

VARIATION OF HEEGNER POINTS IN HIDA FAMILIES

BENJAMIN HOWARD

ABSTRACT. Given a weight two modular form f with associated p -adic Galois representation V_f , for certain quadratic imaginary fields K one can construct canonical classes in the Galois cohomology of V_f by taking the Kummer images of Heegner points on the modular abelian variety attached to f . We show that these classes can be interpolated as f varies in a Hida family and construct an Euler system of big Heegner points for Hida's universal ordinary deformation of V_f . We show that the specialization of this big Euler system to any form in the Hida family is nontrivial, extending results of Cornut and Vatsal from modular forms of weight two and trivial character to all ordinary modular forms, and propose a horizontal nonvanishing conjecture for these cohomology classes. The horizontal nonvanishing conjecture implies, via the theory of Euler systems, a conjecture of Greenberg on the generic ranks of Selmer groups in Hida families.

1. INTRODUCTION

Fix a positive integer N and a prime $p \nmid N$, and fix, once and for all, embeddings of algebraic closures $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$, $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$. We denote by $\omega : (\mathbb{Z}/p\mathbb{Z})^\times \rightarrow \mu_{p-1}$ the Teichmüller character and view ω also as a Dirichlet character modulo Np . Let

$$g = \sum_{n>0} a_n q^n \in S_k(\Gamma_0(Np), \omega^j)$$

be a normalized eigenform (for all Hecke operators T_ℓ for $\ell \nmid Np$ and U_ℓ for $\ell \mid Np$) of weight $k \geq 2$ and character ω^j . The existence of such a form implies $j \equiv k \pmod{2}$. Fix a finite extension F/\mathbb{Q}_p which contains all Fourier coefficients of g and let \mathcal{O}_F denote the ring of integers of F . We assume that g is an *ordinary p -stabilized newform* in the sense that $a_p \in \mathcal{O}_F^\times$ and the conductor of g is divisible by N , (i.e. the system of Hecke eigenvalues $\{a_n \mid (n, Np) = 1\}$ of g agrees with that of a new eigenform of level N or Np). Let $\rho_g : G_{\mathbb{Q}} \rightarrow \mathrm{GL}_2(F)$ be the p -adic Galois representation attached to g by Deligne. Fix a quadratic imaginary field K .

Hypothesis 1.0.1. The data of the previous paragraph is to remain fixed throughout this article, and the following hypotheses are assumed throughout:

- (a) $p \nmid 6N$;
- (b) there is an ideal \mathfrak{N} of the maximal order \mathcal{O} of K such that $\mathcal{O}/\mathfrak{N} \cong \mathbb{Z}/N\mathbb{Z}$;
- (c) the semi-simple residual representation attached to ρ_g is absolutely irreducible.

Note that we impose no hypotheses on the behavior of p in K ; p may be split, ramified, or inert. For the remainder of the introduction we will also assume that $p \nmid \phi(N)$ (Euler's function) and that N is relatively prime to $\mathrm{disc}(K)$, so that the existence of the ideal \mathfrak{N} implies that all prime divisors of N are split in K .

In §2.1 we recall Hida's definition of a local domain R , finite and flat over the Iwasawa algebra $\Lambda = \mathcal{O}_F[[1 + p\mathbb{Z}_p]]$, whose arithmetic prime ideals parametrize the *Hida family* of g . We also recall Hida's construction of a big Galois representation \mathbf{T} which is free of rank two over R and admits a twist \mathbf{T}^\dagger possessing a perfect alternating pairing $\mathbf{T}^\dagger \times \mathbf{T}^\dagger \rightarrow R(1)$. The main result of this article is the construction, for every positive integer c prime to N , of a canonical cohomology class

$$\mathfrak{X}_c \in \tilde{H}_f^1(H_c, \mathbf{T}^\dagger)$$

where H_c is the ring class field of K of conductor c and $\tilde{H}_f^1(H_c, \mathbf{T}^\dagger)$ is Nekovář's extended Selmer group. As the conductor c varies the classes \mathfrak{X}_c form an Euler system in the sense of Kolyvagin. The construction and basic properties of the classes \mathfrak{X}_c are given in §2.2-2.4.

To any arithmetic prime ideal $\mathfrak{p} \subset R$ Hida's theory associates an ordinary modular form $g_{\mathfrak{p}}$ with coefficients in $F_{\mathfrak{p}}$, the residue field of the localization $R_{\mathfrak{p}}$ (so that $F_{\mathfrak{p}}$ is a finite extension of \mathbb{Q}_p). If we define a Galois representation $V_{\mathfrak{p}}^\dagger = \mathbf{T}^\dagger \otimes_R F_{\mathfrak{p}}$ then $V_{\mathfrak{p}}^\dagger$ is a self-dual twist of the p -adic Galois representation attached to $g_{\mathfrak{p}}$ by Deligne. Applying the map on cohomology induced by $\mathbf{T}^\dagger \rightarrow V_{\mathfrak{p}}^\dagger$ to the classes \mathfrak{X}_c we obtain an Euler system for $V_{\mathfrak{p}}^\dagger$. In the case of weight 2 and trivial character this construction essentially recovers the Kummer images of classical Heegner points on modular abelian varieties. In §3.1 and §3.2 we show that the image of \mathfrak{X}_{p^s} in $\tilde{H}_f^1(H_{p^s}, V_{\mathfrak{p}}^\dagger)$ is nontrivial for $s \gg 0$. The precise result, Corollary 3.1.2, is actually somewhat stronger and extends Cornut and Vatsal's proof of Mazur's conjecture on the nonvanishing of Heegner points from the case of modular forms of weight two and trivial character to all ordinary modular forms. Given this nonvanishing result, a suitable extension of Kolyvagin's theory of Euler systems would prove that

$$(1) \quad \dim_{F_{\mathfrak{p}}} \tilde{H}_f^1(D_s, V_{\mathfrak{p}}^\dagger) = p^s + O(1)$$

for every form $g_{\mathfrak{p}}$ in the Hida family. Here D_s is the subfield of the anticyclotomic \mathbb{Z}_p -extension of K (i.e. the unique \mathbb{Z}_p -extension contained in $\cup H_{p^s}$) having degree p^s over K . The weaker result that (1) holds for all but finitely many $g_{\mathfrak{p}}$, and for all $g_{\mathfrak{p}}$ of weight 2, has been proved by Nekovář ([25] Theorems 12.9.11(ii) and 12.9.8(i), respectively).

In §3.3 and §3.4 we propose two conjectures. The first, Conjecture 3.3.1, is a two-variable extension of Perrin-Riou's [29] Iwasawa main conjecture for Heegner points. As above, a suitable extension of the theory of Euler systems would prove one divisibility of this conjecture. See [1, 12, 13] for results toward Perrin-Riou's original conjecture. The second conjecture, Conjecture 3.4.1, is that the corestriction of \mathfrak{X}_1 from H_1 to K is not R -torsion. This conjecture implies, by an extension of Kolyvagin's theory due to Nekovář, a conjecture of Greenberg [7] predicting that the $F_{\mathfrak{p}}$ dimension of the Selmer group $\tilde{H}_f^1(\mathbb{Q}, V_{\mathfrak{p}}^\dagger)$ is equal to zero or one (depending on the sign of the functional equation of the Hida family of g) for all but finitely many $g_{\mathfrak{p}}$ in the Hida family. See Corollary 3.4.3.

We remark that higher weight analogs of Heegner points have been constructed elsewhere in the literature, e.g. [14, 23, 24, 35], using special cycles on Kuga-Sato varieties. Our method is completely different. For ordinary modular forms of even weight and trivial character both constructions are valid, and in these cases it would be interesting to understand the connection between the two.

The author wishes to express his thanks to J. Pottharst for pointing out the ambiguity in Θ discussed in Remark 2.1.4, and to the anonymous referee for providing helpful comments on an earlier version of this article.

Throughout the article Galois cohomology is always understood to mean continuous cohomology.

2. BIG HEEGNER POINTS

Set $\Phi_s = \Gamma_0(N) \cap \Gamma_1(p^s) \subset \mathrm{SL}_2(\mathbb{Z})$ and let Y_s denote the affine modular curve classifying elliptic curves with Φ_s level structure, by which we mean a triple consisting of an elliptic curve E , a cyclic order N subgroup of E , and a point of exact order p^s on E . Let $Y_s \hookrightarrow X_s$ be the usual compactification obtained by adjoining cusps and let J_s be the Jacobian of X_s . Denote by

$$X_{s+1} \xrightarrow{\alpha} X_s$$

the degeneracy map which is given by $(E, C, \pi) \mapsto (E, C, p \cdot \pi)$ on the affine curve Y_{s+1} . We view Y_s , X_s , and J_s as schemes over $\mathrm{Spec}(\mathbb{Q})$.

2.1. Hida theory. We recall the basic facts of Hida theory that we need; the reader may refer to [5, 8, 9, 25] for more details. Identify μ_{p-1} with $(\mathbb{Z}/p\mathbb{Z})^\times$ using the Teichmüller character and abbreviate

$$\Gamma = 1 + p\mathbb{Z}_p \quad \Delta = (\mathbb{Z}/p\mathbb{Z})^\times$$

so that $\mathbb{Z}_p^\times \cong \Delta \times \Gamma$. Define the Iwasawa algebra $\Lambda = \mathcal{O}_F[[\Gamma]]$ and write $z \mapsto [z]$ for the inclusion of group-like elements $\mathbb{Z}_p^\times \rightarrow \mathcal{O}_F[[\mathbb{Z}_p^\times]]^\times$. For each $i \in \mathbb{Z}/(p-1)\mathbb{Z}$ define an idempotent $e_i \in \mathcal{O}_F[[\mathbb{Z}_p^\times]]$ by

$$e_i = \frac{1}{p-1} \sum_{\delta \in \Delta} \omega^{-i}(\delta) [\delta]$$

Let $\mathcal{O}_F[[\mathbb{Z}_p^\times]] \rightarrow \mathfrak{h}^{\mathrm{ord}}$ be Hida's big ordinary Hecke algebra of tame level N , defined as follows. Let $\mathfrak{h}_{r,s}$ be the \mathcal{O}_F -algebra generated by all Hecke operators T_ℓ for $\ell \nmid Np$, together with the operators U_ℓ for $\ell \mid Np$ and the nebentype operators $\langle m \rangle$ for $m \in (\mathbb{Z}/p^s\mathbb{Z})^\times$, acting on the space of p -adic cusp forms $S_r(\Phi_s, \overline{\mathbb{Q}}_p)$. We make $\mathfrak{h}_{r,s}$ into an $\mathcal{O}_F[[\mathbb{Z}_p^\times]]$ -algebra by $[z] \mapsto z^{r-2} \langle z \rangle$ (this normalization differs from much of the literature, in which $[z] \mapsto z^r \langle z \rangle$; our normalization is chosen so that the action of $[z]$ agrees with $\langle z \rangle$ in weight two). Note that $[-1] \mapsto 1$ as $\langle -1 \rangle$ acts as $(-1)^r$ on modular forms of weight r . Hida's ordinary projector $e^{\mathrm{ord}} = \lim U_p^{m!}$ defines an idempotent in each $\mathfrak{h}_{r,s}$, and these are compatible with the natural surjections $\mathfrak{h}_{r,s+1} \rightarrow \mathfrak{h}_{r,s}$. If we define $\mathfrak{h}_{r,s}^{\mathrm{ord}} = e^{\mathrm{ord}} \mathfrak{h}_{r,s}$ then the algebra

$$\mathfrak{h}^{\mathrm{ord}} = \varprojlim_s \mathfrak{h}_{r,s}^{\mathrm{ord}}$$

is finite and flat over Λ and is independent of the weight r by [9, Theorem 1.1].

Definition 2.1.1. If A is any finitely generated commutative Λ -algebra then an \mathcal{O}_F -algebra map $A \rightarrow \overline{\mathbb{Q}}_p$ is *arithmetic* if the composition

$$\Gamma \xrightarrow{\gamma \mapsto [\gamma]} A^\times \rightarrow \overline{\mathbb{Q}}_p^\times$$

has the form $\gamma \mapsto \psi(\gamma)\gamma^{r-2}$ for some integer $r \geq 2$ and some finite order character ψ of Γ . The kernel of an arithmetic map is an *arithmetic prime* of A . If \mathfrak{p} is an arithmetic prime then the residue field $F_{\mathfrak{p}} = A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}$ is a finite extension of F .

The composition $\Gamma \rightarrow A^\times \rightarrow F_{\mathfrak{p}}^\times$ has the form $\gamma \mapsto \psi_{\mathfrak{p}}(\gamma)\gamma^{r-2}$ for a finite order character $\psi_{\mathfrak{p}} : \Gamma \rightarrow F_{\mathfrak{p}}^\times$ called the *wild character* of \mathfrak{p} and an integer r called the *weight* of \mathfrak{p} .

Our fixed cuspform g determines an arithmetic map (denoted the same way)

$$g : \mathfrak{h}^{\text{ord}} \rightarrow \mathfrak{h}_{k,1}^{\text{ord}} \rightarrow \mathcal{O}_F$$

characterized by $T_\ell \mapsto a_\ell$ for $\ell \nmid Np$, $U_\ell \mapsto a_\ell$ for $\ell \mid Np$, and

$$[\delta] \mapsto \omega^{k+j-2}(\delta) \quad [\gamma] \mapsto \gamma^{k-2}$$

for $\delta \in \Delta$ and $\gamma \in \Gamma$. There is a decomposition of $\mathfrak{h}^{\text{ord}}$ as a direct sum of its completions at maximal ideals, and we let $\mathfrak{h}_{\mathfrak{m}}^{\text{ord}}$ be the unique local summand through which g factors. As $g(e_i) = 0$ for $i \neq k + j - 2$, we must have

$$\mathfrak{h}_{\mathfrak{m}}^{\text{ord}} = e_{k+j-2} \mathfrak{h}_{\mathfrak{m}}^{\text{ord}}.$$

According to [25, §12.7.5] the localization of $\mathfrak{h}_{\mathfrak{m}}^{\text{ord}}$ at the kernel of g is a discrete valuation ring. It follows that there is a unique minimal prime $\mathfrak{a} \subset \mathfrak{h}_{\mathfrak{m}}^{\text{ord}}$ such that g factors through the integral domain

$$R \stackrel{\text{def}}{=} \mathfrak{h}_{\mathfrak{m}}^{\text{ord}} / \mathfrak{a}.$$

If we let \mathcal{L} and \mathcal{K} denote the fraction fields of Λ and R , respectively, then \mathcal{K} is a finite extension of \mathcal{L} and is the (primitive) component of $\mathfrak{h}_{\mathfrak{m}}^{\text{ord}} \otimes_{\Lambda} \mathcal{L}$ to which g belongs in the sense of [9, §1]. The Λ -algebra $\mathfrak{h}_{\mathfrak{m}}^{\text{ord}}$ is the *Hida family* of g and R is the *branch* of the Hida family on which g lives. Define $\mathfrak{h}^{\text{ord}}$ -modules

$$\begin{aligned} \text{Ta}_p^{\text{ord}}(J_s) &= e^{\text{ord}}(\text{Ta}_p(J_s) \otimes_{\mathbb{Z}_p} \mathcal{O}_F) \\ \mathbf{Ta}^{\text{ord}} &= \varprojlim \text{Ta}_p^{\text{ord}}(J_s) \\ \mathbf{Ta}_{\mathfrak{m}}^{\text{ord}} &= \mathbf{Ta}^{\text{ord}} \otimes_{\mathfrak{h}^{\text{ord}}} \mathfrak{h}_{\mathfrak{m}}^{\text{ord}} \\ \mathbf{T} &= \mathbf{Ta}_{\mathfrak{m}}^{\text{ord}} \otimes_{\mathfrak{h}^{\text{ord}}} R \end{aligned}$$

(the Hecke operators T_ℓ , U_ℓ , and $\langle \ell \rangle$ act on J_s and on the Tate module $\text{Ta}_p(J_s)$ via the Albanese action as in [20, p. 236], and the inverse limit in the second definition is with respect to α_*). All four modules admit natural $\mathfrak{h}^{\text{ord}}$ -linear actions of $G_{\mathbb{Q}}$.

Proposition 2.1.2. *The $\mathfrak{h}_{\mathfrak{m}}^{\text{ord}}$ -module $\mathbf{Ta}_{\mathfrak{m}}^{\text{ord}}$ is free of rank two. As a Galois representation $\mathbf{Ta}_{\mathfrak{m}}^{\text{ord}}$ is unramified outside Np and the arithmetic Frobenius of a prime $\ell \nmid Np$ acts with characteristic polynomial $X^2 - T_\ell X + [\ell]\ell$. Furthermore,*

$$\mathfrak{h}_{\mathfrak{m}}^{\text{ord}} \cong \text{Hom}_{\Lambda}(\mathfrak{h}_{\mathfrak{m}}^{\text{ord}}, \Lambda)$$

as $\mathfrak{h}_{\mathfrak{m}}^{\text{ord}}$ -modules.

Proof. As we assume that the residual representation attached to ρ_g is irreducible, this is [19, Théorème 7]. \square

Definition 2.1.3. Factor the p -adic cyclotomic character $\epsilon_{\text{cyc}} = \epsilon_{\text{tame}} \cdot \epsilon_{\text{wild}}$ as a product of characters taking values in μ_{p-1} and $1 + p\mathbb{Z}_p$. Define the *critical character* $\Theta : G_{\mathbb{Q}} \rightarrow \Lambda^\times$ by

$$\Theta = \epsilon_{\text{tame}}^{\frac{k+j}{2}-1} \cdot [\epsilon_{\text{wild}}^{1/2}]$$

where $\epsilon_{\text{wild}}^{1/2}$ is the unique square root of ϵ_{wild} taking values in $1 + p\mathbb{Z}_p$. Let R^\dagger denote R viewed as a module over itself but with $G_{\mathbb{Q}}$ acting through Θ^{-1} , and define the *critical twist* $\mathbf{T}^\dagger = \mathbf{T} \otimes_R R^\dagger$.

Remark 2.1.4. The integer j of the introduction is determined only modulo $p-1$, and the resulting ambiguity in $\frac{k+j}{2}$ modulo $p-1$ means that Θ is determined only up to multiplication by the quadratic character of conductor p . The two possible choices of Θ arising from the two possible choices of j modulo $2(p-1)$ are largely indistinguishable for our purposes, although the sign in the functional equation of the two variable p -adic L -function of R , evaluated at Θ and viewed as a function on arithmetic primes, may depend on the choice. See Remark 2.3.4 and Proposition 2.3.6. We now fix a choice of Θ once and for all.

Using ω to identify $\Delta \cong \mu_{p-1}$, the idempotent $e_{k+j-2} \in \mathcal{O}_F[[\mathbb{Z}_p^\times]]$ satisfies

$$e_{k+j-2} \cdot [\zeta] = \zeta^{k+j-2} \cdot e_{k+j-2}$$

for any $\zeta \in \mu_{p-1}$. As noted earlier $\mathfrak{h}_m^{\text{ord}} = e_{k+j-2} \mathfrak{h}_m^{\text{ord}}$, and so $[\epsilon_{\text{tame}}] = \epsilon_{\text{tame}}^{k+j-2}$ in $\mathfrak{h}_m^{\text{ord}}$. It follows that

$$(2) \quad \Theta^2(\sigma) = [\epsilon_{\text{cyc}}(\sigma)]$$

in $\mathfrak{h}_m^{\text{ord}}$ for all $\sigma \in G_{\mathbb{Q}}$. We will sometimes view Θ as a character $\mathbb{Z}_p^\times \rightarrow \Lambda^\times$ by factoring Θ through $\text{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})$ and using the isomorphism

$$\epsilon_{\text{cyc}} : \text{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) \cong \mathbb{Z}_p^\times.$$

Then for all $z \in \mathbb{Z}_p^\times$, $\Theta^2(z) = [z]$ as elements of $\mathfrak{h}_m^{\text{ord}}$. Similarly for any weight r arithmetic prime \mathfrak{p} of R , define $F_{\mathfrak{p}}^\times$ -valued characters

$$\Theta_{\mathfrak{p}} : G_{\mathbb{Q}} \xrightarrow{\Theta} R^\times \rightarrow F_{\mathfrak{p}}^\times \quad [\cdot]_{\mathfrak{p}} : \mathbb{Z}_p^\times \xrightarrow{[\cdot]} R^\times \rightarrow F_{\mathfrak{p}}^\times.$$

As above we may view $\Theta_{\mathfrak{p}}$ as a character of \mathbb{Z}_p^\times , so that

$$\Theta_{\mathfrak{p}}(\delta\gamma) = \omega^{\frac{k+j}{2}-1}(\delta) \cdot \psi_{\mathfrak{p}}^{1/2}(\gamma) \cdot \gamma^{\frac{r-2}{2}}$$

for all $\delta \in \Delta$ and $\gamma \in \Gamma$.

By [26, §1.6.10] or [28, §4] and (2) there is a perfect, alternating, $G_{\mathbb{Q}}$ -invariant, Λ -bilinear pairing

$$\mathbf{Ta}_m^{\text{ord}} \times \mathbf{Ta}_m^{\text{ord}} \rightarrow \Lambda(1) \otimes \Theta^2$$

where $\Lambda(1)$ denotes the usual Tate twist of Λ (and the unadorned Λ has trivial Galois action). By the discussion of [26, §1.6.10] and the final claim of Proposition 2.1.2, this pairing induces a perfect R -bilinear pairing

$$(3) \quad \mathbf{T}^\dagger \times \mathbf{T}^\dagger \rightarrow R(1).$$

Given an arithmetic prime $\mathfrak{p} \subset R$ of weight r set $s = \max\{1, \text{ord}_{\mathfrak{p}}(\text{cond}(\psi_{\mathfrak{p}}))\}$. By a fundamental result of Hida [9, Theorem 1.2] the composition

$$\mathfrak{h}^{\text{ord}} \rightarrow \mathfrak{h}_m^{\text{ord}} \rightarrow R \rightarrow F_{\mathfrak{p}}$$

factors through $\mathfrak{h}_{r,s}^{\text{ord}}$ and determines an ordinary p -stabilized newform

$$g_{\mathfrak{p}} \in S_r(\Phi_s, \psi_{\mathfrak{p}} \omega^{k+j-r}, F_{\mathfrak{p}}).$$

We define a Galois representation

$$V_{\mathfrak{p}}^\dagger = \mathbf{T}^\dagger \otimes_R F_{\mathfrak{p}} \cong \mathbf{T}_{\mathfrak{p}}^\dagger / \mathfrak{p} \mathbf{T}_{\mathfrak{p}}^\dagger.$$

Tensoring the pairing (3) with $F_{\mathfrak{p}}$ yields an alternating nondegenerate pairing

$$V_{\mathfrak{p}}^\dagger \times V_{\mathfrak{p}}^\dagger \rightarrow F_{\mathfrak{p}}(1).$$

Lemma 2.1.5. *Suppose \mathfrak{p} is an arithmetic prime of R of weight $r > 2$ and trivial character (so that r must be even). Then the form $g_{\mathfrak{p}} \in S_r(\Gamma_0(Np), F_{\mathfrak{p}})$ is old at p .*

Proof. If $g_{\mathfrak{p}}$ were new at p then U_p would act with eigenvalue $\alpha_{\mathfrak{p}}$ satisfying $\alpha_{\mathfrak{p}}^2 = p^{r-2}$ [22, Theorem 4.6.17], contradicting $g_{\mathfrak{p}}$ being ordinary. \square

Lemma 2.1.6. *For any arithmetic prime $\mathfrak{p} \subset R$ the localization $R_{\mathfrak{p}}$ is a discrete valuation ring.*

Proof. This follows from the discussion of [25, §12.7.5]. \square

Lemma 2.1.7. *Suppose M is a finitely generated R -module and $m \in M$ is non-torsion. Then $m \notin \mathfrak{p}M_{\mathfrak{p}}$ for all but finitely many arithmetic primes $\mathfrak{p} \subset R$.*

Proof. Let $I \subset R$ be the image of the map $\text{Hom}_R(M, R) \rightarrow R$ defined by $f \mapsto f(m)$. For any arithmetic prime \mathfrak{p}

$$m \in \mathfrak{p}M_{\mathfrak{p}} \implies I \subset \mathfrak{p}R_{\mathfrak{p}} \implies (R/I)_{\mathfrak{p}} \neq 0.$$

By [17, Theorem 6.5] this can only occur for finitely many \mathfrak{p} . \square

2.2. Construction of big Heegner points. Fix a quadratic imaginary field K with maximal order \mathcal{O} as in the introduction, and an ideal \mathfrak{N} with $\mathcal{O}/\mathfrak{N} \cong \mathbb{Z}/N\mathbb{Z}$. For any positive integer c we denote by \mathcal{O}_c the order of conductor c in K and by H_c the ring class field of \mathcal{O}_c . Let $H_c^{(Np)}$ denote the maximal extension of H_c unramified outside Np and set

$$\mathfrak{G}_c = \text{Gal}(H_c^{(Np)}/H_c).$$

Let $\widehat{\mathbb{Q}}$ and \widehat{K} denote the rings of finite adèles of \mathbb{Q} and K , respectively.

Now fix a positive integer c prime to N . For each integer $s \geq 0$ define an elliptic curve $E_{c,s}$ over \mathbb{C} with complex multiplication by \mathcal{O}_{cp^s} by

$$E_{c,s}(\mathbb{C}) \cong \mathbb{C}/\mathcal{O}_{cp^s}.$$

The $\mathfrak{N} \cap \mathcal{O}_{cp^s}$ -torsion subgroup

$$\mathfrak{n}_{c,s} = E_{c,s}[\mathfrak{N} \cap \mathcal{O}_{cp^s}]$$

is cyclic of order N . The inclusion $\mathcal{O}_{cp^{s+1}} \subset \mathcal{O}_{cp^s}$ induces a p -isogeny $E_{c,s+1} \rightarrow E_{c,s}$ compatible with the action of $\mathcal{O}_{cp^{s+1}}$ on the source and target, and taking $\mathfrak{n}_{c,s+1}$ isomorphically to $\mathfrak{n}_{c,s}$. The kernel of the composition

$$j_{c,s} : E_{c,s} \rightarrow E_{c,s-1} \rightarrow \cdots \rightarrow E_{c,1} \rightarrow E_{c,0}$$

is cyclic of order p^s and is characterized as the $p^s \mathcal{O}_c$ -torsion in $E_{c,s}$. Fix a generator ϖ of $\mathcal{O}/\mathbb{Z} \cong \mathbb{Z}$. Then $c\varpi$ generates

$$\ker(j_{c,s}) \cong \mathcal{O}_c/\mathcal{O}_{cp^s}$$

for every s , and defines a $\Gamma_1(p^s)$ -level structure $\pi_{c,s} = c\varpi \in E_{c,s}[p^s]$. Define

$$(4) \quad h_{c,s} = (E_{c,s}, \mathfrak{n}_{c,s}, \pi_{c,s}) \in X_s(\mathbb{C}).$$

By class field theory $\mathbb{Q}(\sqrt{p^*}) \subset H_p$, where $p^* = (-1)^{\frac{p-1}{2}}p$. The restriction of ϵ_{cyc} to $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\sqrt{p^*}))$ takes values in $(\mathbb{Z}_p^\times)^2$, and it follows that there is a unique continuous homomorphism

$$\vartheta : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\sqrt{p^*})) \rightarrow \mathbb{Z}_p^\times / \{\pm 1\}$$

such that $\vartheta^2 = \epsilon_{\text{cyc}}$.

Lemma 2.2.1. *Suppose $s > 0$. The field of moduli of $E_{c,s}$ is contained in H_{cp^s} . After fixing a model of $E_{c,s}$ over H_{cp^s} the subgroup $\mathfrak{n}_{c,s}$ is also defined over H_{cp^s} , and for each $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/H_{cp^s})$ and $P \in \ker(j_{c,s})$ the equality $P^\sigma = \vartheta(\sigma)P$ holds up to the action of $\text{Aut}_{\overline{\mathbb{Q}}}(E_{c,s}) = \{\pm 1\}$.*

Proof. Fix $\sigma \in \text{Aut}(\mathbb{C}/H_{cp^s})$ and let $x \in \widehat{K}^\times$ be a finite idele whose (arithmetic) Artin symbol is equal to the restriction of σ to the maximal abelian extension of K . Let $\widehat{\mathcal{O}}_{cp^s}$ be the closure of \mathcal{O}_{cp^s} in \widehat{K} . As σ fixes H_{cp^s} we must have $x \in K^\times \cdot \widehat{\mathcal{O}}_{cp^s}^\times$, and multiplying x by an element of K^\times we may assume $x \in \widehat{\mathcal{O}}_{cp^s}^\times$. The main theorem of complex multiplication [33, Theorem 5.4] then gives an isomorphism of complex tori

$$E_{c,s}(\mathbb{C}) \cong \mathbb{C}/\mathcal{O}_{cp^s} = \mathbb{C}/x^{-1}\mathcal{O}_{cp^s} \cong E_{c,s}^\sigma(\mathbb{C}).$$

Thus $E_{c,s}$ has a model over H_{cp^s} , which we now fix. All endomorphisms of $E_{c,s}$ are then defined over H_{cp^s} by [33, (5.1.3)], and the characterizations of $\mathfrak{n}_{c,s}$ and $\ker(j_{c,s})$ in terms of I -torsion subgroups for ideals $I \subset \mathcal{O}_{cp^s}$ shows that they are also defined over H_{cp^s} . Let $x_p \in (\mathcal{O}_{cp^s} \otimes \mathbb{Z}_p)^\times$ be the p -component of x , and write $x_p = \alpha + cp^s\beta$ with $\alpha \in \mathbb{Z}_p^\times$ and $\beta \in \mathcal{O} \otimes \mathbb{Z}_p$. In particular

$$\alpha^2 \equiv N_{K/\mathbb{Q}}(x_p) \pmod{p^s}.$$

Again applying the main theorem of complex multiplication we obtain a commutative diagram

$$\begin{array}{ccccc} \mathbb{Z}/p^s\mathbb{Z} & \longrightarrow & (\mathcal{O}_c \otimes \mathbb{Z}_p)/(\mathcal{O}_{cp^s} \otimes \mathbb{Z}_p) & \xrightarrow{\xi} & \ker(j_{c,s}) \\ \alpha^{-1} \cdot \downarrow & & x_p^{-1} \cdot \downarrow & & \downarrow \sigma \\ \mathbb{Z}/p^s\mathbb{Z} & \longrightarrow & (\mathcal{O}_c \otimes \mathbb{Z}_p)/(\mathcal{O}_{cp^s} \otimes \mathbb{Z}_p) & \xrightarrow{\xi'} & \ker(j_{c,s}) \end{array}$$

(the unlabeled horizontal arrows are the isomorphisms determined by $1 \mapsto c\varpi$) for some group isomorphisms ξ and ξ' which agree up to the action of $\mathcal{O}_{cp^s}^\times = \{\pm 1\}$. As the composition

$$\mathbb{Z}_p^\times \rightarrow \widehat{\mathbb{Q}}^\times \rightarrow \text{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) \xrightarrow{\epsilon_{\text{cyc}}} \mathbb{Z}_p^\times$$

is given by $y \mapsto y^{-1}$ and takes $N_{K/\mathbb{Q}}(x_p)$ to $\epsilon_{\text{cyc}}(\sigma)$ (the first arrow is the natural inclusion, the second is the arithmetic Artin symbol), we see that

$$\epsilon_{\text{cyc}}(\sigma) = N_{K/\mathbb{Q}}(x_p^{-1}) \equiv \alpha^{-2} \pmod{p^s}.$$

Hence the action of σ on $\ker(j_{c,s})$ is given as multiplication by the unique (up to ± 1) square root of $\epsilon_{\text{cyc}}(\sigma)$ in $(\mathbb{Z}/p^s\mathbb{Z})^\times$. \square

Corollary 2.2.2. *Suppose $s > 0$ and let $L_{c,s} = H_{cp^s}(\mu_{p^s})$. Then $h_{c,s} \in X_s(L_{c,s})$ and*

$$(5) \quad h_{c,s}^\sigma = \langle \vartheta(\sigma) \rangle \cdot h_{c,s}$$

for all $\sigma \in \text{Gal}(L_{c,s}/H_{cp^s})$.

Proof. Indeed, Lemma 2.2.1 asserts that (5) holds for all $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/H_{cp^s})$. Suppose σ fixes $L_{c,s}$. Then

$$\epsilon_{\text{cyc}}(\sigma) \equiv 1 \pmod{p^s} \implies \vartheta(\sigma) \equiv \pm 1 \pmod{p^s},$$

and so $\langle \vartheta(\sigma) \rangle$ acts trivially on X_s . \square

As in [11, §7.2 Lemma 1] we may define the ordinary projector $e^{\text{ord}} = \lim U_p^m$ acting on the Picard group $\text{Pic}(X_s/L_{c,s}) \otimes \mathcal{O}_F$. The natural short exact sequence

$$0 \rightarrow J_s(L_{c,s}) \otimes \mathcal{O}_F \rightarrow \text{Pic}(X_s/L_{c,s}) \otimes \mathcal{O}_F \xrightarrow{\text{deg}} \mathcal{O}_F \rightarrow 0,$$

is Hecke equivariant, and as the action of U_p on \mathcal{O}_F is by $p = \text{deg}(U_p)$ there is an induced isomorphism

$$J_s(L_{c,s})^{\text{ord}} \cong \text{Pic}(X_s/L_{c,s})^{\text{ord}}.$$

Here we abbreviate

$$J_s(L)^{\text{ord}} = e^{\text{ord}}(J_s(L) \otimes \mathcal{O}_F)$$

for any finite extension L/\mathbb{Q} , and similarly for the Picard group. Viewing $h_{c,s}$ as divisor on $X_s/L_{c,s}$ we obtain an element

$$e^{\text{ord}} h_{c,s} \in J_s(L_{c,s})^{\text{ord}}.$$

If $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/H_{cp^s})$ then σ fixes $\mathbb{Q}(\sqrt{p^*})$, and hence there is a $\xi \in \mu_{p-1}$ for which $\xi^2 = \epsilon_{\text{tame}}(\sigma)$. This implies $\xi \cdot \epsilon_{\text{wild}}^{1/2}(\sigma) = \pm \vartheta(\sigma)$, and so

$$\Theta(\sigma) = \xi^{k+j-2} \langle \epsilon_{\text{wild}}^{1/2}(\sigma) \rangle = \langle \xi \cdot \epsilon_{\text{wild}}^{1/2}(\sigma) \rangle = \langle \vartheta(\sigma) \rangle$$

as endomorphisms of $e_{k+j-2} J_s(L_{c,s})^{\text{ord}}$. If we define

$$y_{c,s} = e_{k+j-2} e^{\text{ord}} h_{c,s} \in J_s(L_{c,s})^{\text{ord}}$$

for every $s > 0$ then Corollary 2.2.2 implies that

$$(6) \quad y_{c,s}^\sigma = \Theta(\sigma) \cdot y_{c,s}$$

for all $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/H_{cp^s})$. Let $\mathfrak{h}_{2,s}^{\text{ord},\dagger}$ denote $\mathfrak{h}_{2,s}^{\text{ord}}$ as a module over itself but with $G_{\mathbb{Q}}$ acting through the character Θ^{-1} , and let $\zeta_s \in \mathfrak{h}_{2,s}^{\text{ord},\dagger}$ be the element corresponding to $1 \in \mathfrak{h}_{2,s}^{\text{ord}}$ under the identification of underlying $\mathfrak{h}_{2,s}^{\text{ord}}$ -modules. For any $\mathfrak{h}_{2,s}^{\text{ord}}$ -module M we abbreviate

$$M \otimes \zeta_s = M \otimes_{\mathfrak{h}_{2,s}^{\text{ord}}} \mathfrak{h}_{2,s}^{\text{ord},\dagger}.$$

The equality (6) implies that

$$y_{c,s} \otimes \zeta_s \in H^0(H_{cp^s}, J_s(L_{c,s})^{\text{ord}} \otimes \zeta_s)$$

and we define

$$x_{c,s} = \text{Cor}_{H_{cp^s}/H_c}(y_{c,s} \otimes \zeta_s) \in H^0(H_c, J_s(L_{c,s})^{\text{ord}} \otimes \zeta_s)$$

where $\text{Cor}_{H_{cp^s}/H_c}$ is corestriction. More explicitly, if for each $\eta \in \text{Gal}(H_{cp^s}/H_c)$ we fix an extension to $\text{Gal}(L_{c,s}/H_c)$ then

$$(7) \quad x_{c,s} = \left(\sum_{\eta \in \text{Gal}(H_{cp^s}/H_c)} \Theta(\eta^{-1}) \cdot y_{c,s}^\eta \right) \otimes \zeta_s \in J_s(L_{c,s})^{\text{ord}} \otimes \zeta_s.$$

We now construct a twisted Kummer map

$$\text{Kum}_s : H^0(H_c, J_s(L_{c,s})^{\text{ord}} \otimes \zeta_s) \rightarrow H^1(\mathfrak{G}_c, \text{Ta}_p^{\text{ord}}(J_s) \otimes \zeta_s).$$

Suppose $P \otimes \zeta_s \in J_s(L_{c,s})^{\text{ord}} \otimes \zeta_s$ is fixed by the action of $\text{Gal}(\overline{\mathbb{Q}}/H_c)$. For each $n > 0$ choose a finite extension $L/L_{c,s}$ contained in $H_c^{(Np)}$ large enough so that there is a point $Q_n \in J_s(L)^{\text{ord}}$ with $p^n Q_n = P$. Abbreviating

$$J_s[p^n]^{\text{ord}} = e^{\text{ord}}(J_s[p^n] \otimes \mathcal{O}_F),$$

for $\sigma \in \mathfrak{G}_c$

$$\begin{aligned} b_n(\sigma) &= (Q_n \otimes \zeta_s)^\sigma - Q_n \otimes \zeta_s \\ &= (\Theta^{-1}(\sigma)Q_n^\sigma - Q_n) \otimes \zeta_s \end{aligned}$$

defines a 1-cycle with values in

$$J_s[p^n]^{\text{ord}} \otimes \zeta_s \cong (\text{Ta}_p^{\text{ord}}(J_s)/p^n \text{Ta}_p^{\text{ord}}(J_s)) \otimes \zeta_s$$

whose image in cohomology does not depend on the choice of L or Q_n . Taking the inverse limit over n yields the desired element

$$\text{Kum}_s(P \otimes \zeta_s) = \varprojlim b_n \in H^1(\mathfrak{G}_c, \text{Ta}_p^{\text{ord}}(J_s) \otimes \zeta_s).$$

The twisted Kummer map is both $\mathfrak{h}_{2,s}^{\text{ord}}$ and $G_{\mathbb{Q}}$ equivariant. Define

$$(8) \quad \mathfrak{X}_{c,s} = \text{Kum}_s(x_{c,s}) \in H^1(\mathfrak{G}_c, \text{Ta}_p^{\text{ord}}(J_s) \otimes \zeta_s).$$

The Albanese map $\alpha_* : J_{s+1} \rightarrow J_s$ induces a map of $\mathfrak{h}^{\text{ord}}$ -modules (abusively denoted the same way)

$$\alpha_* : \text{Ta}_p^{\text{ord}}(J_{s+1}) \otimes \zeta_{s+1} \rightarrow \text{Ta}_p^{\text{ord}}(J_s) \otimes \zeta_s$$

defined by $t \otimes \zeta_{s+1} \mapsto \alpha_*(t) \otimes \zeta_s$. Taking the inverse limit with respect to α_* we obtain an $\mathfrak{h}^{\text{ord}}$ -module

$$\mathbf{Ta}^{\text{ord}} \otimes \zeta = \varprojlim (\text{Ta}_p^{\text{ord}}(J_s) \otimes \zeta_s)$$

which is precisely the module \mathbf{Ta}^{ord} constructed earlier, but with the $G_{\mathbb{Q}}$ action twisted by Θ^{-1} . In particular there is a $G_{\mathbb{Q}}$ equivariant map of $\mathfrak{h}^{\text{ord}}$ -modules

$$(9) \quad \mathbf{Ta}^{\text{ord}} \otimes \zeta \rightarrow \mathbf{T}^\dagger$$

Definition 2.2.3. By Lemma 2.2.4 below we may take the limit over s of the $\mathfrak{X}_{c,s}$ and form the cohomology class

$$(10) \quad \varprojlim U_p^{-s} \mathfrak{X}_{c,s} \in H^1(\mathfrak{G}_c, \mathbf{Ta}^{\text{ord}} \otimes \zeta).$$

Define the *big Heegner point of conductor c*

$$\mathfrak{X}_c \in H^1(\mathfrak{G}_c, \mathbf{T}^\dagger)$$

to be the image of the cohomology class (10) under the map on cohomology induced by (9).

Lemma 2.2.4. *The cohomology classes (8) satisfy $\alpha_*(\mathfrak{X}_{c,s+1}) = U_p \cdot \mathfrak{X}_{c,s}$.*

Proof. The extensions $H_{cp^s}(\mu_{p^\infty})$ and $H_{cp^{s+1}}$ of H_{cp^s} are linearly disjoint, hence we may fix a set $S \subset \text{Aut}(\mathbb{C}/H_{cp^s})$ of extensions of $\text{Gal}(H_{cp^{s+1}}/H_{cp^s})$ in such a way that each $\sigma \in S$ acts trivially on μ_{p^∞} . The map of complex tori

$$\mathbb{C}/\mathcal{O}_{cp^s} \rightarrow \mathbb{C}/\mathcal{O}_{cp^{s+1}}$$

defined by $z \mapsto pz$ determines a p -isogeny $f_s : E_{c,s} \rightarrow E_{c,s+1}$ taking $\mathfrak{n}_{c,s}$ to $\mathfrak{n}_{c,s+1}$ and $\pi_{c,s}$ to $p \cdot \pi_{c,s+1}$. That is, f_s determines an isogeny $f_s : h_{c,s} \rightarrow \alpha(h_{c,s+1})$ of elliptic curves over \mathbb{C} with Φ_s level structure. By Corollary 2.2.2 each $\sigma \in S$ fixes $h_{c,s}$, while the main theorem of complex multiplication implies that the complex tori $E_{c,s+1}^\sigma(\mathbb{C})$ as σ ranges over S are isomorphic to \mathbb{C}/\mathfrak{b} as \mathfrak{b} ranges over a set of representatives for the kernel of $\text{Pic}(\mathcal{O}_{cp^{s+1}}) \rightarrow \text{Pic}(\mathcal{O}_{cp^s})$. The set

$$\{\mathbb{C}/\mathfrak{b} \mid \mathfrak{b} \in \ker(\text{Pic}(\mathcal{O}_{cp^{s+1}}) \rightarrow \text{Pic}(\mathcal{O}_{cp^s}))\}$$

consists of p nonisomorphic complex elliptic curves, and so as σ varies over S the elliptic curves $E_{c,s+1}^\sigma$ are pairwise nonisomorphic. Hence the isogenies

$$\{f_s^\sigma : E_{c,s} \rightarrow \alpha(E_{c,s+1}^\sigma) \mid \sigma \in S\}$$

have distinct kernels and we obtain p distinct degree p isogenies of elliptic curves with Φ_s level structure

$$\{f_s^\sigma : h_{c,s} \rightarrow \alpha(h_{c,s+1}^\sigma) \mid \sigma \in S\}.$$

By definition of the U_p correspondence

$$(11) \quad U_p \cdot h_{c,s} = \sum_{\sigma \in S} \alpha(h_{c,s+1}^\sigma)$$

as divisors on $X_{s/L_{c,s}}$. Applying $e_{k+j-2} \cdot e^{\text{ord}}$ we obtain the equality in $J_s(L_{c,s})^{\text{ord}}$

$$U_p \cdot y_{c,s} = \sum_{\sigma \in S} \alpha_*(y_{c,s+1}^\sigma).$$

Twisting by ζ_s we obtain the equality in $H^0(H_{cp^s}, J_s(L_{c,s})^{\text{ord}} \otimes \zeta_s)$

$$(12) \quad \begin{aligned} U_p(y_{c,s} \otimes \zeta_s) &= \sum_{\sigma \in S} \alpha_*(y_{c,s+1}^\sigma) \otimes \zeta_s \\ &= \sum_{\sigma \in S} \alpha_*(y_{c,s+1} \otimes \zeta_{s+1})^\sigma \\ &= \alpha_*(\text{Cor}_{H_{cp^{s+1}}/H_{cp^s}}(y_{c,s+1} \otimes \zeta_{s+1})). \end{aligned}$$

Corestricting from H_{cp^s} to H_c shows that

$$U_p \cdot x_{c,s} = \alpha_*(x_{c,s+1})$$

and applying the twisted Kummer map to both sides gives

$$U_p \cdot \mathfrak{X}_{c,s} = \text{Kum}_s(\alpha_*(x_{c,s+1})) = \alpha_*(\text{Kum}_{s+1}(x_{c,s+1})) = \alpha_*(\mathfrak{X}_{c,s+1}).$$

□

2.3. Euler system relations. Keep the notation of §2.2. In particular c always denotes a positive integer prime to N and $\mathfrak{X}_c \in H^1(H_c, \mathbf{T}^\dagger)$ is the inflation to $\text{Gal}(\overline{\mathbb{Q}}/H_c)$ -cohomology of the big Heegner point of Definition 2.2.3.

Proposition 2.3.1. *Corestriction from H_{cp} to H_c takes*

$$\mathfrak{X}_{cp} \mapsto U_p \cdot \mathfrak{X}_c.$$

For any prime $\ell \nmid cN$ which is inert in K , corestriction from $H_{c\ell}$ to H_c takes

$$\mathfrak{X}_{c\ell} \mapsto T_\ell \cdot \mathfrak{X}_c.$$

Proof. Directly from the definition (4) we have the equality $h_{cp,s} = \alpha(h_{c,s+1})$ of points on $X_s(\mathbb{C})$. Tracing through the constructions of §2.2, and using (12) for the

third implication, gives

$$\begin{aligned}
 y_{cp,s} &= \alpha_*(y_{c,s+1}) \\
 \implies y_{cp,s} \otimes \zeta_s &= \alpha_*(y_{c,s+1} \otimes \zeta_{s+1}) \\
 \implies \text{Cor}_{H_{cp^{s+1}}/H_{cp^s}}(y_{cp,s} \otimes \zeta_s) &= \alpha_*(\text{Cor}_{H_{cp^{s+1}}/H_{cp^s}}(y_{c,s+1} \otimes \zeta_{s+1})) \\
 \implies \text{Cor}_{H_{cp^{s+1}}/H_{cp^s}}(y_{cp,s} \otimes \zeta_s) &= U_p \cdot (y_{c,s} \otimes \zeta_s) \\
 \implies \text{Cor}_{H_{cp^{s+1}}/H_c}(y_{cp,s} \otimes \zeta_s) &= U_p \cdot \text{Cor}_{H_{cp^s}/H_c}(y_{c,s} \otimes \zeta_s) \\
 \implies \text{Cor}_{H_{cp}/H_c}(x_{cp,s}) &= U_p \cdot x_{c,s}.
 \end{aligned}$$

As the twisted Kummer map is both Hecke and Galois equivariant we obtain

$$\text{Cor}_{H_{cp}/H_c}(\mathfrak{X}_{cp,s}) = U_p \cdot \mathfrak{X}_{c,s},$$

and passing to the limit proves the first claim of the proposition.

Fix a prime ℓ as in the second claim of the proposition. The map $z \mapsto \ell z$ induces an ℓ -isogeny $\mathbb{C}/\mathcal{O}_{cp^s} \rightarrow \mathbb{C}/\mathcal{O}_{c\ell p^s}$ of elliptic curves over \mathbb{C} , which determines an isogeny of elliptic curves with Φ_s level structure

$$f : h_{c,s} \rightarrow h_{c\ell,s}.$$

That is, f takes the extra Φ_s level structure on $E_{c,s}$ isomorphically to that on $E_{c\ell,s}$. As in the proof of Lemma 2.2.4 we may fix a subset $S \subset \text{Aut}(\mathbb{C}/H_{cp^s})$ of extensions of $\text{Gal}(H_{c\ell p^s}/H_{cp^s})$ in such a way that each $\sigma \in S$ acts trivially on μ_{p^∞} . As σ ranges over S the complex tori $E_{c\ell,s}^\sigma(\mathbb{C})$ are given by \mathbb{C}/\mathfrak{b} as \mathfrak{b} ranges over representatives of the kernel of $\text{Pic}(\mathcal{O}_{c\ell p^s}) \rightarrow \text{Pic}(\mathcal{O}_{cp^s})$. The $\ell + 1$ lattices \mathfrak{b} which arise in this way are not \mathbb{C}^\times -homothetic, and therefore the S -conjugates of $E_{c\ell,s}$ are pairwise nonisomorphic. As $\sigma \in S$ varies we obtain $\ell + 1$ distinct ℓ -isogenies $f^\sigma : h_{c,s} \rightarrow h_{c\ell,s}^\sigma$ of elliptic curves with Φ_s level structure, giving the equality of divisors

$$(13) \quad T_\ell \cdot h_{c,s} = \sum_{\sigma \in S} h_{c\ell,s}^\sigma.$$

From this we deduce

$$\begin{aligned}
 \sum_{\sigma \in S} y_{c\ell,s}^\sigma &= T_\ell \cdot y_{c,s} \\
 \implies \sum_{\sigma \in S} (y_{c\ell,s} \otimes \zeta_s)^\sigma &= T_\ell \cdot (y_{c,s} \otimes \zeta_s) \\
 \implies \text{Cor}_{H_{c\ell p^s}/H_{cp^s}}(y_{c\ell,s} \otimes \zeta_s) &= T_\ell \cdot (y_{c,s} \otimes \zeta_s) \\
 \implies \text{Cor}_{H_{c\ell p^s}/H_c}(y_{c\ell,s} \otimes \zeta_s) &= T_\ell \cdot (x_{c,s} \otimes \zeta_s) \\
 \implies \text{Cor}_{H_{c\ell}/H_c}(x_{c\ell,s}) &= T_\ell \cdot x_{c,s} \\
 \implies \text{Cor}_{H_{c\ell}/H_c}(\mathfrak{X}_{c\ell,s}) &= T_\ell \cdot (\mathfrak{X}_{c,s}).
 \end{aligned}$$

Passing to the limit in s proves the claim. \square

Proposition 2.3.2. *Suppose c is positive integer which is prime to N , and that $\ell \nmid cN$ is a prime which is inert in K . Fix a prime v of H_c above ℓ and let w be a place of $\overline{\mathbb{Q}}$ above v . If $\text{Fr}_v \in \text{Gal}(H_c/\mathbb{Q})$ is the arithmetic Frobenius of v then $\mathfrak{X}_{c\ell}$ and $\text{Fr}_v(\mathfrak{X}_c)$ have the same image in $H^1(H_{c\ell,w}, \mathbf{T}^\dagger)$.*

Proof. Fix $s > 0$ and recall $L_{c,s} = H_{cp^s}(\mu_{p^s})$. Set

$$\Phi_0 = (L_{c,s})_w \quad \Phi = (L_{cl,s})_w$$

so that Φ/Φ_0 is totally ramified of degree $\ell + 1$ and

$$\text{Gal}(\Phi/\Phi_0) \cong \text{Gal}(H_{clp^s}/H_{cp^s}).$$

As in the proof of Proposition 2.3.1, fix a set $S \subset \text{Aut}(\mathbb{C}/H_{cp^s})$ of representatives for $\text{Gal}(H_{clp^s}/H_{cp^s})$ in such a way that each $\sigma \in S$ acts trivially on μ_{p^∞} , so that the elements of S give a set of representatives for $\text{Gal}(\Phi/\Phi_0)$. Let W denote the integer ring of Φ , \mathbb{L} the residue field of Φ , and let \underline{X}_s be the canonical (smooth, proper) integral model of $X_{s/\Phi}$ over W . By the valuative criterion of properness any point $x \in X_s(\Phi)$ extends to a point denoted $\underline{x} \in \underline{X}_s(W)$.

Fix $\tau \in \text{Aut}(\mathbb{C}/H_c)$. The equality (13) gives

$$\left(\sum_{\sigma \in S} h_{cl,s}^\sigma \right)^\tau = T_\ell \cdot h_{c,s}^\tau$$

as divisors on $X_{s/L_{cl,s}}$. First replacing S by $\tau S \tau^{-1}$ and then changing base to $\text{Spec}(\Phi)$ gives the equality of divisors

$$\sum_{\sigma \in \text{Gal}(\Phi/\Phi_0)} (h_{cl,s}^\tau)^\sigma = T_\ell \cdot h_{c,s}^\tau$$

on $X_{s/\Phi}$. As Φ/Φ_0 is totally ramified this implies the equality of divisors in the special fiber $\underline{X}_{s/\mathbb{L}}$

$$(\ell + 1) \cdot \underline{h}_{cl,s/\mathbb{L}}^\tau = T_\ell \cdot \underline{h}_{c,s/\mathbb{L}}^\tau$$

where we abbreviate

$$\underline{h}_{c,s/\mathbb{L}}^\tau = \underline{h}_{c,s}^\tau \times_{\text{Spec}(W)} \text{Spec}(\mathbb{L})$$

and similarly with c replaced by cl . Using the Eichler-Shimura relation we deduce

$$(\ell + 1) \cdot \underline{h}_{cl,s/\mathbb{L}}^\tau = \text{Fr}_v(\underline{h}_{c,s/\mathbb{L}}^\tau) + \langle \ell \rangle \cdot \text{Fr}_v^{-1}(\underline{h}_{c,s/\mathbb{L}}^\tau).$$

The elliptic curve underlying $\underline{h}_{c,s}$ has supersingular reduction, and the action of Fr_v^2 on supersingular points in the special fiber is by $\langle \ell \rangle$ (see the proof of [14, Lemma 4.1.1]). Therefore

$$(\ell + 1) \cdot \underline{h}_{cl,s/\mathbb{L}}^\tau = (\ell + 1) \cdot \text{Fr}_v(\underline{h}_{c,s/\mathbb{L}}^\tau)$$

and so $\underline{h}_{cl,s}^\tau$ and $\text{Fr}_v(\underline{h}_{c,s}^\tau)$ have the same reduction to the special fiber. Let \underline{J}_s denote the Néron model of J_s over W and abbreviate

$$\underline{J}_s(\mathbb{L})^{\text{ord}} = e^{\text{ord}}(\underline{J}_s(\mathbb{L}) \otimes \mathcal{O}_F).$$

As the reduction map $J_s(\Phi) \rightarrow \underline{J}_s(\mathbb{L})$ is Hecke equivariant, we deduce from the discussion above that $y_{cl,s}^\tau$ and $\text{Fr}_v(y_{c,s}^\tau)$ have the same image under

$$J_s(L_{cl,s})^{\text{ord}} \rightarrow \underline{J}_s(\mathbb{L})^{\text{ord}}.$$

Letting τ vary over a set of representatives for $\text{Gal}(H_{clp^s}/H_{cl})$, which also gives representatives for $\text{Gal}(H_{cp^s}/H_c)$, the definition (7) shows that $x_{cl,s}$ and $\text{Fr}_v(x_{c,s})$ have the same image under

$$(14) \quad J_s(L_{cl,s})^{\text{ord}} \otimes \zeta_s \rightarrow \underline{J}_s(\mathbb{L})^{\text{ord}} \otimes \zeta_s.$$

Let \mathbb{F} denote the residue field of $H_{cl,w}$. The next claim is that the kernel of

$$(15) \quad H^0(H_{cl}, J_s(L_{c,s})^{\text{ord}} \otimes \zeta_s) \xrightarrow{\text{Kum}_s} H^1(H_{cl}, \mathbf{Ta}_p^{\text{ord}}(J_s) \otimes \zeta_s) \\ \xrightarrow{\text{loc}_w} H^1(H_{cl,w}, \mathbf{Ta}_p^{\text{ord}}(J_s) \otimes \zeta_s)$$

contains the kernel of the map

$$(16) \quad H^0(H_{cl}, J_s(L_{c,s})^{\text{ord}} \otimes \zeta_s) \rightarrow H^0(\mathbb{F}, J_s(\mathbb{L})^{\text{ord}} \otimes \zeta_s)$$

induced by the reduction map (14). Indeed, suppose $P \otimes \zeta_s$ is in the kernel of (16), and let Q_n and b_n be as in the definition of Kum_s , so that the image of $\text{Kum}_s(P \otimes \zeta_s)$ in $H^1(H_{cl}, J_s[p^n]^{\text{ord}} \otimes \zeta_s)$ is given by the cocycle

$$b_n(\sigma) = (\Theta^{-1}(\sigma)Q_n^\sigma - Q_n) \otimes \zeta_s.$$

Let $Q \mapsto \tilde{Q}$ denotes the reduction at w of points on $J_s(L)^{\text{ord}}$, where L is large enough that $Q_n \in J_s(L)^{\text{ord}}$, and extend this to $J_s(L)^{\text{ord}} \otimes \zeta_s$ by

$$\widetilde{Q \otimes \zeta_s} = \tilde{Q} \otimes \zeta_s.$$

By hypothesis $\tilde{P} = 0$, and so $p^n \tilde{Q}_n = 0$. Enlarging L if needed, we may find $R_n \in J_s(L)^{\text{ord}}$ such that

$$p^n R_n = 0 \quad \tilde{R}_n = \tilde{Q}_n.$$

Replacing Q_n by $Q_n - R_n$ we may therefore assume that $\tilde{Q}_n = 0$. This implies that for all σ in the decomposition group of w

$$\widetilde{b_n(\sigma)} = (\Theta^{-1}(\sigma)\tilde{Q}_n^\sigma - \tilde{Q}_n) \otimes \zeta_s = 0.$$

By the injectivity of the reduction map on torsion, we find that the restriction of b_n to the decomposition group of w is trivial. As this holds for all n ,

$$\text{loc}_w(\text{Kum}_s(P \otimes \zeta_s)) = 0.$$

We have now shown that $x_{cl,s}$ and $\text{Fr}_v(x_{c,s})$ have the same image under (14), hence also under (16), and hence also under the composition (15). Therefore

$$\text{loc}_w(\mathfrak{X}_{cl,s}) = \text{loc}_w(\text{Kum}_s(x_{cl,s})) = \text{loc}_w(\text{Kum}_s(\text{Fr}_v(x_{c,s}))) = \text{loc}_w(\text{Fr}_v(\mathfrak{X}_{c,s})).$$

The claim is now immediate from the construction of \mathfrak{X}_c from $\mathfrak{X}_{c,s}$. \square

Let W_N be the usual Atkin-Lehner automorphism of X_s , defined on elliptic curves with Φ_s level structure by

$$W_N \cdot (E, C, P) = (E/C, \ker(f^\vee), f(P))$$

where $f : E \rightarrow E/C$ is the quotient map and f^\vee is the dual isogeny. Note that $W_N^2 = \langle N \rangle$. The induced (Albanese) action on J_s commutes with the nebentype operators, the Hecke operators T_ℓ with $\ell \nmid Np$, and the operator U_p . In particular W_N commutes with the ordinary projector e^{ord} , and so there is an induced action (still denoted W_N) on \mathbf{Ta}^{ord} satisfying $W_N^2 = [N]$. Note that this action need not be $\mathfrak{h}^{\text{ord}}$ -linear, as W_N does not commute with the operators U_ℓ for $\ell \mid N$.

Lemma 2.3.3. *There is an R -linear automorphism W_N of \mathbf{T} making the diagram (of Λ -modules)*

$$\begin{array}{ccc} \mathbf{T}\mathbf{a}^{\text{ord}} & \xrightarrow{W_N} & \mathbf{T}\mathbf{a}^{\text{ord}} \\ \downarrow & & \downarrow \\ \mathbf{T} & \xrightarrow{W_N} & \mathbf{T} \end{array}$$

commute. Furthermore there is a choice of $w = \pm 1$ for which the action of W_N on \mathbf{T} is given by $W_N = w\Theta(-N)$.

Proof. Let \mathfrak{p} be an arithmetic prime of weight two and nontrivial wild character of conductor p^s . By [9, Theorem 3.1(i)] the Γ^{p^s} coinvariants of $\mathbf{T}\mathbf{a}^{\text{ord}}$ are precisely $\text{Ta}_p^{\text{ord}}(J_s)$, and so the natural map $\mathbf{T}\mathbf{a}^{\text{ord}} \rightarrow V_{\mathfrak{p}}$ factors as

$$\mathbf{T}\mathbf{a}^{\text{ord}} \rightarrow \text{Ta}_p(J_s) \otimes_{\mathfrak{h}^{\text{ord}}} F_{\mathfrak{p}} \rightarrow V_{\mathfrak{p}}.$$

The modular form $g_{\mathfrak{p}}$ is new of level Φ_s and so the Galois representation $V_{\mathfrak{p}}$ appears with multiplicity one as a summand of $\text{Ta}_p(J_s) \otimes_{\mathfrak{h}^{\text{ord}}} F_{\mathfrak{p}}$. As the automorphism W_N commutes with the Galois action it must preserve this summand. Furthermore, as $V_{\mathfrak{p}}$ is absolutely irreducible the action of W_N on this summand is through a scalar in $F_{\mathfrak{p}}$. We now have a commutative diagram

$$\begin{array}{ccc} \mathbf{T}\mathbf{a}^{\text{ord}} & \xrightarrow{W_N} & \mathbf{T}\mathbf{a}^{\text{ord}} \\ \downarrow & & \downarrow \\ V_{\mathfrak{p}} & \xrightarrow{W_N} & V_{\mathfrak{p}} \end{array}$$

of Λ -modules in which the bottom arrow is $\mathfrak{h}^{\text{ord}}$ -linear.

For any $h \in \mathfrak{h}^{\text{ord}}$ and $t \in \mathbf{T}\mathbf{a}^{\text{ord}}$ we have shown that the image of $W_N ht - hW_N t$ in $V_{\mathfrak{p}}$ is trivial. As this holds for all arithmetic primes of weight two and nontrivial wild character, Lemma 2.1.7 implies that $W_N ht - hW_N t$ has trivial image in \mathbf{T} . From this it follows that the automorphism W_N of $\mathbf{T}\mathbf{a}^{\text{ord}}$ factors through to an $\mathfrak{h}^{\text{ord}}$ -linear automorphism of \mathbf{T} . By [9, Theorem 2.1] $\mathbf{T} \otimes_R \mathcal{K}$ is an irreducible Galois representation, and by Proposition 2.1.2 complex conjugation acts on $\mathbf{T} \otimes_R \mathcal{K}$ with distinct eigenvalues ± 1 . Combining these, it follows that $\mathbf{T} \otimes_R \mathcal{K}$ is absolutely irreducible. Therefore W_N must act on \mathbf{T} through a scalar $\lambda \in R$ satisfying $\lambda^2 = [N]$. But $\Theta^2(-N) = [N]$ in R , and so for some choice of sign $w = \pm 1$ we have $W_N = w \cdot \Theta(-N)$ as operators on \mathbf{T} . \square

Remark 2.3.4. Note that as $W_N : \mathbf{T} \rightarrow \mathbf{T}$ does not depend on the choice of Θ made in Remark 2.1.4, neither does $w\Theta(-N)$. The two possible choices of Θ differ by $\omega^{\frac{p-1}{2}}$, and making a different choice multiplies w by $\omega^{\frac{p-1}{2}}(-N)$.

Proposition 2.3.5. *Suppose $\tau \in \text{Gal}(H_c/\mathbb{Q})$ acts nontrivially on K . There is a $\sigma \in \text{Gal}(H_c/K)$ such that*

$$\mathfrak{X}_c^\tau = w \cdot \mathfrak{X}_c^\sigma$$

where $w = \pm 1$ is defined by Lemma 2.3.3.

Proof. We may assume that τ is the restriction of the complex conjugation determined by the fixed embedding $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$. Set $\mathfrak{N}_{cp^s} = \mathfrak{N} \cap \mathcal{O}_{cp^s}$ so that the N -isogeny of complex tori $f : E_{c,s}(\mathbb{C}) \rightarrow (E_{c,s}/\mathfrak{n}_{c,s})(\mathbb{C})$ is identified with

$$\mathbb{C}/\mathcal{O}_{cp^s} \rightarrow \mathbb{C}/\mathfrak{N}_{cp^s}^{-1},$$

and the dual isogeny f^\vee is identified with

$$\mathbb{C}/\mathfrak{N}_{cp^s}^{-1} \rightarrow \mathbb{C}/N^{-1}\mathcal{O}_{cp^s}.$$

If we choose $x \in \widehat{K}^\times$ such that $x^{-1}\mathcal{O}_{cp^s} = \mathfrak{N}_{cp^s}$ and let $\sigma \in \text{Aut}(\mathbb{C}/K)$ be such that the restriction of σ to the maximal abelian extension of K agrees with the Artin symbol of x , then the main theorem of complex multiplication [33, Theorem 5.4] gives the left square of the commutative diagram

$$\begin{array}{ccccccc} (E_{c,s}^\sigma/\mathfrak{n}_{c,s}^\sigma)(\mathbb{C}) & \longrightarrow & \mathbb{C}/x^{-1}\mathfrak{N}_{cp^s}^{-1} & \xrightarrow{=} & \mathbb{C}/\tau(\mathcal{O}_{cp^s}) & \longrightarrow & E_{c,s}^\tau(\mathbb{C}) \\ (f^\vee)^\sigma \downarrow & & \downarrow & & \downarrow & & f^\tau \downarrow \\ E_{c,s}^\sigma(\mathbb{C}) & \longrightarrow & \mathbb{C}/x^{-1}N^{-1}\mathcal{O}_{cp^s} & \xrightarrow{=} & \mathbb{C}/\tau(\mathfrak{N}_{cp^s}^{-1}) & \longrightarrow & (E_{c,s}/\mathfrak{n}_{c,s})^\tau(\mathbb{C}) \end{array}$$

in which all horizontal arrows are isomorphisms (the square on the right arises from an elementary argument using the Weierstrass \wp -function). This implies that

$$(17) \quad W_N \cdot (E_{c,s}, \mathfrak{n}_{c,s})^\sigma \cong (E_{c,s}^\sigma/\mathfrak{n}_{c,s}^\sigma, \ker(f^\vee)^\sigma) \cong (E_{c,s}^\tau, \ker(f)^\tau) \cong (E_{c,s}, \mathfrak{n}_{c,s})^\tau$$

as elliptic curves with $\Gamma_0(N)$ level structure. The elliptic curves $E_{c,s}^\sigma/\mathfrak{n}_{c,s}^\sigma$ and $E_{c,s}^\tau$ inherit from $E_{c,s}$ $\Gamma_1(p^s)$ level structures $f(\pi_{c,s})^\sigma$ and $\pi_{c,s}^\tau$ defined as the images of $\pi_{c,s}$ under the maps

$$\ker(j_{c,s}) \xrightarrow{\sigma} E_{c,s}^\sigma \xrightarrow{f^\sigma} E_{c,s}^\sigma/\mathfrak{n}_{c,s}^\sigma \quad \ker(j_{c,s}) \xrightarrow{\tau} E_{c,s}^\tau.$$

Using the isomorphisms in the top row of the diagram above, these images correspond to the images of $c\varpi$ under

$$\mathcal{O}_c/\mathcal{O}_{cp^s} \xrightarrow{x^{-1}} K/\mathcal{O}_{cp^s} \quad \mathcal{O}_c/\mathcal{O}_{cp^s} \xrightarrow{\tau} K/\tau(\mathcal{O}_{cp^s}),$$

and if we demand that x has component $x_p = -1$ in $K \otimes \mathbb{Q}_p$ then both images are $-c\varpi$. Thus

$$(E_{c,s}/\mathfrak{n}_{c,s}, f(\pi_{c,s}))^\sigma \cong (E_{c,s}, \pi_{c,s})^\tau$$

as elliptic curves with $\Gamma_1(p^s)$ level structure. Combining this with (17) we find

$$W_N \cdot h_{c,s}^\sigma = h_{c,s}^\tau.$$

Using the fact that W_N commutes with e^{ord} and with e_{k+j-2} , it follows that $W_N \cdot y_{c,s}^\sigma = y_{c,s}^\tau$. Fix a set $S \subset \text{Gal}(L_{c,s}/H_c)$ of representatives for $\text{Gal}(H_{cp^s}/H_c)$. Let W_N act on $J_s(L_{c,s})^{\text{ord}} \otimes \zeta_s$ by $W_N(P \otimes \zeta_s) = (W_N P) \otimes \zeta_s$. We compute

$$\begin{aligned} x_{c,s}^\tau &= \sum_{\eta \in S} \Theta^{-1}(\eta)(y_{c,s}^\eta)^\tau \otimes \zeta_s^\tau \\ &= \sum_{\eta \in S} \Theta^{-1}(\eta)(y_{c,s}^\tau)^{\tau\eta\tau^{-1}} \otimes \zeta_s^\tau \\ &= W_N \sum_{\eta \in \tau S \tau^{-1}} \Theta^{-1}(\eta)(y_{c,s}^\sigma)^\eta \otimes \zeta_s^\tau \\ &= \Theta(\tau^{-1})W_N \sum_{\eta \in \tau S \tau^{-1}} \Theta^{-1}(\eta)(y_{c,s}^\eta)^\sigma \otimes \zeta_s \\ &= \Theta(\sigma\tau^{-1})W_N \left(\sum_{\eta \in \tau S \tau^{-1}} \Theta^{-1}(\eta)y_{c,s}^\eta \otimes \zeta_s \right)^\sigma \\ &= \Theta(\sigma\tau^{-1})W_N x_{c,s}^\sigma. \end{aligned}$$

As σ acts on μ_{p^∞} through the Artin symbol of $N_{K/\mathbb{Q}}(x)$, an idele of norm N^{-1} , we have $\epsilon_{\text{cyc}}(\sigma) = N^{-1}$. Identifying Θ with a character on \mathbb{Z}_p^\times by factoring through the cyclotomic character, this says $\Theta(\sigma) = \Theta(N)^{-1}$, and similarly $\Theta(\tau) = \Theta(-1)$. Therefore

$$x_{c,s}^\tau = \Theta^{-1}(-N)W_N x_{c,s}^\sigma.$$

By the $G_{\mathbb{Q}}$ and $\text{Aut}(J_s)$ equivariance of the twisted Kummer map this equality holds with $x_{c,s}$ replaced by $\mathfrak{X}_{c,s}$. Passing to the limit in s and using Lemma 2.3.3 (and viewing W_N as an operator on \mathbf{T}^\dagger using the identification $\mathbf{T}^\dagger \cong \mathbf{T}$ of underlying R -modules) it follows that

$$\mathfrak{X}_c^\tau = \Theta^{-1}(-N)W_N \cdot \mathfrak{X}_c^\sigma.$$

As W_N acts as $w\Theta(-N)$ on \mathbf{T}^\dagger by Lemma 2.3.3, we are done. \square

Proposition 2.3.6. *Let \mathfrak{p} be an arithmetic prime of R and let $\mathcal{O}_{\mathfrak{p}}$ denote the ring of integers of $F_{\mathfrak{p}}$. The Mazur-Tate-Teitelbaum [18] p -adic L -function*

$$L_p(g_{\mathfrak{p}}, \cdot) \in \mathcal{O}_{\mathfrak{p}}[[\mathbb{Z}_p^\times]],$$

viewed as a function on characters $\mathbb{Z}_p^\times \rightarrow \overline{\mathbb{Q}_p}^\times$, satisfies the functional equation

$$(18) \quad L_p(g_{\mathfrak{p}}, \chi) = -w\chi^{-1}(-N)\Theta_{\mathfrak{p}}(-N) \cdot L_p(g_{\mathfrak{p}}, \chi^{-1}[\cdot]_{\mathfrak{p}})$$

where $w = \pm 1$ is defined by Lemma 2.3.3. In particular, taking $\chi = \Theta_{\mathfrak{p}}$ and using $\Theta_{\mathfrak{p}}^2 = [\cdot]_{\mathfrak{p}}$ gives

$$L_p(g_{\mathfrak{p}}, \Theta_{\mathfrak{p}}) = -w \cdot L_p(g_{\mathfrak{p}}, \Theta_{\mathfrak{p}}).$$

Proof. According to [5, §3.4] there is a two-variable p -adic L -function $L_p \in R[[\mathbb{Z}_p^\times]]$ whose image under

$$R[[\mathbb{Z}_p^\times]] \rightarrow \mathcal{O}_{\mathfrak{p}}[[\mathbb{Z}_p^\times]]$$

for any arithmetic prime $\mathfrak{p} \subset R$ agrees (up to a nonzero p -adic period) with the one variable p -adic L -function $L_p(g_{\mathfrak{p}}, \cdot)$ of [18]. Such a two variable p -adic L -function also appears in the work of Greenberg-Stevens [8]. If we take \mathfrak{p} to be an arithmetic prime of weight 2 (so that $g_{\mathfrak{p}}$ has character $[\cdot]_{\mathfrak{p}}$) then [18, §I.17, Corollary 2] gives

$$(19) \quad L_p(g_{\mathfrak{p}}, \chi) = -\chi^{-1}(-N)[N]_{\mathfrak{p}} \cdot L_p(g_{\mathfrak{p}}^*, \chi^{-1}[\cdot]_{\mathfrak{p}})$$

where $g_{\mathfrak{p}}^* = \langle N \rangle^{-1}W_N \cdot g_{\mathfrak{p}}$. Here W_N acts on modular forms by the contravariant action on

$$S_2(\Phi_s, F_{\mathfrak{p}}) \cong H^0(X_{s/F_{\mathfrak{p}}}, \Omega_{X_{s/F_{\mathfrak{p}}}^1})$$

(our $\langle N \rangle^{-1}W_N$ is the w_Q of [loc. cit.]). But then

$$g_{\mathfrak{p}}^* = [N]_{\mathfrak{p}}^{-1} \cdot w\Theta_{\mathfrak{p}}(-N) \cdot g_{\mathfrak{p}}$$

as the eigenvalue of W_N acting on $g_{\mathfrak{p}}$ agrees with the eigenvalue $w\Theta_{\mathfrak{p}}(-N)$ of W_N acting on the corresponding factor $V_{\mathfrak{p}}$ of the p -adic Tate module of J_s . Combining this with (19) we find that there are infinitely many arithmetic primes $\mathfrak{p} \subset R$ such that (18) holds for every character χ .

Now fix a character $\chi : \mathbb{Z}_p^\times \rightarrow \mathcal{O}_F^\times$, possibly of infinite order, and define R -module maps

$$\begin{aligned} \pi_\chi : R[[\mathbb{Z}_p^\times]] &\rightarrow R & z &\mapsto \chi(z) \\ \pi_\chi^* : R[[\mathbb{Z}_p^\times]] &\rightarrow R & z &\mapsto \chi^{-1}(z) \cdot [z] \end{aligned}$$

for $z \in \mathbb{Z}_p^\times$. Composing these with $R \rightarrow \mathcal{O}_{\mathfrak{p}}$ for any arithmetic prime \mathfrak{p} gives two more maps

$$\pi_{\chi, \mathfrak{p}}, \pi_{\chi, \mathfrak{p}}^* : R[[\mathbb{Z}_p^\times]] \rightarrow \mathcal{O}_{\mathfrak{p}},$$

and by what we have proved the equality

$$\pi_{\chi, \mathfrak{p}}(L_{\mathfrak{p}}) = -w\chi^{-1}(-N)\Theta_{\mathfrak{p}}(-N)\pi_{\chi, \mathfrak{p}}^*(L_{\mathfrak{p}})$$

holds for all arithmetic primes of weight two. By Lemma 2.1.7 we must have

$$\pi_{\chi}(L_p) = -w\chi^{-1}(-N)\Theta(-N)\pi_{\chi}^*(L_p).$$

This means that for *every* arithmetic prime \mathfrak{p} the equality (18) holds for all characters $\chi : \mathbb{Z}_p^\times \rightarrow \mathcal{O}_{\mathfrak{p}}^\times$, and as $L_p(g_{\mathfrak{p}}, \cdot)$ is determined by its values on such characters we conclude that (18) holds for all arithmetic primes and all characters. \square

2.4. Selmer groups.

Proposition 2.4.1. *Let v be a place of $\overline{\mathbb{Q}}$ above p and let $I_v \subset D_v \subset G_{\mathbb{Q}}$ be the inertia and decomposition groups of v . Let $\eta_v : D_v/I_v \rightarrow R^\times$ be the character taking the arithmetic Frobenius to U_p . There is a short exact sequence of $R[D_v]$ -modules*

$$(20) \quad 0 \rightarrow F_v^+(\mathbf{T}) \rightarrow \mathbf{T} \rightarrow F_v^-(\mathbf{T}) \rightarrow 0$$

such that $F_v^+(\mathbf{T})$ and $F_v^-(\mathbf{T})$ are free of rank one over R , D_v acts on $F_v^-(\mathbf{T})$ through η_v , and D_v acts on $F_v^+(\mathbf{T})$ through $\eta_v^{-1}\epsilon_{\text{cyc}}[\epsilon_{\text{cyc}}]$.

Proof. When $k + j \not\equiv 2 \pmod{p-1}$ the short exact sequence is that of [26, Proposition 1.5.2(iii)] together with the final statement of Proposition 2.1.2 for the isomorphism $R \cong F_v^-(\mathbf{T})$. When $k + j - 2 \equiv 0 \pmod{p-1}$ the short exact sequence is that of [26, Proposition 1.5.4]. In either case the description of the action of D_v follows from [8, Theorem 2.6(d)]. \square

Twisting by Θ^{-1} and tensoring the exact sequence (20) with $R_{\mathfrak{p}}$ or $F_{\mathfrak{p}}$ (for any arithmetic prime $\mathfrak{p} \subset R$), yields an exact sequence of D_v -modules

$$0 \rightarrow F_v^+(M) \rightarrow M \rightarrow F_v^-(M) \rightarrow 0$$

for M any one of $\mathbf{T}_{\mathfrak{p}}$, $V_{\mathfrak{p}}$, $\mathbf{T}_{\mathfrak{p}}^\dagger$, or $V_{\mathfrak{p}}^\dagger$.

Definition 2.4.2. Let L be a finite extension of \mathbb{Q} . For each prime v of L let L_v^{unr} be the maximal unramified extension of L_v . Let M be any $G_{\mathbb{Q}}$ -module for which we have defined $F_v^-(M)$. For any place v of L define the *strict Greenberg local condition* (compare with [6, §2] or [25, §9.6.1])

$$H_{\text{Gr}}^1(L_v, M) = \begin{cases} \ker(H^1(L_v, M) \rightarrow H^1(L_v^{\text{unr}}, M)) & \text{if } v \nmid p \\ \ker(H^1(L_v, M) \rightarrow H^1(L_v, F_v^-(M))) & \text{if } v \mid p \end{cases}$$

and the *strict Greenberg Selmer group*

$$\text{Sel}_{\text{Gr}}(L, M) = \ker(H^1(L, M) \rightarrow \prod_v H^1(L_v, M) / H_{\text{Gr}}^1(L_v, M))$$

where the product is over all finite places of L .

Definition 2.4.3. Suppose $\mathfrak{p} \subset R$ is an arithmetic prime of weight r and let $\alpha_{\mathfrak{p}}$ be the image of U_p under $R \rightarrow F_{\mathfrak{p}}$. We will say that \mathfrak{p} is *exceptional* if $r = 2$, $\psi_{\mathfrak{p}}$ is the trivial character, and $\alpha_{\mathfrak{p}} = \pm 1$.

Lemma 2.4.4. *Let L/\mathbb{Q} be a finite extension and fix a place v of $\overline{\mathbb{Q}}$ above p . If \mathfrak{p} is an arithmetic prime of R which is not exceptional then*

$$H^0(L_v, F_v^-(V_{\mathfrak{p}}^\dagger)) = 0.$$

Furthermore, if \tilde{L}_v is any finite extension of a ramified \mathbb{Z}_p -extension of L_v then

$$H^0(\tilde{L}_v, F_v^-(\mathbf{T}^\dagger)) = 0.$$

Proof. Fix an arithmetic prime \mathfrak{p} of R of weight r . Proposition 2.4.1 implies that the action of $\text{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ on $F_p^-(V_{\mathfrak{p}}^\dagger)$ is through the $F_{\mathfrak{p}}^\times$ valued character $\eta_{v,\mathfrak{p}}\Theta_{\mathfrak{p}}^{-1}$ where $\eta_{v,\mathfrak{p}}$ takes the arithmetic Frobenius to $\alpha_{\mathfrak{p}}$. The claim is that

$$\eta_{v,\mathfrak{p}}\Theta_{\mathfrak{p}}^{-1} \text{ of finite order} \implies \mathfrak{p} \text{ exceptional.}$$

Indeed, if $\eta_{v,\mathfrak{p}}\Theta_{\mathfrak{p}}^{-1}$ is of finite order then $\eta_{v,\mathfrak{p}}$ becomes trivial when restricted to the Galois group of a finite extension of $L_v(\mu_{p^\infty})$. As $\eta_{v,\mathfrak{p}}$ is unramified, it follows that $\eta_{v,\mathfrak{p}}$ is of finite order and so $\alpha_{\mathfrak{p}}$ is a root of unity. But then also $\Theta_{\mathfrak{p}}$ is of finite order, and as

$$\Theta_{\mathfrak{p}}(\sigma) = \epsilon_{\text{tame}}^{\frac{k+j}{2}-1}(\sigma) \cdot \epsilon_{\text{wild}}^{\frac{r}{2}-1}(\sigma) \cdot \psi_{\mathfrak{p}}(\epsilon_{\text{wild}}^{1/2}(\sigma))$$

we must have $r = 2$. By [18, §I.12 Case II] the eigenform $g_{\mathfrak{p}}$ of weight 2 attached to \mathfrak{p} is a newform of level Np and trivial character with $\alpha_{\mathfrak{p}} = \pm 1$. Thus \mathfrak{p} is exceptional.

The first claim of the lemma is now immediate, as $H^0(L_v, F_v^-(V_{\mathfrak{p}}^\dagger)) \neq 0$ implies that $\eta_{v,\mathfrak{p}}\Theta_{\mathfrak{p}}^{-1}$ is of finite order. For the second claim, fix a weight 2 arithmetic prime \mathfrak{p} which is not exceptional, so that $\eta_{v,\mathfrak{p}}\Theta_{\mathfrak{p}}^{-1}$ has infinite order. As $\Theta_{\mathfrak{p}}$ is of finite order, $\eta_{v,\mathfrak{p}}$ is unramified and of infinite order and so cannot become trivial over any extension of L_v whose maximal unramified subfield is finite over \mathbb{Q}_p . In particular $\eta_{v,\mathfrak{p}}$ has nontrivial restriction to any finite extension of \tilde{L}_v , and so $\eta_{v,\mathfrak{p}}\Theta_{\mathfrak{p}}^{-1}$ has nontrivial restriction to \tilde{L}_v . Therefore $\eta_{v,\mathfrak{p}}\Theta_{\mathfrak{p}}^{-1}$ has nontrivial restriction to \tilde{L}_v , and so $H^0(\tilde{L}_v, F_v^-(\mathbf{T}^\dagger)) = 0$. \square

If M is either \mathbf{T}^\dagger or $V_{\mathfrak{p}}^\dagger$ and L/\mathbb{Q} is a finite extension, one also has a family of *extended Selmer groups* $\tilde{H}_f^i(L, M)$ defined by Nekovář [25] using similar local conditions to those defining Sel_{Gr} , but with the local conditions imposed on the level of cochain complexes rather than on cohomology. For $i = 1$ Nekovář's extended Selmer group sits in an exact sequence [25, Lemma 9.6.3]

$$0 \rightarrow \bigoplus_{v|p} H^0(L_v, F_v^-(M)) \rightarrow \tilde{H}_f^1(L, M) \rightarrow \text{Sel}_{\text{Gr}}(L, M) \rightarrow 0.$$

In particular Lemma 2.4.4 implies

$$(21) \quad \tilde{H}_f^1(L, \mathbf{T}^\dagger) \cong \text{Sel}_{\text{Gr}}(L, \mathbf{T}^\dagger)$$

and, if \mathfrak{p} is an arithmetic prime of R which is not exceptional,

$$(22) \quad \tilde{H}_f^1(L, V_{\mathfrak{p}}^\dagger) \cong \text{Sel}_{\text{Gr}}(L, V_{\mathfrak{p}}^\dagger).$$

If \mathfrak{p} has even weight then according to [25, Proposition 12.5.9.2] one also has an exact sequence

$$0 \rightarrow \bigoplus_{v|p} H^0(L_v, F_v^-(V_{\mathfrak{p}}^\dagger)) \rightarrow \tilde{H}_f^1(L, V_{\mathfrak{p}}^\dagger) \rightarrow H_f^1(L, V_{\mathfrak{p}}^\dagger) \rightarrow 0$$

in which $H_f^1(L, V_{\mathfrak{p}}^\dagger)$ is the Bloch-Kato Selmer group. In particular

$$(23) \quad \text{Sel}_{\text{Gr}}(L, V_{\mathfrak{p}}^\dagger) = H_f^1(L, V_{\mathfrak{p}}^\dagger)$$

as both are equal to the image of $\tilde{H}_f^1(L, V_{\mathfrak{p}}^\dagger) \rightarrow H^1(L, V_{\mathfrak{p}}^\dagger)$.

Proposition 2.4.5. *For any positive integer c prime to N there is a nonzero $\lambda \in R$ (which may depend on c) such that*

$$\lambda \cdot \mathfrak{X}_c \in \text{Sel}_{\text{Gr}}(H_c, \mathbf{T}^\dagger).$$

If N is prime to $\text{disc}(K)$ then we may take $\lambda = 1$.

Proof. For any place v of H_c and any $G_{\mathbb{Q}}$ -module M denote by

$$\text{loc}_v : H^1(H_c, M) \rightarrow H^1(H_{c,v}, M)$$

the localization map. If v is a finite prime of H_c not dividing Np , then the unramifiedness of \mathfrak{X}_c at v is part of Definition 2.2.3.

Now suppose $v \mid Np$ and choose a place w of $\overline{\mathbb{Q}}$ above v . Let \mathfrak{p} be an arithmetic prime of weight 2, and let $s = \max\{1, \text{ord}_p(\text{cond}(\psi_{\mathfrak{p}}))\}$ so that the natural map $\mathbf{Ta}^{\text{ord}} \rightarrow V_{\mathfrak{p}}$ factors through $\text{Ta}_p^{\text{ord}}(J_s)$. Let $\mathfrak{X}_{c,\mathfrak{p}}$ denote the image of \mathfrak{X}_c in $H^1(H_c, V_{\mathfrak{p}}^\dagger)$. If we set $L_{c,s} = H_{c p^s}(\mu_{p^s})$ then $V_{\mathfrak{p}}^\dagger \cong V_{\mathfrak{p}}$ after restriction to $L_{c,s}$, and directly from the construction we see that the restriction of $\mathfrak{X}_{c,\mathfrak{p}}$ to $H^1(L_{c,s}, V_{\mathfrak{p}}^\dagger)$ lies in the image of the composition

$$J_s(L_{c,s})^{\text{ord}} \rightarrow H^1(L_{c,s}, \text{Ta}_p^{\text{ord}}(J_s)) \rightarrow H^1(L_{c,s}, V_{\mathfrak{p}}) \cong H^1(L_{c,s}, V_{\mathfrak{p}}^\dagger)$$

where the first arrow is the usual (untwisted) Kummer map, and is therefore contained in the Bloch-Kato Selmer group by [2, Example 3.11] (see also [32, Proposition 1.6.8]). By (23) the restriction of $\mathfrak{X}_{c,\mathfrak{p}}$ to $L_{c,s}$ lies in $\text{Sel}_{\text{Gr}}(L_{c,s}, V_{\mathfrak{p}}^\dagger)$. If $v \mid N$ then the fact that $L_{c,s,w}/H_{c,v}$ is unramified implies that

$$(24) \quad \text{loc}_v(\mathfrak{X}_{c,\mathfrak{p}}) \in H_{\text{Gr}}^1(H_{c,v}, V_{\mathfrak{p}}^\dagger).$$

If $v \mid p$ then the restriction map

$$H^1(H_{c,v}, F_v^-(V_{\mathfrak{p}}^\dagger)) \rightarrow H^1(L_{c,s,w}, F_v^-(V_{\mathfrak{p}}^\dagger))$$

is injective, as the kernel

$$H^1(L_{c,s,w}/H_{c,v}, H^0(L_{c,s,w}, V_{\mathfrak{p}}^\dagger))$$

is both an $F_{\mathfrak{p}}$ -vector space and is annihilated by $[L_{c,s,w} : H_{c,v}]$. Therefore (24) holds in this case as well. We have now shown that

$$(25) \quad \mathfrak{X}_{c,\mathfrak{p}} \in \text{Sel}_{\text{Gr}}(H_{c,v}, V_{\mathfrak{p}}^\dagger)$$

for all arithmetic primes of weight 2.

Suppose $v \mid p$. For any arithmetic prime \mathfrak{p} we may, by Lemma 2.1.6, fix a generator π of the maximal ideal of $R_{\mathfrak{p}}$. The exactness of

$$0 \rightarrow F_v^-(\mathbf{T}_{\mathfrak{p}}^\dagger) \xrightarrow{\pi} F_v^-(\mathbf{T}_{\mathfrak{p}}^\dagger) \rightarrow F_v^-(V_{\mathfrak{p}}^\dagger) \rightarrow 0$$

shows that the natural map

$$(26) \quad \frac{H^1(H_{c,v}, F_v^-(\mathbf{T}_{\mathfrak{p}}^\dagger))_{\mathfrak{p}}}{\mathfrak{p} \cdot H^1(H_{c,v}, F_v^-(\mathbf{T}_{\mathfrak{p}}^\dagger))_{\mathfrak{p}}} \rightarrow H^1(H_{c,v}, F_v^-(V_{\mathfrak{p}}^\dagger))$$

is injective. By (25) the image of \mathfrak{X}_c in the right hand side of (26) is trivial for infinitely many \mathfrak{p} . Combining [25, Proposition 4.2.3] and [27, Theorem 7.1.8(iii)] the

R -module $H^1(H_{c,v}, F_v^-(\mathbf{T}^\dagger))$ is finitely generated. Therefore Lemma 2.1.7 applies and the image of \mathfrak{X}_c under

$$(27) \quad H^1(H_c, \mathbf{T}^\dagger) \rightarrow H^1(H_{c,v}, F_v^-(\mathbf{T}^\dagger))$$

is a torsion element. Let $S_n \subset H^1(H_{cp^n, w}, F_v^-(\mathbf{T}^\dagger))$ be the R -torsion submodule. By the Euler system relations of Proposition 2.3.1 and the discussion above (which holds equally well with c replaced by cp^n), the image of \mathfrak{X}_c under (27) lies in the image of $\varprojlim S_n \rightarrow S_0$, where the inverse limit is with respect to corestriction. Set

$$\mathbf{V} = F_v^-(\mathbf{T}^\dagger) \otimes_R \mathcal{K}$$

(recall that \mathcal{K} is the fraction field of R) and define \mathbf{A} by the exactness of

$$0 \rightarrow F_v^-(\mathbf{T}^\dagger) \rightarrow \mathbf{V} \rightarrow \mathbf{A} \rightarrow 0.$$

The restriction of $\eta_v \Theta^{-1}$, the character giving the Galois action on \mathbf{V} , to $H_{cp^\infty, w}$ is nontrivial by Lemma 2.4.4, and it follows that

$$S_n \cong H^0(H_{cp^n, w}, \mathbf{A}).$$

If we pick a $\sigma \in \text{Gal}(\overline{\mathbb{Q}}_p/H_{cp^\infty, w})$ such that $(\eta_v \Theta^{-1})(\sigma) \neq 1$ then, as $\mathbf{A} \cong \mathcal{K}/R$ as R -modules,

$$H^0(H_{cp^\infty, w}, \mathbf{A}) \subset \mathbf{A}[\sigma - 1] \cong R/((\eta_v \Theta^{-1})(\sigma) - 1).$$

In particular $H^0(H_{cp^\infty, w}, \mathbf{A})$ is finitely generated as an R -module, and so for a sufficiently large m the restriction map $S_m \rightarrow S_n$ is an isomorphism for all $n \geq m$. This implies that the image of corestriction $S_n \rightarrow S_m$ is divisible by p^{n-m} . As S_m , being finitely generated over R , has no nontrivial p -divisible submodules,

$$\varprojlim S_n = 0.$$

This proves that the image of \mathfrak{X}_c under (27) is trivial, and so

$$\text{loc}_v(\mathfrak{X}_c) \in H_{\text{Gr}}^1(H_{c,v}, \mathbf{T}^\dagger).$$

Now suppose $v \mid N$. We know from above that the image \mathfrak{X}_c under

$$\frac{H^1(H_{c,v}^{\text{unr}}, \mathbf{T}^\dagger)_{\mathfrak{p}}}{\mathfrak{p}H^1(H_{c,v}^{\text{unr}}, \mathbf{T}^\dagger)_{\mathfrak{p}}} \rightarrow H^1(H_{c,v}^{\text{unr}}, V_{\mathfrak{p}}^\dagger)$$

is trivial for infinitely many arithmetic primes \mathfrak{p} . The finite generation of the R -module $H^1(H_{c,v}^{\text{unr}}, \mathbf{T}^\dagger)$ is a consequence of [25, Proposition 4.2.3] as above, provided one knows that $H^1(H_{c,v}^{\text{unr}}, M)$ is finite for every finite Galois module M of p -power order. This follows from the proof of [27, Theorem 7.1.8(iii)], the essential point being that one knows the finiteness of $H^i(B, \mu_{p^n})$ for every finite extension $B/H_{c,v}^{\text{unr}}$ by passing to the limit over finite subfields in [27, Theorem 7.1.8(ii)]. As in the case $v \mid p$, this implies that the restriction of \mathfrak{X}_c to $H^1(H_{c,v}^{\text{unr}}, \mathbf{T}^\dagger)$ is R -torsion. Thus there is a nonzero $\lambda_v \in R$ such that

$$\text{loc}_v(\lambda_v \mathfrak{X}_c) \in H_{\text{Gr}}^1(H_{c,v}, \mathbf{T}^\dagger).$$

Taking $\lambda = \prod_{v \mid N} \lambda_v$ we then have $\lambda \mathfrak{X}_c \in \text{Sel}_{\text{Gr}}(H_c, \mathbf{T}^\dagger)$. If we assume that N is prime to $\text{disc}(K)$ then v splits in K and it follows that v is finitely decomposed in H_{cp^∞} . By the Euler system relations (Proposition 2.3.1) \mathfrak{X}_c is a universal norm from the \mathbb{Z}_p -extension H_{cp^∞}/H_c , hence the image of \mathfrak{X}_c in $H^1(H_c, \mathbf{T}^\dagger/\mathfrak{m}^k \mathbf{T}^\dagger)$ for

every $k \geq 0$ (\mathfrak{m} is the maximal ideal of R) is unramified at v by [32, Corollary B.3.5]. It follows that \mathfrak{X}_c has trivial image in

$$H^1(H_{c,v}^{\text{unr}}, \mathbf{T}^\dagger) = \varprojlim_k H^1(H_{c,v}^{\text{unr}}, \mathbf{T}^\dagger/\mathfrak{m}^k \mathbf{T}^\dagger),$$

using [25, Lemma 4.2.2] to justify passing to the limit, and so

$$\text{loc}_v(\mathfrak{X}_c) \in H_{\text{Gr}}^1(H_{c,v}, \mathbf{T}^\dagger).$$

□

Remark 2.4.6. The proof of Proposition 2.4.5 shows that \mathfrak{X}_c satisfies the correct local conditions to lie in $\text{Sel}_{\text{Gr}}(H_c, \mathbf{T}^\dagger)$, except possibly at places dividing both N and $\text{disc}(K)$.

3. IWASAWA THEORY

Throughout all of §3 we assume that N and $\text{disc}(K)$ are relatively prime and that $p \nmid \phi(N)$, where ϕ is Euler's function. In particular for every positive integer c prime to N the big Heegner point \mathfrak{X}_c of Definition 2.2.3 lies in $\text{Sel}_{\text{Gr}}(H_c, \mathbf{T}^\dagger)$ by Proposition 2.4.5

3.1. The vertical nonvanishing theorem. Let D_∞ be the anticyclotomic \mathbb{Z}_p -extension of K . Define $\mathcal{G} = \text{Gal}(H_{p^\infty}/K)$ and let

$$\mathcal{G}_{\text{tors}} = \text{Gal}(H_{p^\infty}/D_\infty)$$

be the torsion subgroup of \mathcal{G} . Keep R , \mathbf{T} , and \mathbf{T}^\dagger as in §2.2. Let \mathfrak{m} be the maximal ideal of R . The modular form g of the introduction furnishes us with a surjection $R \rightarrow \mathcal{O}_F$ as in §2.1 inducing an isomorphism of residue fields $R/\mathfrak{m} \cong \mathcal{O}_F/\mathfrak{m}\mathcal{O}_F$. Fix a character $\chi : \mathcal{G}_{\text{tors}} \rightarrow \mathcal{O}_F^\times$ and set

$$e_\chi = \sum_{g \in \mathcal{G}_{\text{tors}}} \chi(g) \cdot g \in \mathcal{O}_F[\mathcal{G}_{\text{tors}}].$$

The proof of the following theorem, which follows closely the methods of Cornut and Vatsal [3, 4, 34], will be given in §3.2.

Theorem 3.1.1. *Let*

$$\text{Heeg}_s \subset H^1(H_{p^s}, \mathbf{T}^\dagger/\mathfrak{m}\mathbf{T}^\dagger)$$

be the $R[\text{Gal}(H_{p^s}/K)]$ -submodule generated by the image of \mathfrak{X}_{p^s} . As $s \rightarrow \infty$ the R/\mathfrak{m} dimension of $e_\chi \text{Heeg}_s$ grows without bound.

Corollary 3.1.2. *Let $\mathfrak{p} \subset R$ be any arithmetic prime. For all $s \gg 0$, the image of $e_\chi \mathfrak{X}_{p^s}$ in $\text{Sel}_{\text{Gr}}(H_{p^s}, V_{\mathfrak{p}}^\dagger)$ is nontrivial.*

Proof of Corollary 3.1.2. Let $T_{\mathfrak{p}}^\dagger$ denote the image of $\mathbf{T}^\dagger \rightarrow V_{\mathfrak{p}}^\dagger$. As in [14, Lemma 5.1.5] the torsion submodule of $H^1(H_{p^s}, T_{\mathfrak{p}}^\dagger)$ has bounded order as $s \rightarrow \infty$. Thus if $e_\chi \mathfrak{X}_{p^s}$ had torsion image in $H^1(H_{p^s}, T_{\mathfrak{p}}^\dagger)$ for all s then $e_\chi \text{Heeg}_s$ would have bounded dimension as $s \rightarrow \infty$ contradicting Theorem 3.1.1. Thus $e_\chi \mathfrak{X}_{p^s}$ is nontrivial in $H^1(H_{p^s}, V_{\mathfrak{p}}^\dagger)$ for some s , and then by the Euler system relations of Proposition 2.3.1 it must be nontrivial for all $s \gg 0$. □

3.2. **Proof of Theorem 3.1.1.** For all $s > 0$ define

$$L_s^* = H_{p^{s+1}}(\mu_p) = L_{p^s,1}.$$

Set $L_\infty^* = \cup L_s^*$ and $\mathcal{G}^* = \text{Gal}(L_\infty^*/K)$. Let

$$\mathcal{G}_{\text{ram}} = \langle \text{Fr}_{Q_1}, \dots, \text{Fr}_{Q_t} \rangle \subset \mathcal{G}_{\text{tors}}$$

be the subgroup generated by the Frobenius automorphisms of all ramified primes Q_1, \dots, Q_t of K which are prime to p (all of which have order two and are linearly independent over $\mathbb{Z}/2\mathbb{Z}$). Let $\mathfrak{D} = Q_1 \cdots Q_t$ and $D = \text{Norm}(\mathfrak{D})$, and define

$$\mathcal{R}_{\text{ram}} = \{ \text{Fr}_I \mid \mathfrak{D} \subset I \subset \mathcal{O} \} \subset \mathcal{G}^*$$

where $\text{Fr}_I \in \mathcal{G}^*$ is the Frobenius of I . The quotient map $\mathcal{G}^* \rightarrow \mathcal{G}$ takes \mathcal{R}_{ram} bijectively to \mathcal{G}_{ram} . Fix a subset $\mathcal{R} \subset \mathcal{G}^*$ whose elements represent the distinct cosets $\mathcal{G}_{\text{tors}}/\mathcal{G}_{\text{ram}}$, so that $\mathcal{G}^* \rightarrow \mathcal{G}$ takes the set

$$\mathcal{R}_{\text{tors}} \stackrel{\text{def}}{=} \{ \sigma\tau \mid \sigma \in \mathcal{R}, \tau \in \mathcal{R}_{\text{ram}} \} \subset \mathcal{G}^*$$

bijectionally to $\mathcal{G}_{\text{tors}}$. Abbreviate

$$\Phi = \Phi_1 = \Gamma_0(N) \cap \Gamma_1(p)$$

and write $X(\Phi)$ instead of X_1 . Set

$$h_s^* = h_{p^s,1} \in X(\Phi)(L_s^*).$$

and define

$$\tilde{h}_s^* = (E_{p^s,1}, \tilde{\mathfrak{n}}_{p^s,1}, \pi_{p^s,1}) \in X(\tilde{\Phi})(L_s^*),$$

where

$$\tilde{\mathfrak{n}}_{p^s,1} = E_{p^s,1}[\mathfrak{D}\mathfrak{N} \cap \mathcal{O}_{p^{s+1}}] \quad \tilde{\Phi} = \Gamma_0(DN) \cap \Gamma_1(p),$$

so that under the forgetful degeneracy map $X(\tilde{\Phi}) \rightarrow X(\Phi)$ we have $\tilde{h}_s^* \mapsto h_s^*$.

Fix a finite set \mathcal{S} of degree two primes of K and assume that for every $v \in \mathcal{S}$, $\text{Norm}(v) \equiv 1 \pmod{Np}$. Note that no $v \in \mathcal{S}$ divides D , and all $v \in \mathcal{S}$ are split completely in L_∞^* . For each $v \in \mathcal{S}$ fix a place \bar{v} of $\overline{\mathbb{Q}}$ above v , let \mathbb{F}_v be the residue field of v , and let $X_v^{\text{ss}}(\tilde{\Phi})$ denote the set of supersingular points on the reduction of $X(\tilde{\Phi})$ at v . Our assumption that $\text{Norm}(v) \equiv 1 \pmod{p}$ implies that all supersingular points have residue field \mathbb{F}_v (if ℓ is the prime below v then the square of the absolute Frobenius acts as $\langle \ell \rangle = \langle \pm 1 \rangle$ on the supersingular locus, as in the proof of Proposition 2.3.2). The set $X_v^{\text{ss}}(\Phi)$ is defined similarly. Given $v \in \mathcal{S}$ and any \mathcal{G}^* -conjugate h of \tilde{h}_s^* , we may define the v -reduction of h

$$(28) \quad \text{red}_v(h) \in X_v^{\text{ss}}(\tilde{\Phi}),$$

to be the reduction at \bar{v} of h . Define

$$\text{Red}_v(h) \in X_v^{\text{ss}}(\tilde{\Phi})^{\mathcal{R}}$$

to be the $|\mathcal{R}|$ -tuple with $\text{red}_v(h^\sigma)$ in the σ component for each $\sigma \in \mathcal{R}$.

Theorem 3.2.1 (Cornut-Vatsal). *Let $G \subset \mathcal{G}^*$ be a compact open subgroup and let $G\tilde{h}_s^*$ be the G -orbit of \tilde{h}_s^* . For all $s \gg 0$ the function*

$$G\tilde{h}_s^* \xrightarrow{\prod_{v \in \mathcal{S}} \text{Red}_v} \prod_{v \in \mathcal{S}} X_v^{\text{ss}}(\tilde{\Phi})^{\mathcal{R}}$$

is surjective.

Proof. This is a special case of [4, Theorem 3.5]. The set \mathcal{R} satisfies the hypotheses of that theorem by the discussion of [4, §3.3.2]. \square

For each positive divisor d of D there is a degeneracy map

$$\lambda_d : X(\tilde{\Phi}) \rightarrow X(\Phi)$$

defined on moduli by $(E, C, P) \mapsto (E/C', C'', f(P))$ where C is a cyclic order DN subgroup of E , P is a point of exact order p of E , $C' \subset C$ is the unique order d subgroup of C , $f : E \rightarrow E/C'$ is the quotient map, and $C'' \subset f(C)$ is the unique order N subgroup.

Lemma 3.2.2. *Let d be a positive divisor of D and let $\sigma \in \mathcal{R}_{\text{ram}}$ be the Frobenius of the unique ideal of \mathcal{O} of norm d . Then $\lambda_d(\tilde{h}_s^*) = (h_s^*)^\sigma$.*

Proof. Let $\mathfrak{D}_{p^{s+1}} = \mathfrak{D} \cap \mathcal{O}_{p^{s+1}}$ and $\mathfrak{N}_{p^{s+1}} = \mathfrak{N} \cap \mathcal{O}_{p^{s+1}}$, and let $x \in \widehat{K}^\times$ be a finite idele which is a uniformizer at every prime divisor of d and has trivial component at all other primes. In particular σ is the Artin symbol of x . The effect of the degeneracy map λ_d on \tilde{h}_s^* is

$$\begin{aligned} \tilde{h}_s^* &\cong (\mathbb{C}/\mathcal{O}_{p^{s+1}}, (\mathfrak{D}_{p^{s+1}}\mathfrak{N}_{p^{s+1}})^{-1}/\mathcal{O}_{p^{s+1}}, p^s\varpi) \\ &\mapsto (\mathbb{C}/x^{-1}\mathcal{O}_{p^{s+1}}, (x\mathfrak{N}_{p^{s+1}})^{-1}/x^{-1}\mathcal{O}_{p^{s+1}}, p^s\varpi). \end{aligned}$$

On the other hand, the main theorem of complex multiplication provides an isomorphism of elliptic curves with $\Gamma_0(N) \cap \Gamma_1(p)$ level structure

$$\begin{aligned} (h_s^*)^\sigma &\cong (\mathbb{C}/\mathcal{O}_{p^{s+1}}, \mathfrak{N}_{p^{s+1}}^{-1}/\mathcal{O}_{p^{s+1}}, p^s\varpi)^\sigma \\ &\cong (\mathbb{C}/x^{-1}\mathcal{O}_{p^{s+1}}, (x\mathfrak{N}_{p^{s+1}})^{-1}/x^{-1}\mathcal{O}_{p^{s+1}}, p^s x^{-1}\varpi). \end{aligned}$$

As x has trivial component at p , $p^s\varpi$ and $p^s x^{-1}\varpi$ determine the same element of

$$\widehat{K}/x^{-1}\widehat{\mathcal{O}}_{p^{s+1}} = K/x^{-1}\mathcal{O}_{p^{s+1}} \cong E_{p^s, 1}^\sigma(\mathbb{C})_{\text{tors}},$$

and so $\lambda_d(\tilde{h}_s^*) = (h_s^*)^\sigma$. \square

Proposition 3.2.3 (Ribet). *Fix a $v \in \mathcal{S}$ and let $M_v(\Phi)$ and $M_v(\tilde{\Phi})$ denote the \mathbb{Z} -modules of degree zero divisors on $X_v^{\text{ss}}(\Phi)$ and $X_v^{\text{ss}}(\tilde{\Phi})$, respectively. The product of degeneracy maps*

$$\prod_{d|D} \lambda_{d,*} : M_v(\tilde{\Phi}) \rightarrow \prod_{d|D} M_v(\Phi)$$

is surjective.

Proof. By induction on the number of prime divisors of D it suffices to prove that the product of degeneracy maps

$$(29) \quad M_v(\Gamma_0(ND'q) \cap \Gamma_1(p)) \rightarrow M_v(\Gamma_0(ND') \cap \Gamma_1(p)) \times M_v(\Gamma_0(ND') \cap \Gamma_1(p))$$

is surjective for any divisor $D'q \mid D$ with q prime (using the obvious generalization of the notation $M_v(\Phi)$). If one replaces $\Gamma_1(p)$ by $\Gamma_0(p)$ then this is precisely [31, Theorem 3.15]. We give the full proof in the general case.

Let A be a supersingular elliptic curve over \mathbb{F}_v endowed with a $\Gamma_0(ND')$ -level structure, C , and a $\Gamma_1(p)$ -level structure, $P \in A[p]$. The first claim is that for any $t \in (\mathbb{Z}/p\mathbb{Z})^\times$ there is an endomorphism of A which has degree an odd power of q , restricts to an isomorphism of C , and takes P to tP . Indeed let

$$S = \{f \in \text{End}_{\mathbb{F}_v}(A) \mid f(C) \subset C, f(P) \in \mathbb{Z} \cdot P\}.$$

Then S is a level $ND'p$ Eichler order in a rational quaternion algebra B of discriminant $\ell = \text{char}(\mathbb{F}_v)$. Set $\widehat{S} = S \otimes_{\mathbb{Z}} \widehat{\mathbb{Z}}$ and define \widehat{B} similarly. The action of $S \otimes \mathbb{Z}_p$ on the subgroup generated by P determines a surjective character

$$\psi : \widehat{S}^\times \rightarrow (S \otimes \mathbb{Z}_p)^\times \rightarrow (\mathbb{Z}/p\mathbb{Z})^\times$$

whose kernel is a compact open subgroup $U \subset \widehat{B}^\times$. Pick $\tau \in \widehat{S}^\times$ such that $\psi(\tau) = t$ and such that τ has trivial components away from p . Using strong approximation as in [16, Proposition 3.1] we may write $\tau = \beta ub$ in which $\beta \in B^\times$, $u \in U$ has trivial component at q , and $b \in \widehat{B}^\times$ has trivial components away from q and reduced norm satisfying $\text{ord}_q(N(b)) = -1$. These conditions imply that β lies in the $\mathbb{Z}[1/q]$ -order $S[1/q]$, has reduced norm q , and satisfies $\psi(\beta) = \psi(\tau) = t$. Multiplying β by a sufficiently large power of q gives an element $f = q^e \beta \in S$ having reduced norm (= degree) an odd power of q , and we are free to assume that $q^e \equiv 1 \pmod{p}$. But then

$$f(P) = \psi(q^e \beta) \cdot P = \psi(\beta) \cdot P = \psi(\tau) \cdot P = t \cdot P.$$

As the degree of f is prime to ND' , f restricts to an isomorphism of C and so satisfies the desired properties.

Now suppose we are given two supersingular elliptic curves A and A' over \mathbb{F}_v , each endowed with a $\Gamma_0(ND') \cap \Gamma_1(p)$ -level structure. According to [31, Lemma 3.1.7] there is an isogeny $A \rightarrow A'$ having degree an odd power of q and preserving the $\Gamma_0(ND'p)$ -level structures. Pre-composing this isogeny with an endomorphism of A as in the preceding paragraph we obtain an isogeny $A \rightarrow A'$ of degree an *even* power of q which takes the $\Gamma_0(ND') \cap \Gamma_1(p)$ -level structure on A isomorphically to that on A' . We may factor this isogeny as

$$A_0 \xrightarrow{\pi_0} A_1 \xrightarrow{\pi_1} \cdots \rightarrow A_{2i-1} \xrightarrow{\pi_{2i-1}} A_{2i}$$

in which $A = A_0$, $A' = A_{2i}$, and each π_j has degree q . We define $\Gamma_0(ND') \cap \Gamma_1(p)$ -level structures on each A_j in such a way that the π_j 's preserve the level. Each π_j and its dual π_j^\vee then define $\Gamma_0(q)$ -level structures on A_j and A_{j+1} , respectively. Abusing notation, we write π_j to indicate A_j with its $\Gamma_0(ND') \cap \Gamma_1(p)$ -level structure, together with its $\Gamma_0(q)$ -level structure determined by π_j . Similarly we write π_j^\vee for A_{j+1} with its $\Gamma_0(ND') \cap \Gamma_1(p)$ -level structure together with its $\Gamma_0(q)$ -level structure determined by π_j^\vee . Then

$$\pi_0 - \pi_1^\vee + \pi_2 - \pi_3^\vee + \cdots + \pi_{2i-2} - \pi_{2i-1}^\vee$$

is an element of $M_v(\Gamma_0(ND'q) \cap \Gamma_1(p))$, and a simple calculation shows that the image of this element under (29) is the pair $(A - A', 0)$, where we view A and A' (with their added level structures) as divisors on $X(\Gamma_0(ND') \cap \Gamma_1(p))$. Replacing π_j by its dual everywhere gives a similar element of $M_v(\Gamma_0(ND'q) \cap \Gamma_1(p))$ whose image under (29) is $(0, A - A')$. As elements of this form generate the right hand side of (29), we are done. \square

Theorem 3.2.4 (Ihara). *Let J_1 be the Jacobian of $X(\Phi) = X_1$ and write \underline{J}_1 for the Néron model of J_1 over $\text{Spec}(\mathbb{Z})$. For every $v \in \mathcal{S}$ the cokernel of the natural map $M_v(\Phi) \rightarrow \underline{J}_1(\mathbb{F}_v)$ has order dividing $\phi(N)$.*

Proof. This is similar to [30, Proposition 3.6] and to [14, §4.2], and we give a sketch of the proof. In all that follows, all geometric objects are defined over \mathbb{F}_v unless otherwise indicated. The cokernel of the map in question is isomorphic to the

Galois group of the maximal unramified abelian extension $C/X(\Phi)$ in which all supersingular points split completely. Ihara [15] defines a curve $X_{\text{Ih}}(Np)$ whose base change to $\overline{\mathbb{F}}_v$ is isomorphic to a connected component of the modular curve $X(Np)_{/\overline{\mathbb{F}}_v}$ classifying elliptic curves with full $\Gamma(Np)$ -level structure. Owing to our assumption that $N(v) \equiv 1 \pmod{Np}$, the modular curve $X(Np)$ has all of its geometric components already defined over \mathbb{F}_v , and Ihara's curve is isomorphic (over \mathbb{F}_v) to every component. Fixing one such isomorphism, Ihara's curve admits a degeneracy map to $X(\Phi)$. By the main result of [15] all supersingular points on $X_{\text{Ih}}(Np)$ are defined over \mathbb{F}_v and there are no unramified extensions of $X_{\text{Ih}}(Np)$ in which all supersingular points split completely. It follows that C is a subextension of $X_{\text{Ih}}(Np)$, and being abelian C is then a subextension of $X_1(Np)$. The theorem follows. \square

Let $\text{Div}^0(\mathcal{G}^*h_s^*)$ denote the group of degree zero divisors on $X(\Phi)_{/L_s^*}$ which are supported on the \mathcal{G}^* orbit of h_s^* . For each $v \in \mathcal{S}$ define

$$\text{Red}_v : J_1(L_s^*) \rightarrow \underline{J}_1(\mathbb{F}_v)^{\mathcal{R}_{\text{tors}}}$$

to be the map taking $P \in J_1(L_s^*)$ to the $|\mathcal{R}_{\text{tors}}|$ -tuple having the reduction at \bar{v} of P^σ in the $\sigma \in \mathcal{R}_{\text{tors}}$ component.

Lemma 3.2.5. *For $s \gg 0$ the composition*

$$(30) \quad \text{Div}^0(\mathcal{G}^*h_s^*) \otimes \mathcal{O}_F \rightarrow J_1(L_s^*) \otimes \mathcal{O}_F \xrightarrow{\oplus_{v \in \mathcal{S}} \text{Red}_v} \oplus_{v \in \mathcal{S}} \underline{J}_1(\mathbb{F}_v)^{\mathcal{R}_{\text{tors}}} \otimes \mathcal{O}_F$$

is surjective.

Proof. Let $\text{Div}^0(\mathcal{G}^*\tilde{h}_s^*)$ be the group of degree zero divisors of $X(\tilde{\Phi})_{/L_s^*}$ supported on the \mathcal{G}^* orbit of \tilde{h}_s^* . Identify $\mathcal{R}_{\text{tors}} = \mathcal{R} \times \mathcal{R}_{\text{ram}}$ and identify \mathcal{R}_{ram} with the set of positive divisors of D by taking $d \mid D$ to the Frobenius of the unique \mathcal{O} -ideal of norm d . Consider the diagram

$$\begin{array}{ccccc} \text{Div}^0(\mathcal{G}^*\tilde{h}_s^*) & \longrightarrow & \text{Div}^0(\mathcal{G}^*\tilde{h}_s^*)^{\mathcal{R}} & \longrightarrow & \bigoplus_{v \in \mathcal{S}} M_v(\tilde{\Phi})^{\mathcal{R}} \\ \downarrow \lambda_{1,*} & & \downarrow \prod_{d \mid D} \lambda_{d,*} & & \downarrow \prod_{d \mid D} \lambda_{d,*} \\ \text{Div}^0(\mathcal{G}^*h_s^*) & \longrightarrow & \text{Div}^0(\mathcal{G}^*h_s^*)^{\mathcal{R}_{\text{tors}}} & \longrightarrow & \bigoplus_{v \in \mathcal{S}} M_v(\Phi)^{\mathcal{R}_{\text{tors}}} \end{array}$$

in which the upper left horizontal arrow takes h to the $|\mathcal{R}|$ -tuple $(h^\sigma)_\sigma$ and similarly for the bottom left horizontal arrow. The upper right horizontal arrow is the map on divisors induced by (28) and the lower right arrow is defined in a similar way. The composition of the upper row is then the map on divisors induced by the function of Theorem 3.2.1, and so is surjective for $s \gg 0$ by that theorem. The commutativity of the left hand square follows from Lemma 3.2.2, while the commutativity of the right hand square is clear. The rightmost vertical arrow is surjective by Proposition 3.2.3. Hence the bottom horizontal composition is surjective for $s \gg 0$, and the surjectivity of (30) then follows from Theorem 3.2.4 and our hypothesis that p does not divide $\phi(N)$. \square

Proof of Theorem 3.1.1. By [9, Lemma 8.1] $\text{Ta}_p^{\text{ord}}(J_1)$ is the module of Γ coinvariants of \mathbf{Ta}^{ord} . This allows us to identify

$$(31) \quad \text{Ta}_p^{\text{ord}}(J_1) / \mathfrak{m} \text{Ta}_p^{\text{ord}}(J_1) \cong \mathbf{T} / \mathfrak{m} \mathbf{T}.$$

Define \mathcal{H}_s to be the image of the composition

$$\mathrm{Div}^0(\mathcal{G}^*h_s^*) \otimes \mathcal{O}_F \rightarrow J_1(L_s^*) \otimes \mathcal{O}_F \rightarrow H^1(L_s^*, \mathrm{Ta}_p^{\mathrm{ord}}(J_1)) \rightarrow H^1(L_s^*, \mathbf{T}/\mathfrak{m}\mathbf{T})$$

and define

$$e'_\chi : H^1(L_s^*, \mathrm{Ta}_p^{\mathrm{ord}}(J_1)) \rightarrow H^1(L_s^*, \mathrm{Ta}_p^{\mathrm{ord}}(J_1))$$

by

$$e'_\chi(h) = \sum_{\sigma \in \mathcal{R}_{\mathrm{tors}}} (\Theta^{-1}\chi)(\sigma) \cdot h^\sigma.$$

We claim that the dimension of $e'_\chi \mathcal{H}_s$ as an R/\mathfrak{m} -vector space goes to ∞ as $s \rightarrow \infty$.

We may compute the image of $e'_\chi \mathcal{H}_s$ under the sum of localization maps

$$H^1(L_s^*, \mathbf{T}/\mathfrak{m}\mathbf{T}) \rightarrow \bigoplus_{v \in \mathcal{S}} H^1(L_{s,v}^*, \mathbf{T}/\mathfrak{m}\mathbf{T})$$

as the image of the composition of (30) and

$$(32) \quad \bigoplus_{v \in \mathcal{S}} J_1(\mathbb{F}_v)^{\mathcal{R}_{\mathrm{tors}}} \otimes \mathcal{O}_F \rightarrow \bigoplus_{v \in \mathcal{S}} H^1(\mathbb{F}_v, \mathrm{Ta}_p^{\mathrm{ord}}(J_1))^{\mathcal{R}_{\mathrm{tors}}} \\ \rightarrow \bigoplus_{v \in \mathcal{S}} H^1(\mathbb{F}_v, \mathbf{T}/\mathfrak{m}\mathbf{T})^{\mathcal{R}_{\mathrm{tors}}} \xrightarrow{e'_\chi} \bigoplus_{v \in \mathcal{S}} H^1(\mathbb{F}_v, \mathbf{T}/\mathfrak{m}\mathbf{T}),$$

using the isomorphism

$$H^1(\mathbb{F}_v, \mathbf{T}/\mathfrak{m}\mathbf{T}) \cong H_{\mathrm{unr}}^1(L_{s,v}^*, \mathbf{T}/\mathfrak{m}\mathbf{T}).$$

In the above composition the arrow labeled e'_χ preserves the v component for each $v \in \mathcal{S}$ and takes the $|\mathcal{R}_{\mathrm{tors}}|$ -tuple $(x_\sigma)_{\sigma \in \mathcal{R}_{\mathrm{tors}}}$ to

$$\sum_{\sigma \in \mathcal{R}_{\mathrm{tors}}} (\Theta^{-1}\chi)(\sigma) \cdot x_\sigma \in H^1(\mathbb{F}_v, \mathbf{T}/\mathfrak{m}\mathbf{T}).$$

Each arrow in the composition (32) is surjective; this follows from the fact that the absolute Galois group of \mathbb{F}_v has cohomological dimension 1, and, for the first arrow, Lang's theorem on the vanishing of $H^1(\mathbb{F}_v, J_1(\overline{\mathbb{F}_v}))$ as in [21, Proposition I.3.8]. Combining this with Lemma 3.2.5, for $s \gg 0$ the dimension of $e'_\chi \mathcal{H}_s$ is at least that of $\bigoplus_{v \in \mathcal{S}} H^1(\mathbb{F}_v, \mathbf{T}/\mathfrak{m}\mathbf{T})$. If we choose \mathcal{S} in such a way that the Frobenius of the prime of \mathbb{Q} below each $v \in \mathcal{S}$ acts as (a conjugate of) complex conjugation on the extension of $K(\mu_{Np})$ cut out by $\mathbf{T}/\mathfrak{m}\mathbf{T}$, then

$$\dim_{R/\mathfrak{m}} H^1(\mathbb{F}_v, \mathbf{T}/\mathfrak{m}\mathbf{T}) = 2.$$

Thus the dimension of $e'_\chi \mathcal{H}_s$ over R/\mathfrak{m} is at least $2|\mathcal{S}|$ for $s \gg 0$. As we may take \mathcal{S} as large as we like, $\dim(e'_\chi \mathcal{H}_s) \rightarrow \infty$.

Recall $L_s^* = H_{p^{s+1}}(\mu_p) = L_{p^s,1}$ and $h_s^* = h_{p^s,1}$. The character

$$\Theta : G_{\mathbb{Q}} \rightarrow (R/\mathfrak{m})^\times$$

is trivial over $\mathbb{Q}(\mu_p)$, and twisting the isomorphism (31) by Θ^{-1} gives an isomorphism

$$H^1(L_{s-1}^*, \mathbf{T}^\dagger/\mathfrak{m}\mathbf{T}^\dagger) \cong H^1(L_{s-1}^*, \mathrm{Ta}_p^{\mathrm{ord}}(J_1)/\mathfrak{m}\mathrm{Ta}_p^{\mathrm{ord}}(J_1)) \otimes \zeta_1$$

taking the image of \mathfrak{X}_{p^s} to the image of $U_p^{-1}\mathfrak{X}_{p^s,1}$ (by Definition 2.2.3). Tracing through the constructions of §2.2, the image of h_s^* under

$$X(\Phi)(L_s^*) \rightarrow \mathrm{Div}(X(\Phi)/L_s^*) \otimes \mathcal{O}_F \xrightarrow{e^{\mathrm{ord}}} J_1(L_s^*)^{\mathrm{ord}} \rightarrow H^1(L_s^*, \mathbf{T}/\mathfrak{m}\mathbf{T})$$

agrees with the Kummer image of $y_{p^s,1} \in J_1(L_s^*)^{\text{ord}}$, which is taken to $\mathfrak{X}_{p^s,1}$ under

$$(33) \quad H^1(L_s^*, \mathbf{T}/\mathfrak{m}\mathbf{T}) \xrightarrow{\text{cor}} H^1(L_{s-1}^*, \mathbf{T}/\mathfrak{m}\mathbf{T}) \xrightarrow{h \mapsto h \otimes \zeta_1} H^1(L_{s-1}^*, \mathbf{T}/\mathfrak{m}\mathbf{T}) \otimes \zeta_1.$$

It follows that (33) takes \mathcal{H}_s to the restriction of Heeg_s to L_{s-1}^* . But

$$N(h_s^*) = N(h_{p^s,1}) = N(\alpha_*(h_{p^{s-1},2})) = U_p \cdot h_{p^{s-1},1} = U_p \cdot h_{s-1}^*.$$

by (11), where all norms are from L_s^* to L_{s-1}^* , and so $\text{cor}(\mathcal{H}_s) = \mathcal{H}_{s-1}$. We conclude

$$\mathcal{H}_{s-1} \otimes \zeta_1 = \text{res}_{H_{p^s}(\mu_p)/H_{p^s}}(\text{Heeg}_s)$$

and in particular

$$\begin{aligned} (e'_\chi \mathcal{H}_{s-1}) \otimes \zeta_1 &= \left(\sum_{\sigma \in \mathcal{R}_{\text{tors}}} \chi(\sigma) \sigma \right) \cdot (\mathcal{H}_{s-1} \otimes \zeta_1) \\ &= \text{res}_{H_{p^s}(\mu_p)/H_{p^s}}(e_\chi \text{Heeg}_s). \end{aligned}$$

As the dimension of $e'_\chi \mathcal{H}_{s-1}$ is unbounded as $s \rightarrow \infty$, so is that of $e_\chi \text{Heeg}_s$. \square

3.3. A two-variable main conjecture. Let D_s/K be the subfield of D_∞ of degree p^s over K . There is a nonnegative integer δ such that the fixed field $(H_{p^{s+1}})^{\mathcal{G}_{\text{tors}}} = H_{p^{s+1}} \cap D_\infty$ is equal to $D_{p^{s+\delta}}$ for all $s \gg 0$. If p does not divide the class number of K then $\delta = 0$. Define, for any $s \geq 0$ and using (21) and Proposition 2.4.5,

$$\mathfrak{Z}_s \in \tilde{H}_f^1(D_s, \mathbf{T}^\dagger)$$

to be the image of $U_p^{-t} \cdot \mathfrak{X}_{p^{t+1}}$ under corestriction

$$\tilde{H}_f^1(H_{p^{t+1}}, \mathbf{T}^\dagger) \rightarrow \tilde{H}_f^1(D_s, \mathbf{T}^\dagger)$$

for any t large enough that $D_s \subset H_{p^{t+1}}$. By Proposition 2.3.1 the class \mathfrak{Z}_s does not depend on the choice of t , and as s varies these classes are norm compatible. We may therefore define a module

$$\tilde{H}_{f,\text{Iw}}^i(D_\infty, \mathbf{T}^\dagger) = \varprojlim \tilde{H}_f^i(D_s, \mathbf{T}^\dagger)$$

over the ring $R_\infty = R[[\text{Gal}(D_\infty/K)]]$ and define $\mathfrak{Z}_\infty \in \tilde{H}_{f,\text{Iw}}^1(D_\infty, \mathbf{T}^\dagger)$ by

$$\mathfrak{Z}_\infty = \varprojlim \mathfrak{Z}_s.$$

By Corollary 3.1.2, \mathfrak{Z}_∞ is not R_∞ -torsion. Indeed, if \mathfrak{p} is any arithmetic prime of R and \mathfrak{P} denotes the kernel of the map $R_\infty \rightarrow R_\infty \otimes_R F_{\mathfrak{p}}$, then \mathfrak{P} is a height one prime of R_∞ at which \mathfrak{Z}_∞ is locally nontrivial. As there are infinitely many such \mathfrak{P} , \mathfrak{Z}_∞ is nontorsion (exactly as in the proof of Lemma 2.1.7).

The following conjecture is an extension of the Heegner point main conjecture for elliptic curves formulated by Perrin-Riou [29]. Partial results toward Perrin-Riou's conjecture have been obtained by Bertolini [1] and the author [12, 13]. Assume that R is regular, so that $R_{\infty, \mathfrak{P}}$ is a discrete valuation ring for every height one prime \mathfrak{P} of R_∞ . If M is a finitely generated torsion R_∞ -module, define the characteristic ideal

$$\text{char}(M) = \prod_{\mathfrak{P}} \mathfrak{P}^{\text{length}(M_{\mathfrak{P}})}$$

where the product is over height one primes of R_∞ . If M is not torsion then set $\text{char}(M) = 0$.

Conjecture 3.3.1. *Assuming that R is regular*

$$\text{char}(\tilde{H}_{f,\text{Iw}}^1(D_\infty, \mathbf{T}^\dagger)/R_\infty \mathfrak{Z}_\infty)^2 = \text{char}(\tilde{H}_{f,\text{Iw}}^2(D_\infty, \mathbf{T}^\dagger)_{\text{tors}})$$

in which the subscript tors indicates the R_∞ -torsion submodule.

Remark 3.3.2. As we assume that N is prime to $\text{disc}(K)$, the branch R of the Hida family does not have complex multiplication by K (that is, R does not arise by the construction of [10, §7] from a Hecke character of K). In this situation Nekovář, using results of Cornut-Vatsal and duality theorems for Selmer complexes, proves [25, Theorem 12.9.11] that for $i = 1, 2$

$$\text{rank}_{R_\infty}(\tilde{H}_{f,\text{Iw}}^i(D_\infty, \mathbf{T}^\dagger)) = 1.$$

Remark 3.3.3. Iwasawa main conjectures are more often expressed in terms of the Pontryagin dual of a Selmer group attached to the discrete Galois module $\mathbf{A}^\dagger = \text{Hom}_{\mathbb{Z}_p}(\mathbf{T}^\dagger, \mu_{p^\infty})$. Conjecture 3.3.1 may be reformulated in this manner using the isomorphism of Poitou-Tate global duality [25, §0.13]

$$\tilde{H}_{f,\text{Iw}}^2(D_\infty, \mathbf{T}^\dagger) \cong \text{Hom}_{\mathbb{Z}_p}(\tilde{H}_f^1(D_\infty, \mathbf{A}^\dagger), \mathbb{Q}_p/\mathbb{Z}_p)$$

for an appropriate extended Selmer group $\tilde{H}_f^1(D_\infty, \mathbf{A}^\dagger)$.

3.4. The horizontal nonvanishing conjecture. Let \mathfrak{X}_1 be the big Heegner point of conductor $c = 1$ as in Definition 2.2.3, so that

$$\mathfrak{Z}_0 = \text{Cor}_{H_1/K}(\mathfrak{X}_1) \in \tilde{H}_f^1(K, \mathbf{T}^\dagger).$$

Conjecture 3.4.1. *The cohomology class \mathfrak{Z}_0 is not R -torsion.*

The theory of Euler systems allows one to use the cohomology classes \mathfrak{X}_c to bound the Selmer group of $V_{\mathfrak{p}}^\dagger$.

Theorem 3.4.2 (Nekovář). *Let $\mathfrak{p} \subset R$ be an arithmetic prime with trivial wild character and weight $r \equiv k + j \pmod{p-1}$ with $r > 2$. If \mathfrak{Z}_0 has nontrivial image in $\tilde{H}_f^1(K, V_{\mathfrak{p}}^\dagger)$ then $\dim_{F_{\mathfrak{p}}} \tilde{H}_f^1(K, V_{\mathfrak{p}}^\dagger) = 1$.*

Proof. Our hypotheses imply that the modular form $g_{\mathfrak{p}}$ attached to \mathfrak{p} has even weight and trivial character. In particular by (22) and (23) the Greenberg, Nekovář, and Bloch–Kato Selmer groups for $V_{\mathfrak{p}}^\dagger$ all agree. By Lemma 2.1.5 the Galois representation $V_{\mathfrak{p}}^\dagger$ is a self-dual twist of the representation associated to a newform of level N . Specializing the Euler system of big Heegner points to an Euler system for $V_{\mathfrak{p}}^\dagger$, the stated theorem follows from the results of [23]. The Euler system used by Nekovář is different from the one constructed here (or at least the construction is different), but the proofs in [23, §6–13] only require the existence of some family of cohomology classes satisfying the Euler system relations of §2.3 and lying in the Bloch–Kato Selmer group. We note that the hypothesis $p \nmid (r-2)!$ of [23] is used only in the construction of the Euler system classes and not in the bounding of the Selmer group. \square

Corollary 3.4.3. *Assume Conjecture 3.4.1. Then $\tilde{H}_f^1(K, \mathbf{T}^\dagger)$ is a rank one R -module and*

$$\text{rank}_R \tilde{H}_f^1(\mathbb{Q}, \mathbf{T}^\dagger) = \begin{cases} 1 & \text{if } w = 1 \\ 0 & \text{if } w = -1 \end{cases}$$

where $w = \pm 1$ is as in Proposition 2.3.6.

Proof. By [25, Proposition 4.2.3] and [27, Theorem 8.3.19] the extended Selmer group $\tilde{H}_f^i(K, \mathbf{T}^\dagger)$ is finitely generated over R for all i . Let $\mathfrak{p} \subset R$ be an arithmetic prime. Using Lemma 2.1.6, Nekovář's theory [25, Proposition 12.7.13.4(i)] provides an exact sequence of extended Selmer groups

$$0 \rightarrow \tilde{H}_f^1(K, \mathbf{T}^\dagger)_{\mathfrak{p}} / \mathfrak{p} \tilde{H}_f^1(K, \mathbf{T}^\dagger)_{\mathfrak{p}} \rightarrow \tilde{H}_f^1(K, V_{\mathfrak{p}}^\dagger) \rightarrow \tilde{H}_f^2(K, \mathbf{T}^\dagger)_{\mathfrak{p}}[\mathfrak{p}] \rightarrow 0$$

induced by the exact sequence

$$0 \rightarrow \mathbf{T}_{\mathfrak{p}}^\dagger \xrightarrow{\pi} \mathbf{T}_{\mathfrak{p}}^\dagger \rightarrow V_{\mathfrak{p}}^\dagger \rightarrow 0$$

for any generator $\pi \in \mathfrak{p}R_{\mathfrak{p}}$. It follows from Lemma 2.1.7 that \mathfrak{Z}_0 has nontrivial image in $\tilde{H}_f^1(K, V_{\mathfrak{p}}^\dagger)$ for all but finitely many \mathfrak{p} . Theorem 3.4.2 now shows that $\tilde{H}_f^1(K, V_{\mathfrak{p}}^\dagger)$ is one dimensional for infinitely many arithmetic primes \mathfrak{p} . The finite generation of $\tilde{H}_f^2(K, \mathbf{T}^\dagger)$ implies that $\tilde{H}_f^2(K, \mathbf{T}^\dagger)_{\mathfrak{p}}$ has no $R_{\mathfrak{p}}$ torsion for all but finitely many arithmetic primes \mathfrak{p} . From the above exact sequence of extended Selmer groups and Nakayama's lemma we deduce that the R -module $\tilde{H}_f^1(K, \mathbf{T}^\dagger)$ is locally generated by a single element at infinitely many arithmetic primes \mathfrak{p} . The torsion submodule of $\tilde{H}_f^1(K, \mathbf{T}^\dagger)$ has finite support, and so $\tilde{H}_f^1(K, \mathbf{T}^\dagger)$ is locally free of rank one at infinitely many arithmetic primes. The existence of any one such prime implies that $\tilde{H}_f^1(K, \mathbf{T}^\dagger)$ has rank one. Proposition 2.3.5 shows that complex conjugation acts as w on \mathfrak{Z}_0 , and so the second claim follows from the first. \square

REFERENCES

- [1] M. Bertolini. Selmer groups and Heegner points in anticyclotomic \mathbb{Z}_p -extensions. *Compositio Math.*, 99(2):153–182, 1995.
- [2] S. Bloch and K. Kato. L -functions and Tamagawa numbers of motives. In *The Grothendieck Festschrift, Vol. I*, volume 86 of *Progr. Math.*, pages 333–400. Birkhäuser Boston, Boston, MA, 1990.
- [3] C. Cornut. Mazur's conjecture on higher Heegner points. *Invent. Math.*, 148(3):495–523, 2002.
- [4] C. Cornut and V. Vatsal. CM points and quaternion algebras. *Doc. Math.*, 10:263–309 (electronic), 2005.
- [5] M. Emerton, R. Pollack, and T. Weston. Variation of Iwasawa invariants in Hida families. Preprint available at math.bu.edu/people/rpollack, 2004.
- [6] R. Greenberg. Iwasawa theory for motives. In *L-functions and arithmetic, proceedings of the Durham symposium, July, 1989*, volume 153 of *London Math. Soc. Lecture Note Series*, pages 211–233. Cambridge University Press, Cambridge, UK, 1991.
- [7] R. Greenberg. Elliptic curves and p -adic deformations. In *Elliptic curves and related topics*, volume 4 of *CRM Proc. Lecture Notes*, pages 101–110. Amer. Math. Soc., Providence, RI, 1994.
- [8] R. Greenberg and G. Stevens. p -adic L -functions and p -adic periods of modular forms. *Invent. Math.*, 111(2):407–447, 1993.
- [9] H. Hida. Galois representations into $\mathrm{GL}_2(\mathbb{Z}_p[[X]])$ attached to ordinary cusp forms. *Invent. Math.*, 85(3):545–613, 1986.
- [10] H. Hida. Iwasawa modules attached to congruences of cusp forms. *Ann. Sci. École Norm. Sup. (4)*, 19(2):231–273, 1986.
- [11] H. Hida. *Elementary theory of L-functions and Eisenstein series*, volume 26 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 1993.
- [12] B. Howard. The Heegner point Kolyvagin system. *Compos. Math.*, 140(6):1439–1472, 2004.
- [13] B. Howard. Iwasawa theory of Heegner points on abelian varieties of GL_2 type. *Duke Math. J.*, 124(1):1–45, 2004.
- [14] B. Howard. Special cohomology classes for modular Galois representations. *J. Number Theory*, 117(2):406–438, 2006.

- [15] Y. Ihara. On modular curves over finite fields. In *Discrete Subgroups of Lie Groups and Applications to Moduli (Internat. Colloq., Bombay, 1973)*, pages 161–202. Oxford Univ. Press, Bombay, 1975.
- [16] B. Jordan and R. Livné. Integral Hodge theory and congruences between modular forms. *Duke Math. J.*, 80(2):419–484, 1995.
- [17] H. Matsumura. *Commutative ring theory*, volume 8 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, second edition, 1989. Translated from the Japanese by M. Reid.
- [18] B. Mazur, J. Tate, and J. Teitelbaum. On p -adic analogues of the conjectures of Birch and Swinnerton-Dyer. *Invent. Math.*, 84(1):1–48, 1986.
- [19] B. Mazur and J. Tilouine. Représentations galoisiennes, différentielles de Kähler et “conjectures principales”. *Inst. Hautes Études Sci. Publ. Math.*, (71):65–103, 1990.
- [20] B. Mazur and A. Wiles. Class fields of abelian extensions of \mathbb{Q} . *Invent. Math.*, 76(2):179–330, 1984.
- [21] J. S. Milne. *Arithmetic Duality Theorems*, volume 1 of *Perspectives in Mathematics*. Academic Press Inc., Boston, MA, 1986.
- [22] T. Miyake. *Modular forms*. Springer-Verlag, Berlin, 1989. Translated from the Japanese by Yoshitaka Maeda.
- [23] J. Nekovář. Kolyvagin’s method for Chow groups of Kuga-Sato varieties. *Invent. Math.*, 107(1):99–125, 1992.
- [24] J. Nekovář. On the p -adic height of Heegner cycles. *Math. Ann.*, 302(4):609–686, 1995.
- [25] J. Nekovář. Selmer Complexes, fourth version. Available at www.math.jussieu.fr/~nekoavar, 2006.
- [26] J. Nekovář and A. Plater. On the parity of ranks of Selmer groups. *Asian J. Math.*, 4(2):437–497, 2000.
- [27] J. Neukirch, A. Schmidt, and K. Wingberg. *Cohomology of number fields*, volume 323 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 2000.
- [28] M. Ohta. On the p -adic Eichler-Shimura isomorphism for Λ -adic cusp forms. *J. Reine Angew. Math.*, 463:49–98, 1995.
- [29] B. Perrin-Riou. Fonctions L p -adiques, théorie d’Iwasawa et points de Heegner. *Bull. Soc. Math. France*, 115(4):399–456, 1987.
- [30] D. Prasad. Ribet’s theorem: Shimura-Taniyama-Weil implies Fermat. In *Seminar on Fermat’s Last Theorem (Toronto, ON, 1993–1994)*, volume 17 of *CMS Conf. Proc.*, pages 155–177. Amer. Math. Soc., Providence, RI, 1995.
- [31] K. A. Ribet. On modular representations of $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ arising from modular forms. *Invent. Math.*, 100(2):431–476, 1990.
- [32] K. Rubin. *Euler systems*, volume 147 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, 2000. Hermann Weyl Lectures. The Institute for Advanced Study.
- [33] G. Shimura. *Introduction to the arithmetic theory of automorphic functions*. Publications of the Mathematical Society of Japan, No. 11. Iwanami Shoten, Publishers, Tokyo, 1971.
- [34] V. Vatsal. Uniform distribution of Heegner points. *Invent. Math.*, 148(1):1–46, 2002.
- [35] S. Zhang. Heights of Heegner cycles and derivatives of L -series. *Invent. Math.*, 130(1):99–152, 1997.

DEPT. OF MATHEMATICS, UNIVERSITY OF CHICAGO, 5734 S. UNIVERSITY AVE., CHICAGO, IL 60637

Current address: Dept. of Mathematics, Boston College, Chestnut Hill, MA 02467

E-mail address: howardbe@bc.edu