojlim_N G(\mathbb{Z}/N\mathbb{Z})$ acts on Y, and $SL_2(\widehat{\mathbb{Z}})$ preserves the connected component $Y_{\zeta_\infty} = \varprojlim_N Y_{\zeta_N}(N)$.

A remarkable fact Shimura found is that this action of $G(\widehat{\mathbb{Z}})$ can be extended to the finite adele group $G(\mathbb{A}^{(\infty)})$ (see [IAT] Chapter 6). An interpretation by Deligne of this fact is fascinating (see [PAF] 4.2.1): To explain Deligne's idea, we define the Tate module $T(E) = \varprojlim_N E[N]$ for an elliptic curve $E_{/A}$ for a $\mathbb{Q}$-algebra A. Strictly speaking, taking a geometric point $s = \mathrm{Spec}(k) \in \mathrm{Spec}(A)$ (for an algebraically closed field k) in each connected component of $\mathrm{Spec}(A)$, we are thinking of the $\widehat{\mathbb{Z}}$-module $T(E) = \varprojlim_N E[N](k)$ (the choice of s does not matter, and the module structure over $\pi_1(\mathrm{Spec}(A))$ of $T(E)$ is determined up to inner conjugation of the algebraic fundamental group $\pi_1(\mathrm{Spec}(A))$; see [PAF] Chapter 4, Appendix). Then $T(E) \cong \widehat{\mathbb{Z}}^2$ and $V(E) = T(E) \otimes_{\mathbb{Z}} \mathbb{A}^{(\infty)} \cong (\mathbb{A}^{(\infty)})^2$. Deligne realized that Y represents the following functor defined over $\mathbb{Q}$-ALG:

$$\mathcal{E}^{(\infty)}(A) = \{(E, \eta : (\mathbb{A}^{(\infty)})^2 \cong V(E))_{/A}\}/\text{isogenies},$$

where an isogeny $\phi : E \to E'$ is a morphism of group schemes with finite kernel (so dominant). Here $\mathbb{A}^{(\infty)}$ is the finite adele ring. Then $g \in G(\mathbb{A})$ sends a point $(E, \eta)_{/A} \in \mathcal{E}^{(\infty)}(A)$ to $(E, \eta \circ g^{(\infty)})_{/A}$ for the projection $g^{(\infty)}$ of g to $\mathbb{A}^{(\infty)}$.

Take the prime-to-p part $Y^{(p)} = \varprojlim_{p \nmid N} Y(N)$. Here N runs over all positive integers prime to p. Then $Y^{(p)}$ classifies $(E, \eta^{(p)})_{/A}$ up to prime-to-p isogenies for $\mathbb{Z}_{(p)}$-algebras A ($\mathbb{Z}_{(p)} = \mathbb{Q} \cap \mathbb{Z}_p$). Here putting $V^{(p)}(E) = T(E) \otimes_{\mathbb{Z}} \mathbb{A}^{(p\infty)}$, $\eta^{(p)}$ is the prime-to–p level structure $\eta^{(p)} : (\mathbb{A}^{(p\infty)})^2 \cong V^{(p)}(E)$. In other words, $Y^{(p)}$ represents the following functor defined over $\mathbb{Z}_{(p)}$-ALG:

$$\mathcal{E}^{(p)}(A) = \{(E, \eta : (\mathbb{A}^{(p\infty)})^2 \cong V^{(p)}(E))_{/A}\}/\text{prime-to-}p\text{ isogenies},$$

where an isogeny ϕ is prime to p if the order of the kernel of ϕ is prime to all primes in p. This pro-scheme $Y^{(p)}$ is defined over $\mathbb{Z}_{(p)}$; so, its restriction to $\overline{\mathbb{F}}_p$-algebras $Y^{(p)}_{/\overline{\mathbb{F}}_p}$ is a characteristic $\overline{\mathbb{F}}_p$-scheme classifying $(E, \eta^{(p)})_{/A}$ for $\overline{\mathbb{F}}_p$-algebras A. On $Y^{(p)}$, again $G(\mathbb{A}^{(p)})$ acts.

If we have a prime-to-p non-central endomorphism $\alpha : E \to E$, then E has complex multiplication by $M = \mathbb{Q}[\alpha]$, and we can write $\alpha \circ \eta = \eta \circ \rho(\alpha)$ for $\rho(\alpha) \in G(\mathbb{A}^{(\infty)})$. Thus if $x = (E, \eta) \in Y(A)$, we find that $\rho(\alpha)(x) = x$. For any elliptic curve E, we have $\mathbb{Q} \subset \mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$; so, the central element $\xi \in \mathbb{Q}^\times \subset G(\mathbb{A}^{(\infty)})$ acts trivially on Y. Thus, $x = (E, \eta)$ has CM by an imaginary quadratic field M if and only if $M^\times/\mathbb{Q}^\times$ is the stabilizer of x in $\mathrm{Aut}(Y)$.

Pick an elliptic curve $E = X$ with complex multiplication by $R_n = \mathbb{Z} + \ell^n R$, where R is the integer ring of M. We suppose that p splits into $(p) = \mathfrak{p}\overline{\mathfrak{p}}$ in R_n. Consider $W = W(\overline{\mathbb{F}}_p)$ inside $\mathbb{C}_p = \widehat{\overline{\mathbb{Q}}}_p$ and its field of fractions K. We put $\mathcal{W} = W \cap \overline{\mathbb{Q}}$ which is a strict henselization of $\mathbb{Z}_{(p)}$. We suppose that $\mathfrak{p} = R_n \cap \mathfrak{m}_{\mathcal{W}}$ and $X[\overline{\mathfrak{p}}^\infty]$ is étale over $\mathcal{W}$. Then we can pick a level p-structure $\eta_p : \mu_{p^\infty} \cong X[\mathfrak{p}^\infty]$. Identify $X(\mathbb{C}) = \mathbb{C}/\mathfrak{a}$ for an R_n-ideal $\mathfrak{a}$ and fix a base w_1, w_2 of $\mathfrak{a} \otimes_{\mathbb{Z}} (\mathbb{Z}_p \times \mathbb{A}^{(p\infty)})$, which induces prime-to–p level structure $\eta^{(p)} : (\mathbb{A}^{(p\infty)})^2 \cong \mathfrak{a} \otimes_{\mathbb{Z}} \mathbb{A}^{(p\infty)} = V^{(p)}(X)$. We assume that $\rho(\alpha) w_{1,p} = \alpha w_{1,p}$ for $R_n \hookrightarrow R_{\mathfrak{p}}$. Since $\alpha \in R^\times_{(p)}$ induces an isogeny $\alpha : X \to X$ sending $\alpha\eta^{(p)} = \eta^{(p)}\rho(\alpha)$, the point $x = (X, \eta^{(p)})$

is fixed by $\rho(\alpha)$. Consider the formal completion $\widehat{Y} = \widehat{Y}_x$ of $Y^{(p)}_{/\mathcal{W}}$ along $x \in Y^{(p)}(\overline{\mathbb{F}}_p)$. Then by the universality of Y, $\widehat{Y}$ satisfies

$$\widehat{Y}(A) \cong \widehat{\mathcal{E}}(A),$$

where A runs through p-profinite W-algebras with $A/\mathfrak{m}_A = W/\mathfrak{m}_W = \overline{\mathbb{F}}_p$ and $\widehat{\mathcal{E}}(A) = \left[E_{/A} \middle| E \otimes_A \overline{\mathbb{F}}_p = X_{/\overline{\mathbb{F}}_p}\right]$. Indeed $\widehat{Y}$ classifies $(E, \eta^{(p)})_{/A}$ with $(E, \eta^{(p)}_E) \times_A \overline{\mathbb{F}}_p = (X, \eta^{(p)})$, but $\eta^{(p)}$ uniquely determines $\eta^{(p)}_E$; so, we can drop the datum of the level structure. By the deformation theory of Serre-Tate, $\widehat{Y} \cong \widehat{\mathbb{G}}_m$ canonically. This goes as follows. First $E_{/A} \in \widehat{\mathcal{E}}(A)$ is determined by the extension $E[p^\infty]^\circ \hookrightarrow E[p^\infty] \twoheadrightarrow E[p^\infty]^{et}$ of the Barsotti-Tate groups. Such an extension over A is classified by

$$\mathrm{Hom}(E[p^\infty]^{et}, E[p^\infty]^\circ) \cong \mathrm{Hom}(\mathbb{Q}_p/\mathbb{Z}_{p/A}, \mu_{p^\infty/A}) = \varprojlim_n \mu_{p^n}(A) = \widehat{\mathbb{G}}_m(A).$$

For this identification, we need to fix $\eta_p : \mu_{p^\infty} \cong X[\mathfrak{p}^\infty]$ and its dual $X[\overline{\mathfrak{p}}^\infty] \cong \mathbb{Q}_p/\mathbb{Z}_p$. Since $\rho(\alpha)$ fix x, it acts on $\widehat{Y}$.

Lemma 2.1. *Identifying $\widehat{Y}$ with $\widehat{\mathbb{G}}_m = \mathrm{Spf}(\varprojlim_n W[t, t^{-1}]/(t-1)^n)$, we have $\rho(\alpha)(t) = t^{\alpha^{1-c}}$ for complex conjugation c.*

Let $\zeta \in \widehat{Y}(W[\mu_{p^n}])$ be a p-power root of unity. Then if $\alpha \equiv \alpha^c \mod p^n$, $\alpha^{1-c} \equiv 1 \mod p^n$ we have $\zeta^{\alpha^{1-c}} = \zeta$. This shows that the point $\zeta \in \widehat{Y}$ carries an elliptic curve X_ζ with an isogeny $\alpha \in \mathrm{End}(X_\zeta)$ inducing $t \mapsto t^{\alpha^{1-c}}$ on $\widehat{Y}$. Thus X_ζ has complex multiplication by $R'_n = \mathbb{Z} + p^n R$. If X is actually defined over $\mathbb{F}_{p^h}$, we have the relative Frobenius map $\phi = \alpha \in \mathrm{End}(X)$ of degree p^h. Then the relative Frobenius map F of $\widehat{Y}_{/\mathbb{F}_{p^h}}$ can be written as $\rho(\alpha)$. We then have $\rho(\alpha^n)(\zeta) = 1$ for $\zeta \in \mu_{p^{nh}}$, and $\alpha^n : X_\zeta \to X$ is an isogeny of degree p^{nh}. In other words, we have

$$\{X_\zeta\} = \{X/C | C \neq X[p^{nh}]^\circ\text{: cyclic subgroups of } X \text{ of order } p^{nh}\}.$$

By this, we can see that the modular Hecke operator $U(p)$ coincides with the $\mathbb{G}_m$ Hecke operator $U(p)$.

3. Nonvanishing modulo p of Hecke L–values

In 1899, Hurwitz studied an analogue of the Riemann zeta function:

$$L(4k) = \sum_{a+bi\in\mathbb{Z}[i]-\{0\}} \frac{1}{(a+bi)^{4k}}$$

of Gaussian integers $\mathbb{Z}[i]$ and showed that for positive integer k,

$$\frac{L(4k)}{\Omega^{4k}} \in \mathbb{Q} \quad \left(\Omega = 2\int_0^1 \frac{dx}{\sqrt{1-x^4}} = \int_\gamma \frac{dx}{y} : \text{period of the lemniscate}\right).$$

Nowadays, we regard this value as a special value of a Hecke L-function:

$$L(s,\lambda) = \sum_{\mathfrak{a}} \lambda(\mathfrak{a})N(\mathfrak{a})^{-s} \quad \text{of the Gaussian field } \mathbb{Q}[i].$$

Here λ is a Hecke ideal character of $\mathbb{Q}[i]$ with $\lambda((\alpha)) = \alpha^{-4k}$ and $L(4k) = 4L(0,\lambda)$.

We shall give a sketch of a proof of non-vanishing modulo p of almost all Hecke L–values for general imaginary quadratic fields $M = \mathbb{Q}[\sqrt{-D}]$. The Hurwitz formulation is modular: For any lattice $L = \mathbb{Z}w_1 + \mathbb{Z}w_2 \subset \mathbb{C}$, we can think about

$$E_{2k}(L) = \frac{1}{2}\sum_{aw_1+bw_2\in L} \frac{1}{(aw_1+bw_2)^{2k}} \quad \text{(Eisenstein series)},$$

which is a function of lattices satisfying $E_{2k}(\alpha L) = \alpha^{-2k}E_{2k}(L)$. The quotient $\mathbb{C}/L$ gives rise to an elliptic curve $X(L) \subset \mathbf{P}^2$ by Weierstrass theory. Since $X(L)$ has a unique nowhere vanishing differential du for the variable u of $\mathbb{C}$ and we can recover out of $(X(L), du)$ the lattice L as $\{\int_\gamma du | \gamma \in H_1(E,\mathbb{Z})\}$, we can think of E_{2k} as a function of the pairs (X,ω) of an elliptic curve X and a nowhere vanishing differential ω satisfying $E_{2k}(E,\alpha\omega) = \alpha^{-2k}E_{2k}(E,\omega)$. Note that $E_4(E,\omega) = \frac{1}{120}g_2(E,\omega)$ and $E_6(E,\omega) = \frac{1}{280}g_3(E,\omega)$. More generally, E_{2k} is a rational isobaric polynomial of g_2 and g_3. Thus E_{2k} is a modular form f of weight $2k$.

Write R for the integer ring of M. We assume that p splits into $p = \mathfrak{p}\overline{\mathfrak{p}}$ in R so that $\mathfrak{p}$ gives rise to a p–adic place $i_p : \overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$. We write W for the ring of Witt vectors with coefficients in an algebraic closure $\overline{\mathbb{F}}_p$ of the finite field $\mathbb{F}_p$ and regard it as a valuation subring of $\mathbb{C}_p \supset \overline{\mathbb{Q}}_p$ (in other words, W is the closure in $\mathbb{C}_p$ of the p-adic integer ring of the maximal unramified extension of $\mathbb{Q}_p$). We define $\mathcal{W} = \mathcal{W}_p = i_p^{-1}(W)$ with maximal ideal $\mathfrak{P}$. Important facts are

(E1) For a lattice $\mathfrak{a} \subset R$ prime to p ($\mathfrak{a}$ is prime to p if $[R:\mathfrak{a}]$ is prime to p), $X(\mathfrak{a})$ is p-integral defined over $\mathcal{W} \subset \overline{\mathbb{Q}}$;

(E2) E_{2k} is defined over $\mathbb{Q}$ (actually over $\mathbb{Z}_{(p)}$ for almost all k) by the q-expansion principle;

(E3) Let $\omega = \Omega du$ be a generator of $H^0(X(R), \Omega_{X(R)/\mathcal{W}})$ (which means that $H^0(X(\mathfrak{a}), \Omega_{X(\mathfrak{a})/\mathcal{W}}) = \mathcal{W}\omega$, because $\mathfrak{a}$ is prime to p), in other words, $\Omega = \int_\gamma \omega$ for a 1-cycle γ with $R_{(p)}\gamma = H_1(X(\mathfrak{a}), \mathbb{Z}_{(p)})$. Then $\frac{E_{2k}(X(\mathfrak{a}),\omega)}{N(\mathfrak{a})^{2k}\lambda(\mathfrak{a})}$ is the partial L–value of the ideal class of $\mathfrak{a}^{-1}$:

$$\frac{E_{2k}(X(\mathfrak{a}),\omega)}{N(\mathfrak{a})^{2k}\lambda(\mathfrak{a})} = \frac{E_{2k}(X(\mathfrak{a}),\Omega du)}{N(\mathfrak{a})^{2k}\lambda(\mathfrak{a})} = \frac{E_{2k}(X(\mathfrak{a}),du)}{\Omega^{2k}N(\mathfrak{a})^{2k}\lambda(\mathfrak{a})} = \frac{L_{\mathfrak{a}^{-1}}(2k,\lambda)}{\Omega^{2k}} \in \overline{\mathbb{Q}},$$

because

$$\frac{E_{2k}(X(\mathfrak{a}),du)}{N(\mathfrak{a})^{2k}\lambda(\mathfrak{a})} = L_{\mathfrak{a}^{-1}}(2k,\lambda) = \sum_{\mathfrak{b}\sim\mathfrak{a}^{-1}} \lambda(\mathfrak{b})N(\mathfrak{b})^{-2k}$$

for a Hecke character λ with $\lambda((\alpha)) = \alpha^{-2k}$.

In order to get p-integrality and an $U(\ell)$-eigenform, we modify the Eisenstein series E_{2k} into $\mathcal{E}_{2k}(z) = E_{2k}(z) - E_{2k}(\ell z)$. Then we have $\mathcal{E}_{2k}(X(\mathfrak{a}),\omega) \in \mathcal{W}$.

Fix a prime $\ell \neq p$. A character $\chi : \{\text{ideals of } M \text{ prime to } \ell\} \to \mathbb{C}^\times$ is called ℓ-anticyclotomic if $\chi(\mathfrak{a}^c) = \chi(\mathfrak{a})^{-1}$ for complex conjugation c and $\chi((\alpha)) = 1$ if $\alpha \equiv 1 \mod \ell^n$ for some $n \gg 0$.

As described above, which is a result of Hurwitz, Damerell and Weil combined, that

$$\frac{(2k-1)!L^{(\ell)}(0,\lambda\chi)}{\Omega^{2k}} \in \mathcal{W} \text{ for } \ell\text{-anticyclotomic } \chi,$$

where $L^{(\ell)}(0,\lambda\chi) = \left\{\prod_{\mathfrak{l}|\ell}(1-\lambda\chi(\mathfrak{l}))\right\} L(0,\lambda\chi)$. Then we have

Theorem 3.1. *Fix a prime $\ell \neq p$. We have $\frac{(2k-1)!L^{(\ell)}(0,\lambda\chi)}{\Omega^{2k}} \not\equiv 0 \mod \mathfrak{P}$ except for finitely many ℓ-anticyclotomic characters χ.*

Here we shall give a sketch of the proof of this special case in the following couple of sections as outlined in the case of $(\mathbb{G}_m, \mu_{\ell^\infty})$. The result in the above imaginary quadratic cases are also treated by Finis (see [Fi]) under different assumptions (see also Vatsal's papers [V] and [V1] for related topics).

3.1. **Modular forms of $\Gamma_0(\ell^n)$.** We take the following moduli theoretic definition of modular form on $\Gamma_0(\ell^n)$. A level $\Gamma_0(\ell^n)$-structure on $(E,\omega)_{/B}$ (for a base $\mathbb{Z}_{(p)}$-algebra B) is an étale subgroup $C \subset E[\ell^n]$ defined over B étale locally isomorphic to $\mathbb{Z}/\ell^n\mathbb{Z}$. Then $f \in G_k(\Gamma_0(\ell^n); B)$

is a functorial morphism for all B-algebras A,

$$\mathcal{P}_{\Gamma_0(\ell^n)}(A) = \left[(E, C, \omega)_{/A}\right] \to \mathbf{A}^1(A) = A$$

satisfying the following conditions: Regarding f as a function of isomorphism classes of $(E, C, \omega)_{/A}$ with $f((E, C, \omega)_{/A}) \in A$ satisfying

(G1) $f((E, C, a\omega)_{/A}) = a^{-k} f((E, C, \omega)_{/A})$ for $a \in A^\times = \mathbb{G}_m(A)$;
(G2) If $\rho : A \to A'$ is a morphism of B-algebras, then we have

$$f((E, C, \omega)_{/A} \times_A A') = \rho(f((E, C, \omega)_{/A}));$$

(G3) The function has finite q-expansion at the Tate curves with level $\Gamma_0(\ell^n)$-structure.

3.2. **Measure associated to a Hecke eigenform.** The first step towards the proof of the theorem is a construction of a measure interpolating values of a Hecke eigenform at CM points. We apply this to Eisenstein series E_{2k}.

Take the base ring A to be $\overline{\mathbb{F}}_p = \mathcal{W}/\mathfrak{P}$. We add a datum of a cyclic ℓ-subgroup to the definition of modular forms. A modular form g on $\Gamma_0(\ell)$ assigns its value $g(E, C, \omega) \in A$ to each isomorphism class of a triple $(E, C, \omega)_{/A}$ defined over an $\overline{\mathbb{F}}_p$–algebra A, where $C_{/A}$ is a cyclic subgroup of order ℓ.

Summing over ℓ-cyclic subgroups C' of E different from C, the Hecke operator $U(\ell)$ is defined by

$$g|U(\ell) = \frac{1}{\ell} \sum_{C'} g(E/C', C + C'/C', \pi_*\omega), \tag{3.1}$$

where π is the étale projection $\pi : E \to E/C'$. We could have started modular forms over $\mathcal{A} = \mathcal{W}_p \cap \mathcal{W}_\ell$. Then each E has C giving the connected component over $\mathcal{A}$, and under this circumstance, modular $U(\ell)$ coincides with the $\mathbb{G}_m$-version of $U(\ell)$ as already seen.

If we write the standard q-expansion of g at ∞ $g(q) = \sum_n a(n, g)q^n$, we have $a(n, g|U(\ell)) = a(n\ell, g)$.

Fix a modular form f on $\Gamma_0(\ell)$ of weight $2k$ with $f|U(\ell) = a(\ell)f$. We again rediscover

$$a(n, f|U(\ell)) = a(n\ell, f) = a(\ell) \cdot a(n, f). \tag{UL}$$

Hereafter we simply write a for $a(\ell)$. Fix an imaginary quadratic field $M = \mathbb{Q}[\sqrt{-D}] \subset \overline{\mathbb{Q}}$ in which p splits: $(p) = \mathfrak{p}\overline{\mathfrak{p}}$. Consider the order $R_n := \mathbb{Z} + \ell^n R$ for the integer ring R of M. We write

$$Cl_n := \frac{\text{projective fractional } R_n\text{-ideals}}{\text{principal } R_n\text{-ideals}} = M^\times \backslash (M_{\mathbb{A}}^{(\infty)})^\times / (\mathbb{A}^{(\infty)})^\times \widehat{R}_n^\times,$$

which is the ring class group of R_n. We define $Cl_\infty = \varprojlim_n Cl_n$ for the projection $\pi_{m+n,n} : Cl_{n+m} \twoheadrightarrow Cl_n$ taking $\mathfrak{a}$ to $\mathfrak{a}R_n$. The group Cl_∞ is isomorphic to the Galois group of the maximal anticyclotomic abelian extension of M unramified outside ℓ.

As before, $X(\mathfrak{a})_{/\mathcal{W}}$ is the CM elliptic curve with $X(\mathfrak{a})(\mathbb{C}) = \mathbb{C}/\mathfrak{a}$. We fix a basis w_1, w_2 of $\widehat{R}$ so that its p-component is given by idempotent $e_\mathfrak{p}$ of $R_\mathfrak{p}$ and $e_{\overline{\mathfrak{p}}}$ of $R_{\overline{\mathfrak{p}}}$. At ℓ, write $R_\ell = \mathbb{Z}_\ell + \mathbb{Z}_\ell\sqrt{d}$ with $d \in \mathbb{Z}_\ell$ choosing $d \in \mathbb{Z}_\ell^\times$ if $R_\ell/\mathbb{Z}_\ell$ is unramified. If $[\mathfrak{a}] \in Cl_n$ is a proper R_n-ideal, we may choose $\mathfrak{a}$ so that $\mathfrak{a}_\ell = (\mathbb{Z}_\ell, \mathbb{Z}_\ell)\left(\begin{smallmatrix} 1 & j/\ell^n \\ 0 & 1 \end{smallmatrix}\right)\alpha_n{}^t(1, \sqrt{d})$ for $\alpha_n = \left(\begin{smallmatrix} 1 & 0 \\ 0 & \ell^n \end{smallmatrix}\right)$ and some integer j unique modulo ℓ^n. Then we take a basis ${}^t(w_1(\mathfrak{a}), w_2(\mathfrak{a}))$ of $\widehat{\mathfrak{a}}$ as follows: At ℓ, it is given by $\alpha_n{}^t(1, \sqrt{d})$ and outside ℓ, $(w_1(\mathfrak{a})^{(\ell)}, w_2(\mathfrak{a})^{(\ell)}) = (aw_1^{(\ell)}, aw_2^{(\ell)})$ for $a \in (M_\mathbb{A}^{(\infty)})^\times$ with $aR = \mathfrak{a}R$. Out of this, we have a unique $x(\mathfrak{a}) = (X(\mathfrak{a}), \eta(\mathfrak{a})) \in Y/I_0(\ell)$ with $I_0(\ell) = \{x \in GL_2(\widehat{\mathbb{Z}}) | (x_\ell \mod \ell) \in B(\mathbb{F}_\ell)\}$ for the upper triangular Borel subgroup $B \subset G$. Moreover, we have

$$\rho(\alpha)(x(\mathfrak{a})) = x(\alpha\mathfrak{a}) \quad \text{for all } \alpha \in R_{(\ell)}^\times, \tag{3.2}$$

and

$$\pi_{n,n-1}^{-1}([\mathfrak{a}_0]) = \left\{ \begin{pmatrix} 1 & \frac{j}{\ell} \\ 0 & 1 \end{pmatrix} \alpha_1(x(\mathfrak{a}_0)) \quad \text{for } j \in \mathbb{Z}/\ell\mathbb{Z} \right\} \quad \text{for } n \geq 2. \tag{3.3}$$

We choose the Néron differential $\omega(R)$ so that $\Omega_{X(R)/\mathcal{W}} = \mathcal{W}\omega(R)$. Since $X(\mathfrak{a})$ is étale isogenous to $X(R)$, $\omega(R)$ induces a differential $\omega(\mathfrak{a})$ on $X(\mathfrak{a})$ with $\Omega_{X(\mathfrak{a})/\mathcal{W}} = \mathcal{W}\omega(\mathfrak{a})$. Since $\mathfrak{a}_\ell = a_\ell R_{n,\ell}$ for $a_\ell \in M_\ell^\times$, we have a cyclic subgroup $C(\mathfrak{a}) := a_\ell(R_{n-1}/R_n)$ of $X(\mathfrak{a})$. This subgroup is $\eta(\mathfrak{a})(\ell^{-1}\mathbb{Z}_p/\mathbb{Z}_p \oplus 0)$. The λ-twisted value

$$f([\mathfrak{a}]) = (a\ell^{1-2k})^{-n}\lambda(\mathfrak{a})^{-1} f(X(\mathfrak{a}), C(\mathfrak{a}), \omega(\mathfrak{a}))$$

depends only on the ideal class $[\mathfrak{a}]$ in Cl_n.

For a given projective R_n–ideal $\mathfrak{a}$, there are exactly ℓ projective R_{n+1}-ideals $\mathfrak{a}_i$ with $\mathfrak{a}_i/\mathfrak{a} \cong \mathbb{F}_\ell$ ($\Leftrightarrow X(\mathfrak{a}_i) = X(\mathfrak{a})/C'$ for some C' of cyclic of order ℓ not equal to $C(\mathfrak{a})$), and we find from (3.1) and $f|U(\ell) = af$

$$f([\mathfrak{a}]) = \sum_{i=1}^{\ell} f([\mathfrak{a}_i]). \tag{3.4}$$

We define a measure df on Cl_∞ as follows: if ϕ factors through Cl_n,

$$\int_{Cl_\infty} \phi df = \sum_{[\mathfrak{a}] \in Cl_n} \phi(\mathfrak{a}) f([\mathfrak{a}]).$$

By the distribution relation (3.4), this is a well defined independently of the choice of n. Let $E = E_{2k}(z) - E_{2k}(\ell z)$ be the Eisenstein series of weight k on $\Gamma_0(\ell)$ with $E|U(\ell) = \ell^{2k-1}E$ and

$$\int \chi dE = \frac{(2k-1)!L^{(\ell)}(0,\chi^{-1}\lambda)}{\Omega^{2k}}. \tag{3.5}$$

3.3. **Density of CM points.** Each integral R–ideal $\mathfrak{A}$ of M prime to ℓ gives rise to a unique proper R_n–ideal $\mathfrak{a}_n = \mathfrak{A} \cap R_n$, and the limit $[\mathfrak{A}] = \varprojlim_n [\mathfrak{a}_n]$ is a well defined element of Cl_∞. We extend this construction to fractional ideals by $[\mathfrak{A}\mathfrak{B}^{-1}] := [\mathfrak{A}][\mathfrak{B}]^{-1}$. Thus the ideal group I of fractional ideals of R (prime to ℓ) is a subgroup of Cl_∞.

If $[\mathfrak{a}]$ is an ideal class in Cl_n, then $x[\mathfrak{a}] = (X(\mathfrak{a}), C(\mathfrak{a}))_{/\overline{\mathbb{F}}_p}$ gives a unique closed point $x[\mathfrak{a}]$ of the modular curve $X_0(\ell)$. Let $\underline{n} : 0 < n_1 < n_2 < \cdots < n_j < \cdots$ be an infinite sequence of integers. Define

$$\Xi = \Xi_{\underline{n}} = \left\{[\mathfrak{a}] \middle| [\mathfrak{a}] \in \mathrm{Ker}(\pi_{n_j,n_1}) \text{ for } j = 1, 2, \ldots\right\}$$

and put $\Xi^{\mathcal{Q}}_{\underline{n}} = \left\{(x[\delta\mathfrak{a}])_{\delta\in\mathcal{Q}} \in X_0(\ell)^{\mathcal{Q}} \middle| [\mathfrak{a}] \in \Xi\right\}$. for a subset $\mathcal{Q} \subset Cl_\infty$, where $X_0(\ell)^{\mathcal{Q}} = \prod_{\delta\in\mathcal{Q}} X_0(\ell)$ and $\delta\mathfrak{a}$ is the product of $\pi_{\infty,n_j}(\delta)$ and $[\mathfrak{a}]$ in Cl_{n_j}. By the same argument as in the Dirichlet character case (using the q-expansion in place of the t-expansion), the desired result follows from

Theorem 3.2 (density)**.** *If $\mathcal{Q}$ is finite and injects into Cl_∞/I, the subset $\Xi^{\mathcal{Q}}_{\underline{n}}$ is Zariski-dense in $X_0(\ell)^{\mathcal{Q}}_{/\overline{\mathbb{F}}_p}$.*

Thus if $\sum_\delta f_\delta([\delta\mathfrak{a}]) = 0$ for all $\mathfrak{a} \in \Xi$ for $(f_\delta)_{\delta\in\mathcal{Q}}$ with modular form f_δ on $X_0(N)$, the individual f_δ vanishes.

To relate the theorem to Chai's Hecke orbit conjecture, write $\mathcal{Q} = (\delta_1, \ldots, \delta_h)$. we take the CM point $x_j = (X(\mathfrak{a}), \eta^{(p)}) \in Y^{(p)}$. Let $\rho : R^\times_{(p)} \to \mathrm{Aut}(Y^{(p)})$ given by $\alpha\eta^{(p)} = \eta^{(p)}\rho(\alpha)$. We let $\mathcal{T} = R^{(p)}/\mathbb{Z}^\times_{(p)}$ act on V^h by $\prod_j \rho$. This action fix $x = (x, \cdots, x)$. Theorem 3.2 in turn follows from the following theorem proving a version of Chai's Hecke orbit conjecture:

Theorem 3.3 (C.-L. Chai)**.** *Let $\mathcal{T}$ acts on $V_{/\overline{\mathbb{F}}_p} = (Y^{(p)})^m$ diagonally. Let Z be an irreducible subvariety Z of V containing a fixed point of $\mathcal{T}$. If for a subgroup $T \subset \mathcal{T}$ whose p-adic closure is open in $R^\times_p/\mathbb{Z}^\times_p$ leaves Z stable, then Z is a Shimura subvariety of V.*

We admit this theorem basically proven in [C2] Section 8 (see also [H06a] Corollary 3.13). In [C2] Section 8, a weakly Tate-linear subvariety of V is proved to be a Shimura subvariety. In [H06a], the subvariety stable under T is proved to be weakly Tate-linear. See these papers for the definition of Tate-linearity.

After permutation of factors $Y^{(p)}$, any nontrivial Shimura subvariety of V is contained in $(Y^{(p)})^{m-2} \times \Delta_{g,g'}$ for $g, g' \in G(\mathbb{A}^{(p\infty)})$, where

$$\Delta_{g,g'} = \{(z \cdot g, z \cdot g')|z \in Y^{(p)}\} \overset{z \cdot g \mapsto z}{=} \{(z, z \cdot g^{-1}g')|z \in Y^{(p)}\}.$$

Note here the action of $G(\mathbb{A}^{(p\infty)})$ on $Y^{(p)}$ is a right action. Here we call a Shimura subvariety trivial if it is in $(Y^{(p)})^{m-1} \times x$ for a CM point x. Since Z contains a fixed point $(x_1, \dots, x_m)$ of $\mathcal{T}$, the elliptic curves X_i sitting over x_i are isogenous and have complex multiplication by M; so, they are isogenous. Thus, moving Z by an action of $G(\mathbb{A}^{(p\infty)})^m$, we may assume that the fixed point is $(x, x, \dots, x)$. Since $\Delta_{g,g'}$ contains a fixed point (x, x). Writing X for the elliptic curve sitting over x, $g^{-1}g'$ induces an endomorphism of X; so, $g^{-1}g' = \alpha \in M^\times$. Now we prove Theorem 3.2. Let $m = h$ and $\pi : V \to X_0(\ell)^{\mathcal{Q}}$ be the projection. Let Z_1 be the Zariski closure of $\pi^{-1}(\Xi)$. Since the action of $\alpha \in \mathcal{T}$ permutes points in $\pi^{-1}(\Xi^{\mathcal{Q}})$ if $\alpha \equiv 1 \mod \ell^n$ for $n = n_1$ (by (3.2)), the $\mathcal{T}_1 = \{\alpha \in \mathcal{T}|\alpha \equiv 1 \mod \ell^n\}$ leaves Z_1 stable. Take an irreducible component Z of Z_1 containing $(x(R_n), \dots, x(R_n))$. Then the stabilizer of $\mathcal{T}_1$ of Z is of finite index in $\mathcal{T}_1$ whose p-adic closure in $R_p^\times/\mathbb{Z}_p^\times$ is an open subgroup. Thus we can apply Chai's theorem. After permuting the factors of V, $Z \subset (Y^{(p)})^{h-2} \times \Delta_{g,g'}$. Thus $\delta_{h-1}/\delta_h = g^{-1}g' = \alpha$ in $\mathrm{Aut}(\widehat{Y}_x^{(p)})$. Since $\widehat{Y}_x^{(p)} \cong \widehat{\mathbb{G}}_m = \mathrm{Spf}(\widehat{\mathbb{Z}_p[t, t^{-1}]})$ and $\mathrm{Aut}(\widehat{\mathbb{G}}_m) = \mathbb{Z}_p^\times$ via $\mathbb{Z}_p^\times \ni \alpha \mapsto (t \mapsto t^\alpha) \in \mathrm{Aut}(\widehat{\mathbb{G}}_m)$, this implies $\delta_{h-1}I = \delta_h I$, a contradiction. Thus $Z = V$ and hence Theorem 3.2 follows.

3.4. **Nonvanishing of L–values modulo p.** If $\int \chi dE = 0$ for all characters $\chi : Cl_\infty \to \overline{\mathbb{F}}_p^\times$, then by orthogonality relation, we find $E([\mathfrak{a}]) = 0$ for all $\mathfrak{a} \in Cl_n$ for all n. Then a trivial form of the density theorem applied to the single copy $X_0(\ell)$ tells us that the individual E has to vanish on $X_0(\ell)$, which is a contradiction because the q-expansion of E does not vanish modulo p.

We want to get the same type of contradiction only assuming the vanishing of the integral for infinitely many χ. The technique of Sinnott still allows us to do this under the stronger form of the density theorem if the measure were supported by $\mathbb{Z}_\ell$-torsion free group (instead of Cl_∞). Thus we want to have a measure on a torsion-free group still interpolating $E([\mathfrak{a}])$.

We decompose $Cl_\infty = \Gamma \times \Delta$ with a torsion-free subgroup $\Gamma \cong \mathbb{Z}_\ell$ and a finite group Δ. We project the measure dE down to Γ and write it dE_Γ. To make explicit this measure dE_Γ, we choose a complete representative set $\mathcal{Q}$ for $Cl_\infty/\Gamma \cong \Delta$ made of split primes $\mathfrak{q}$. We write $q = N(\mathfrak{q})$ which is a rational prime. Pick $\mathfrak{q} \in \mathcal{Q}$, and write $(q) =$

$\mathfrak{q}\mathfrak{q}'$. At q, we choose $w_{1,q}$ and $w_{2,q}$ for the idempotent of $R_{\mathfrak{q}}$ and $R_{\mathfrak{q}'}$, respectively. Then for the degeneration map $f|[q](z) = q^{2k-1}f(qz)$, $f|[q]([\mathfrak{a}]) = f([\mathfrak{a}\mathfrak{q}^{-1}])$.

For simplicity, we assume that M ramifies at only one prime (to avoid appearance of nontrivial ambiguous class). Then the projection $\{[\mathfrak{q}]_\Gamma\}_{\mathfrak{q}\in\mathcal{Q}}$ to Γ is independent modulo I.

Then by computation, we get

$$\int_\Gamma \phi(x)dE_\Gamma(x) = \sum_{\mathfrak{q}\in\mathcal{Q}} \int_\Gamma \phi([\mathfrak{q}]_\Gamma^{-1}x)d(E|[q])(x).$$

We suppose a weaker condition that we have a infinitely many characters $\{\chi_j : \Gamma \to \mu_{\ell^\infty}\}_{j=1,2,\dots,\infty}$ with vanishing integral $\int_\Gamma \chi_j dE_\Gamma = 0$. Take a sequence of integers n_j so that χ_j factors through Cl_{n_j}. By a technique invented by Sinnott, from the stronger form of the density theorem for the sequence $\{n_j\}_j$, we can conclude the vanishing of $E|[q]$ on the $\mathfrak{q}$-th copy $X_0(\ell)$ if for each $\sigma \in \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_q)$ (if $\lambda \mod \mathfrak{P}$ has values in $\mathbb{F}_q^\times$), we have

$$\text{(S)} \qquad \int_\Gamma \chi^\sigma dE_\Gamma = 0 \Leftrightarrow \int_\Gamma \chi dE_\Gamma = 0.$$

This assertion (S) follows from the reciprocity law at the CM point $x(\mathfrak{a})$ in the following way: The reciprocity law (of Kronecker-Shimura; see [PAF] 2.1.4) tells us that for the Frobenius map $\Phi(x) = x^p$ for $x \in \overline{\mathbb{F}}_p$,

$$\Phi(E([\mathfrak{a}])) = E([\mathfrak{p}^{-1}\mathfrak{a}]),$$

where $p = \mathfrak{p}\overline{\mathfrak{p}}$ and $\mathfrak{p}$ corresponds to ι_p. Then we have (for positive integer m)

$$\Phi^m(\int_{Cl_\infty} \chi dE_\Gamma) = \chi^\sigma(\mathfrak{p}^m)\int_{Cl_\infty} \chi^\sigma dE_\Gamma,$$

which shows (S), and we get the theorem.

Let us give slightly more details of the argument. By our assumption, we have an infinite sequence of characters $\{\chi_j : \Gamma/\Gamma^{\ell^{n_j}} \to \mu_{\ell^\infty}(\overline{\mathbb{F}}_p)\}_j$ of order ℓ^{n_j} with $\int_\Gamma \chi_j dE_\Gamma = 0$, which implies by variable change: $\int_\Gamma \chi_j(x)dE_\Gamma(ax) = 0$ for any $a \in \Gamma$. Recall that λ has values in $\mathbb{F}_q^\times$ (for $q = p^r$). By (S), taking the trace of $\int_\Gamma \chi(x)dE_\Gamma(ax)$ from the field $\mathbb{F}_q[\chi_j]$ generated by the values of χ_j to $\mathbb{F}_q[\mu_\ell]$, we find that, putting $\Psi(x) = \sum_{\mathfrak{q}\in\mathcal{Q}} E|[\mathfrak{q}]([\mathfrak{q}]_\Gamma x)$,

$$\sum_{u\in\chi_j^{-1}(\mathbb{F}_q[\mu_\ell])} \chi_j(u)\Psi(au) = 0$$

for all $a \in \Gamma/\Gamma^{\ell^{n_j}}$. Writing the order of the ℓ–primary part of $(\mathbb{F}_q[\mu_\ell])^\times$ as ℓ^m, note that the above sum only involves $u \in \Gamma^{\ell^{n_j-m}}/\Gamma^{\ell^{n_j}}$. Taking n_j so that $n_j \geq 2m$, we can identify the multiplicative group $\Gamma^{\ell^{n_j-m}}/\Gamma^{\ell^{n_j}}$ with the additive one $\mathbb{Z}/\ell^m\mathbb{Z}$ by $\mathbb{Z}/\ell^m\mathbb{Z} \ni v \mapsto 1+\ell^{n_j-m}v = u$, and $u[\mathfrak{a}] = \left(\begin{smallmatrix} 1 & v/\ell^m \\ 0 & 1 \end{smallmatrix}\right)[\mathfrak{a}]$ by (3.3). We can then write $\chi_j(u) = \zeta_m^{b_j v}$ for $b_j \in (\mathbb{Z}/\ell^m\mathbb{Z})^\times$ and $\zeta_n^{au} = \zeta_n^a \zeta_m^v$. Since $\{\chi_j\}$ is infinite, we may assume that b_j is a constant b. We have for any $a \in \Gamma$, by (3.3)

$$\sum_{v \mod \ell^m} \zeta_m^{bv}\Psi(au) = \sum_{v \mod \ell^m} \zeta_m^{bv}\Psi|\left(\begin{smallmatrix} 1 & v/\ell^m \\ 0 & 1 \end{smallmatrix}\right)(a) = 0.$$

Since $\pi(\Xi)$ is still dense in Y, by the density theorem, we have

$$E_b = \sum_{v \mod \ell^m} \zeta_m^{bv} E|[q]|\left(\begin{smallmatrix} 1 & v/\ell^m \\ 0 & 1 \end{smallmatrix}\right) = 0.$$

By computing q-expansion, the q-expansion coefficient $a(n, E_b)$ of E_b for q^n for $n \equiv -b \mod \ell^m$ is equal to $\ell^m a(n, E|[q])$, and we can easily find such n with $a(n, E|[q]) \not\equiv 0 \mod p$, a contradiction, which proves the desired assertion.

References

Books

[ALG] R. Hartshorne, *Algebraic Geometry*, Graduate Texts in Mathematics **52**, Springer, New York, 1977.

[GME] H. Hida, *Geometric Modular Forms and Elliptic Curves*, World Scientific, Singapore, 2000.

[IAT] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*, Princeton University Press, Princeton, NJ, and Iwanami Shoten, Tokyo, 1971.

[ICF] L. C. Washington, *Introduction to Cyclotomic Fields*, Graduate Text in Mathematics, **83**, Springer, New York, 1980.

[LFE] H. Hida, *Elementary Theory of L-Functions and Eisenstein Series*, LMSST **26**, Cambridge University Press, Cambridge, England, 1993.

[PAF] H. Hida, *p-Adic Automorphic Forms on Shimura Varieties*, Springer Monographs in Mathematics, 2004, Springer

Articles

[C] C.-L. Chai, A rigidity result for p–divisible formal groups, preprint, 2003 (downloadable at: `www.math.upenn.edu/~chai`)

[C1] C.-L. Chai, Hecke orbits on Siegel modular varieties, preprint, 2004 (downloadable at: `www.math.upenn.edu/~chai`)

[C2] C.-L. Chai, Families of ordinary abelian varieties: canonical coordinates, p-adic monodromy, Tate-linear subvarieties and Hecke orbits, preprint 2003 (downloadable at: `www.math.upenn.edu/~chai`)

[FW] B. Ferrero and L. Washington, The Iwasawa invariant μ_p vanishes for abelian number fields, Ann. of Math. **109** (1979), 377–395

[Fi] T. Finis, Divisibility of anticyclotomic L–functions and theta functions with complex multiplication, preprint 2001, to appear in Annals of Math.

[H04] H. Hida, Non-vanishing modulo p of Hecke L–values, in: "*Geometric Aspects of Dwork's Theory, II*" (edited by Alan Adolphson, Francesco Baldassarri, Pierre Berthelot, Nicholas Katz, and Francois Loeser), Walter de Gruyter, 2004, pp. 735–784 (preprint downloadable at www.math.ucla.edu/~hida)

[H06a] H. Hida, The Iwasawa μ–invariant of p–adic Hecke L–functions, preprint, 2004 (preprint downloadable at www.math.ucla.edu/~hida)

[H06b] H. Hida, Non-vanishing modulo p of Hecke L–values and application, to appear in the Proceedings of the Durham symposium, 2004 (preprint downloadable at www.math.ucla.edu/~hida)

[Si] W. Sinnott, On the μ–invariant of the Γ–transform of a rational function, Inventiones Math. **75** (1984), 273–282

[Si1] W. Sinnott, On a theorem of L. Washington, Astérisque **147-148** (1987), 209–224

[V] V. Vatsal, Uniform distribution of Heegner points, Invent. Math. **148** (2002), 1–46

[V1] V. Vatsal, Special values of anticyclotomic L-functions. Duke Math. J. **116** (2003), 219–261

[W] L. Washington, Class numbers and $\mathbb{Z}_p$-extensions, Math. Ann. **214**(1975), 177–193

[W1] L. Washington, The non-p–part of the class number in a cyclotomic $\mathbb{Z}_p$–extension, Inventiones Math. **49** (1978), 87–97