

IWASAWA THEORY OF HEEGNER POINTS ON ABELIAN VARIETIES OF GL_2 -TYPE

BENJAMIN HOWARD

ABSTRACT. In an earlier paper the author proved one divisibility of Perrin-Riou's Iwasawa main conjecture for Heegner points on elliptic curves. In the present paper, that result is generalized to abelian varieties of GL_2 -type (i.e. abelian varieties with real multiplication defined over totally real fields) under the hypothesis that the abelian variety is associated to a Hilbert modular form via a construction of Zhang.

CONTENTS

0.	Introduction	1
1.	Hilbert modular forms and Heegner points	3
2.	Bounding the Selmer group	9
3.	Iwasawa theory	18
	References	33

0. INTRODUCTION

Let E be a CM field with $[E : \mathbf{Q}] = 2g$, $F \subset E$ the maximal real subfield, and ϵ the quadratic character associated to E/F . Let N be an integral ideal of F which is prime to the relative discriminant of E/F , and which satisfies the *weak Heegner hypothesis* that $\epsilon(N) = (-1)^{g-1}$. Given a Hilbert modular eigenform ϕ of parallel weight 2 for $\Gamma_0(N)$, the recent work of Zhang associates to ϕ an isogeny class of abelian varieties over F occurring as quotients of the Jacobian of a certain Shimura curve X associated to the data (N, E) . These abelian varieties have good reduction away from N and admit real multiplication by the totally real field F_ϕ generated by the Hecke eigenvalues of ϕ . Fix one such quotient $\text{Jac}(X) \rightarrow A$, let $\mathcal{O} \subset F_\phi$ be an order with $\mathcal{O} \hookrightarrow \text{End}_F(A)$, and choose an \mathcal{O} -linear polarization of A .

We abbreviate $G_E = \text{Gal}(\bar{E}/E)$. For any rational prime p , the p -adic Tate module of A decomposes as a direct sum of G_E -submodules

$$T_p(A) \cong \bigoplus_{\mathfrak{P}|p} T_{\mathfrak{P}}(A)$$

where the sum is over the primes of F_ϕ above p . Fix a prime \mathfrak{P} of F_ϕ , let $\mathcal{O}_{\mathfrak{P}}$ be the completion of \mathcal{O} at \mathfrak{P} , and let p be the rational prime below \mathfrak{P} . We assume

2000 *Mathematics Subject Classification.* 11G05, 11G10, 11R23.

This research was partially conducted by the author for the Clay Mathematics Institute.

- (1) the order $\mathcal{O}_{\mathfrak{P}}$ is the maximal order of $F_{\phi, \mathfrak{P}}$ and that p does not divide 2, the class number of E , the index $[\mathcal{O}_E^\times : \mathcal{O}_F^\times]$, the absolute norm of N , or the degree of the fixed polarization of A ,
- (2) the image of $\rho_{\mathfrak{P}} : G_E \rightarrow \text{Aut}_{\mathcal{O}_{\mathfrak{P}}}(T_{\mathfrak{P}}(A)) \cong GL_2(\mathcal{O}_{\mathfrak{P}})$ is equal to the subgroup $G_{\mathfrak{P}} \subset GL_2(\mathcal{O}_{\mathfrak{P}})$ consisting of matrices whose determinant lies in $\mathbf{Z}_p^\times \subset \mathcal{O}_{\mathfrak{P}}^\times$.

We remark that $G_{\mathfrak{P}}$ is the largest image one could hope for, as the determinant of $\rho_{\mathfrak{P}}$ is equal to the cyclotomic character $G_E \rightarrow \mathbf{Z}_p^\times$. Furthermore the results of [19] suggest that when A has exactly real multiplication, i.e. $F_\phi \cong \text{End}_{\bar{E}}(A) \otimes \mathbf{Q}_p$, then condition (2) should hold for all but finitely many \mathfrak{P} . Note that this condition implies that G_E acts transitively on the nonzero elements of $A[\mathfrak{P}]$, and hence $A(L)[\mathfrak{P}] = 0$ for any abelian extension L/E .

For every finite extension L/E we have the two \mathfrak{P} -power Selmer groups which fit into the descent sequences

$$0 \rightarrow A(L) \otimes_{\mathcal{O}} \mathcal{O}_{\mathfrak{P}} \rightarrow S_{\mathfrak{P}}(A/L) \rightarrow \varprojlim \text{III}(A/L)[\mathfrak{P}^k] \rightarrow 0$$

$$0 \rightarrow A(L) \otimes_{\mathcal{O}} (\Phi_{\mathfrak{P}}/\mathcal{O}_{\mathfrak{P}}) \rightarrow \text{Sel}_{\mathfrak{P}^\infty}(A/L) \rightarrow \text{III}(A/L)[\mathfrak{P}^\infty] \rightarrow 0$$

in which $\Phi_{\mathfrak{P}}$ is the field of fractions of $\mathcal{O}_{\mathfrak{P}}$. The abelian variety A comes equipped with a family of Heegner points defined over ring class fields of E . Let $h[1]$ be the Heegner point of conductor 1, defined over the Hilbert class field $E[1]$. Generalizing the work of Kolyvagin, Kolyvagin and Logachev, and Zhang we will prove the following theorem in Section 2:

Theorem A. *Assume $\text{Norm}_{E[1]/E}(h[1]) \in A(E)$ has infinite order. Then $S_{\mathfrak{P}}(A/E)$ is free of rank one over $\mathcal{O}_{\mathfrak{P}}$, $\text{III}(A/E)[\mathfrak{P}^\infty]$ is finite, and there is an isomorphism*

$$\text{Sel}_{\mathfrak{P}^\infty}(A/E) \cong (\Phi_{\mathfrak{P}}/\mathcal{O}_{\mathfrak{P}}) \oplus M \oplus M$$

in which the order of M is bounded by the index of the $\mathcal{O}_{\mathfrak{P}}$ -submodule of $S_{\mathfrak{P}}(A/E)$ generated by $\text{Norm}_{E[1]/E}(h[1])$.

Now let \mathfrak{p} be a prime of F above p and assume, in addition to conditions (1) and (2) above, that p is unramified in E . Denote by $E[\mathfrak{p}^k]$ the ring class field of conductor \mathfrak{p}^k . Then $\cup E[\mathfrak{p}^k]$ contains a unique subfield E_∞/E with $\Gamma = \text{Gal}(E_\infty/E) \cong \mathbf{Z}_p^f$, where f is the residue degree of \mathfrak{p} . Let $\Lambda = \mathcal{O}_{\mathfrak{P}}[[\Gamma]]$ be the f -variable Iwasawa algebra, and let $E_k \subset E_\infty$ be the fixed field of Γ^{p^k} . Since we assume that p does not divide the class number of E , E_k is the maximal p -power subextension of $E[p^{k+1}]/E$, and we define h_k to be the norm from $E[\mathfrak{p}^{k+1}]$ to E_k of the Heegner point of conductor \mathfrak{p}^{k+1} . Let H_k be the Λ -module generated by all h_j with $j \leq k$, and set $H_\infty = \varprojlim H_k$. Define finitely-generated Λ -modules

$$S_{\mathfrak{P}, \infty} = \varprojlim S_{\mathfrak{P}}(A/E_k) \quad X = \varprojlim \text{Hom}_{\mathcal{O}_{\mathfrak{P}}}(\text{Sel}_{\mathfrak{P}^\infty}(A/E_k), \Phi_{\mathfrak{P}}/\mathcal{O}_{\mathfrak{P}}).$$

Let $X_{\Lambda\text{-tors}}$ denote the Λ -torsion submodule of X . In Section 3 we generalize the results of Bertolini, Nekovar, and the author. The main result is

Theorem B. *Suppose that \mathfrak{p} is the unique prime of F above p , and that A has ordinary reduction at \mathfrak{p} . Assume further that $h_k \in A(E_k)$ has infinite order for some k . Then*

- (a) H_∞ and $S_{\mathfrak{P}, \infty}$ are torsion-free, rank one Λ -modules,
- (b) X has rank one as a Λ -module,

(c) $X_{\Lambda\text{-tors}}$ decomposes as

$$X_{\Lambda\text{-tors}} \sim M \oplus M \oplus M_{\mathfrak{P}}$$

in which M has $\text{char}(M)$ prime to $\mathfrak{P}\Lambda$ and $\text{char}(M_{\mathfrak{P}})$ is a power of $\mathfrak{P}\Lambda$,

(d) $\text{char}(M)$ is fixed by the involution of Λ induced by inversion in Γ ,

(e) $\text{char}(M)$ divides the characteristic ideal of $S_{\mathfrak{P},\infty}/H_{\infty}$,

where \sim denotes pseudo-isomorphism of Λ -modules and char denotes characteristic ideal.

A few remarks are in order concerning Theorem B. Following the conjectures of Perrin-Riou in [18], we conjecture that equality holds in part (e), up to powers of $\mathfrak{P}\Lambda$. The recent success of Cornut and Vatsal in proving Mazur's conjecture on the nonvanishing of Heegner points gives us hope that the hypothesis of some h_k having infinite order is always satisfied. The hypothesis that some h_k has infinite order is not needed for the proofs of parts (c) and (d). We expect that the assumption that F has a unique prime above p is not needed.

Even in the case where $F = \mathbf{Q}$ and ϕ has rational coefficients (i.e. the case of an elliptic curve over \mathbf{Q}), the above results are still stronger than those of [9]. The reason is that we have replaced the classical Heegner hypothesis that all primes dividing the level N are split in E by the weaker hypothesis that $\epsilon(N) = 1$. Results similar to those of Theorem B in the case where $\epsilon(N) = -1$ have recently been obtained by Bertolini and Darmon in [2].

The methods used in the proofs of the two main theorems draw very heavily from methods of Mazur and Rubin in [13]. Furthermore, large portions require only trivial modifications from arguments of [9], and when this is the case we will only give sketches of the proofs.

The following notation will remain in effect throughout: F is a totally real number field of degree g and discriminant d_F , \mathcal{O}_F is the ring of integers of F , \mathbf{A} is the adèle ring of F , \mathbf{A}_f the subring of finite adèles, and \mathbf{A}_{∞} the infinite component. If v is any place of F we denote by F_v the completion of F at v , and if A is any F -algebra we let $A_v = A \otimes_F F_v$. If M is an abelian group set $\hat{M} = M \otimes_{\mathbf{Z}} \hat{\mathbf{Z}}$. In particular, $\mathbf{A}_f \cong \hat{F}$.

If L is a perfect field we let \bar{L} be an algebraic closure and $G_L = \text{Gal}(\bar{L}/L)$. If L is a number field and I is an ideal of the ring of integers of L , then we denote by $\mathbf{N}(I)$ the absolute norm of I . Given a topological G_L -module, M , and any place v of L , we let $\text{loc}_v : H^i(L, M) \rightarrow H^i(L_v, M)$ be the localization map.

We denote by \mathfrak{H} and \mathfrak{H}^{\pm} the upper half-plane and the union of the upper and lower half-planes, respectively. If E/F is a quadratic extension with E totally complex, then we say that E is a *CM-extension* of F . For any rational prime p , the p -adic Tate module of $\mu_{p^{\infty}}$ is denoted $\mathbf{Z}_p(1)$. If M is any \mathbf{Z}_p -module we set $M(1) = M \otimes \mathbf{Z}_p(1)$.

1. HILBERT MODULAR FORMS AND HEEGNER POINTS

In Section 1 we summarize some of the work of Shimura and Zhang, closely following [25] and [26], to which we refer the reader for proofs. Useful references on Hilbert modular forms and abelian varieties with real multiplication include [7] and [23]. Useful references on Shimura curves include [21] and [22], especially Chapter 9. The standard reference on quaternion algebras is [24].

1.1. **Hilbert modular forms.** For any integral ideal $N \subset \mathcal{O}_F$ let

$$K_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\hat{\mathcal{O}}_F) \mid c \equiv 0 \pmod{N} \right\}.$$

Identify \mathbf{A}^\times with the center $Z(\mathbf{A}) \subset \mathrm{GL}_2(\mathbf{A})$, and for any $\theta = (\theta_v) \in \mathbf{A}_\infty$ set

$$r(\theta) = \begin{pmatrix} \cos \theta & \sin \theta \\ -\sin \theta & \cos \theta \end{pmatrix} \in \mathrm{SO}_2(\mathbf{A}_\infty).$$

Definition 1.1.1. By a *Hilbert modular form* of (parallel) weight k and level N we mean a smooth function ϕ on $\mathrm{GL}_2(\mathbf{A})$ satisfying

- (a) ϕ is left invariant by $\mathrm{GL}_2(F)$ and right invariant by $K_0(N)Z(\mathbf{A})$,
- (b) for $r(\theta) \in \mathrm{SO}_2(\mathbf{A}_\infty)$,

$$\phi(g \cdot r(\theta)) = \phi(g) \cdot \prod_{v|\infty} e^{ik\theta_v},$$

- (c) ϕ is of *moderate growth* in the sense that for every $c > 0$ and every compact $\Omega \subset \mathrm{GL}_2(\mathbf{A})$, there is a constant M such that

$$\phi \left(\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} g \right) = O(|a|^M)$$

for all $g \in \Omega$ and $a \in \mathbf{A}^\times$ with $|a| > c$.

- (d) for every $h \in \mathrm{GL}_2(\mathbf{A}_f)$ the function

$$x + iy \mapsto |y|^{-k/2} \phi \left(\begin{pmatrix} y & x \\ 0 & 1 \end{pmatrix} h \right)$$

is holomorphic in $x + iy \in \mathfrak{H}^g$.

To any Hilbert modular form ϕ there is an associated complex-valued function a_ϕ , defined on the integral ideals of F . The value $a_\phi(m)$ is called the m^{th} *Fourier coefficient* of ϕ , and these coefficients determine ϕ uniquely. There is a notion of cusp form [26, §3.1.1], and the space of Hilbert modular cusp forms of weight k and level N is denoted $S_k(K_0(N))$.

Fix a level N , and let m be an integral ideal of \mathcal{O}_F . Let $\hat{\mathcal{O}}_F$ be the closure of \mathcal{O}_F in \mathbf{A}_f . Define a subset of $M_2(\hat{\mathcal{O}}_F)$ by

$$H(m) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : (d, N) = \hat{\mathcal{O}}_F, c \in N\hat{\mathcal{O}}_F, (ad - bc)\hat{\mathcal{O}}_F = m\hat{\mathcal{O}}_F \right\},$$

and define the Hecke operator T_m acting on $S_k(K_0(N))$ by

$$(T_m \phi)(g) = N(m)^{k/2-1} \int_{H(m)} \phi(gh) dh$$

where dh is Haar measure on $\mathrm{GL}_2(\mathbf{A}_f)$ normalized so that $K_0(N)$ has measure 1. Let $\mathbb{T}_k(K_0(N))$ denote the \mathbf{Q} -subalgebra of $\mathrm{End}_{\mathbf{C}}(S_k(K_0(N)))$ generated by the T_m with m prime to N . The Fourier coefficients of $T_m \phi$ are given by

$$a_{T_m \phi}(n) = \sum_{a|(m,n)} N(a)^{k-1} a_\phi(mn/a^2),$$

and the Hecke operators satisfy the formal identity

$$\sum \frac{T_m}{m^s} = \prod_{\mathfrak{p}|N} (1 - T_{\mathfrak{p}} N(\mathfrak{p})^{-s})^{-1} \prod_{\mathfrak{p}/N} (1 - T_{\mathfrak{p}} N(\mathfrak{p})^{-s} + N(\mathfrak{p})^{1-2s})^{-1}.$$

If N_1 is a proper divisor of N , ϕ is a cusp form of level N_1 , and $d \in \mathrm{GL}_2(\mathbf{A}_f)$ is such that $d^{-1}K_0(N)d \subset K_0(N_1)$, then the function $\phi(gd)$ is a cusp form (of the same weight) of level N . The subspace of $S_k(K_0(N))$ generated by such functions as N_1 and d vary is called the space of *old forms*. The orthogonal complement of this subspace is denoted $S_k^{\mathrm{new}}(K_0(N))$. We say that $\phi \in S_k^{\mathrm{new}}(K_0(N))$ is a *newform* if $a_\phi(1) = 1$ and if ϕ is a simultaneous eigenform for all operators in $\mathbb{T}(K_0(N))$. If this is the case then the Fourier coefficients of ϕ are algebraic integers, and generate an order in a totally real number field. Furthermore, if $\sigma \in \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ is any automorphism, then the $a_\phi(m)^\sigma$ are the Fourier coefficients of another newform which we denote by ϕ^σ . By the strong multiplicity one theorem, if ϕ is a newform of level N then ϕ , a priori only an eigenform for T_m with $(m, N) = 1$, is in fact an eigenform for all T_m . Also ϕ is an eigenvector of the involution w_N defined by

$$(w_N\phi)(g) = \phi\left(g\begin{pmatrix} 0 & 1 \\ t & 0 \end{pmatrix}\right)$$

where $t \in \mathbf{A}$ is such that t_f , the projection of t to \mathbf{A}_f , generates $N\hat{\mathcal{O}}_F$ and has component -1 at the archimedean places. Let $\gamma \in \{\pm 1\}$ be such that $w_N\phi = \gamma\phi$. For ϕ of weight 2, the L -function of ϕ is defined by

$$\begin{aligned} L(s, \phi) &= \prod_{\ell|N} \frac{1}{1 - a_\phi(\ell)\mathbf{N}(\ell)^{-s}} \prod_{\ell \nmid N} \frac{1}{1 - a_\phi(\ell)\mathbf{N}(\ell)^{-s} + \mathbf{N}(\ell)^{1-2s}} \\ &= \sum_m \frac{a_\phi(m)}{\mathbf{N}(m)^s}. \end{aligned}$$

Let d_N denote the absolute norm of N . The completed L -function

$$L^*(s, \phi) = d_N^{s/2} d_F^s \left(\frac{\Gamma(s)}{(2\pi)^s} \right)^g L(s, \phi)$$

has analytic continuation and satisfies the functional equation

$$L^*(s, \phi) = \gamma L^*(2 - s, \phi).$$

1.2. Heegner points on Shimura curves. Let F be a totally real number field of degree g , $\xi : F \hookrightarrow \mathbf{R}$ a fixed embedding, and N an ideal of \mathcal{O}_F . Fix a CM-extension E/F whose relative discriminant, $D_{E/F}$, is prime to N , and let $\epsilon : F^\times \backslash \mathbf{A}^\times \rightarrow \{\pm 1\}$ be the quadratic character associated to E/F . We assume the *weak Heegner hypothesis* that $\epsilon(N) = (-1)^{g-1}$.

Let N_B be the squarefree product of primes $\mathfrak{P}|N$ which are inert in E and have $\mathrm{ord}_{\mathfrak{P}}(N)$ odd, and fix an integral ideal N_E of E with relative norm N/N_B . Since $\epsilon(N_B) = \epsilon(N) = (-1)^{g-1}$, there is a unique quaternion algebra B/F which is ramified exactly at the prime divisors of N_B and the archimedean primes other than ξ . Fix an isomorphism

$$B \otimes_{\mathbf{Q}} \mathbf{R} \cong M_2(F_\xi) \oplus \mathbf{H}^{g-1}$$

where \mathbf{H} denotes the real quaternions. The group of units B^\times can be given the structure of the set of rational points of a reductive algebraic group G over F , $G(F) \cong B^\times$, and the projection

$$G(\mathbf{A}_\infty) \cong (B \otimes_{\mathbf{Q}} \mathbf{R})^\times \rightarrow \mathrm{GL}_2(F_\xi)$$

defines an action of $G(\mathbf{A}_\infty)$ (and so also of B^\times) on \mathfrak{H}^\pm . We let U_∞ be the stabilizer of i and identify

$$\mathfrak{H}^\pm \cong G(\mathbf{A}_\infty)/U_\infty.$$

The projection $G(\mathbf{A}_\infty) \rightarrow \mathfrak{H}^\pm$ admits a smooth section s defined by

$$(1) \quad s(x + iy) = \left(\left(\begin{array}{cc} y & x \\ 0 & 1 \end{array} \right), 1, \dots, 1 \right).$$

At every place at which B is ramified $E \otimes_F F_v$ is a field, and so there exists an embedding $q : E \rightarrow B$. There is a unique point $w(q) \in \mathfrak{H}$ which is fixed by $q(\alpha)$ for every $\alpha \in E^\times$. The embedding q and its conjugate embedding share the same fixed point, and exactly one of them is *normalized* in the sense that

$$q(\alpha) \begin{bmatrix} w(q) \\ 1 \end{bmatrix} = \alpha \begin{bmatrix} w(q) \\ 1 \end{bmatrix}$$

where $q(\alpha)$ is viewed as an element of $GL_2(\mathbf{R})$ on the left hand side, and α is a scalar multiplier on the right hand side. We assume that q is the normalized choice.

Let \mathcal{O}_B be a maximal order of B containing $q(\mathcal{O}_E)$ and define an order R of reduced discriminant N by

$$R = q(\mathcal{O}_E) + q(N_E)\mathcal{O}_B.$$

Let $U \subset G(\mathbf{A}_f)$ be image of \hat{R}^\times under the isomorphism $\hat{B}^\times \cong G(\mathbf{A}_f)$, and let Z be the center of G , so that $Z(\mathbf{A}_f) \cong \hat{F}^\times$. Define the complex curve $X(\mathbf{C})$ to be the quotient

$$\begin{aligned} X(\mathbf{C}) &= G(F) \backslash \mathfrak{H}^\pm \times G(\mathbf{A}_f) / Z(\mathbf{A}_f)U \cup \{\text{cusps}\} \\ &= G(F) \backslash G(\mathbf{A}) / Z(\mathbf{A})UU_\infty \cup \{\text{cusps}\}. \end{aligned}$$

This is a compact and possibly disconnected Riemann surface. The set of cusps is nonempty only when $F = \mathbf{Q}$ and $B = M_2(\mathbf{Q})$. If $F = \mathbf{Q}$ and every prime divisor of N splits in E , then $X(\mathbf{C})$ is none other than the classical level N modular curve $X_0(N)$.

If $(z, g) \in \mathfrak{H} \times G(\mathbf{A}_f)$, we write $[(z, g)]$ for the class of (z, g) in $X(\mathbf{C})$. The normalizer of U in $G(\mathbf{A}_f)$ acts on $X(\mathbf{C})$ by $\alpha \cdot [(z, g)] = [(z, g\alpha^{-1})]$. In Shimura's language, this is the automorphism $J(\alpha) = J_{UU}(\alpha)$. Let $\pi_0(X(\mathbf{C}))$ denote the set of connected components of $X(\mathbf{C})$. The reduced norm $\nu : G(\mathbf{A}) \rightarrow \mathbf{A}^\times$ induces a bijection

$$\pi_0(X(\mathbf{C})) \cong F^\times \backslash \mathbf{A}^\times / \nu(Z(\mathbf{A})UU_\infty).$$

If F_X is the abelian extension of F with

$$\text{Gal}(F_X/F) \cong F^\times \backslash \mathbf{A}^\times / \nu(Z(\mathbf{A})UU_\infty)$$

via the Artin symbol, we let $\sigma : G(\mathbf{A}_f) \rightarrow \text{Gal}(F_X/F)$ be the map taking $\alpha \mapsto \nu(\alpha)^{-1}$. It is easily checked that $\nu(U) = \hat{\mathcal{O}}_F^\times$, and so F_X is a subfield of the narrow Hilbert class field of F . We define an action of $\text{Gal}(F_X/F)$ on $\pi_0(X(\mathbf{C}))$ by the commutativity of

$$(2) \quad \begin{array}{ccc} X(\mathbf{C}) & \xrightarrow{J(\alpha)} & X(\mathbf{C}) \\ \downarrow \nu & & \downarrow \nu \\ \pi_0(X(\mathbf{C})) & \xrightarrow{\sigma(\alpha)} & \pi_0(X(\mathbf{C})). \end{array}$$

Let m be an integral ideal of F which is prime to N . At every prime $\ell|m$ the algebra B is split, and the component of U is a maximal compact open subgroup of $G(F_\ell)$. Let $\Delta(m)$ (resp. $\Delta(1)$) be the set of elements of $\hat{\mathcal{O}}_B$ with component 1 away from m , and whose determinant generates m (resp. is a unit) at every prime divisor of m . We define a correspondence T_m on $X(\mathbf{C})$ by

$$(3) \quad T_m \cdot [(z, g)] = \sum_{\Delta(m)/\Delta(1)} [(z, g\gamma)]$$

as a divisor on $X(\mathbf{C})$.

We let $T \subset G$ be the torus defined by $q(E^\times) = T(F)$, and let $w(q)$ denote the unique fixed point of $T(F)$ in \mathfrak{H} . Define

$$\text{CM}_E = T(F) \backslash G(\mathbf{A}_f) / Z(\mathbf{A}_f),$$

the set of CM-points by E . We map CM_E to $X(\mathbf{C})$ via $g \mapsto (w(q), g)$ and call the image the CM-points of $X(\mathbf{C})$. Define an action of $\text{Gal}(E^{\text{ab}}/E)$ on the CM-points by

$$(4) \quad [(w(q), g)]^{[s, E]} = [(w(q), s \cdot g)] \quad \forall s \in T(\mathbf{A}_f)$$

where $[\cdot, E] : T(F) \backslash T(\mathbf{A}_f) \cong \text{Gal}(E^{\text{ab}}/E)$ is the Artin symbol. In particular note that $Z(\mathbf{A}_f) \cong \mathbf{A}_f^\times$ acts trivially on all CM points.

If x is a CM-point represented by $(w(q), g) \in \mathfrak{H} \times G(\mathbf{A}_f)$, we define the endomorphism ring of x to be the preimage of \hat{R} under the map $g^{-1}qg : E \rightarrow \hat{B}$. It is an order of E of the form $\mathcal{O}_c = \mathcal{O}_F + c\mathcal{O}_E$ for some integral ideal $c \subset \mathcal{O}_F$ called the *conductor* of x . Let

$$T[c] = q(\hat{\mathcal{O}}_c^\times) \subset T(\mathbf{A}_f).$$

The abelian extension of E associated to $T[c]Z(\mathbf{A}_f)$ by class field theory is called the *ring class field* of conductor c and is denoted $E[c]$. It is Galois over F , and is the natural field of definition of x .

We want to give an explicit construction of some CM-points of various conductors. Let ℓ be a prime of F not dividing $D_{E/F}N$, and fix an isomorphism $B_\ell \cong M_2(F_\ell)$ in such a way that R_ℓ is identified with $M_2(\mathcal{O}_{F,\ell})$, and so that

$$q(\mathcal{O}_{E,\ell}) = \left\{ \begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix} : x, y \in \mathcal{O}_{F,\ell} \right\}$$

in the case where ℓ splits in E , or

$$q(\mathcal{O}_{E,\ell}) = \left\{ \begin{pmatrix} x & yu \\ y & x \end{pmatrix} : x, y \in \mathcal{O}_{F,\ell} \right\}$$

for some $u \in \mathcal{O}_{F,\ell}^\times$ not a square, in the case where ℓ is inert in E . Fix a uniformizer ϖ of F_ℓ , and let $h[\ell^k]$ be the element of B_ℓ such that

$$h[\ell^k] \mapsto \begin{cases} \begin{pmatrix} \varpi^k & 1 \\ & 1 \end{pmatrix} & \text{if } \ell \text{ splits in } E \\ \begin{pmatrix} \varpi^k & \\ & 1 \end{pmatrix} & \text{if } \ell \text{ inert in } E \end{cases}$$

under the above isomorphism. View $h[\ell^k]$ as an element of $G(\mathbf{A}_f)$ with trivial components away from ℓ , and extend h multiplicatively to a map on all integral ideals prime to $D_{E/F}N$.

Direct calculation yields the following properties of the points $h[m]$:

Proposition 1.2.1. *There is a collection of CM-points of $h[m] \in X(\mathbf{C})$, where m runs over all positive integers prime to $D_{E/F}N$, such that $h[m]$ has conductor m and such that*

$$\begin{aligned} & [\mathcal{O}_m^\times : \mathcal{O}_{m\ell}^\times] \cdot \text{Norm}_{E[m\ell]/E[m]}(h[m\ell]) \\ &= \begin{cases} T_\ell(h[m]) & \text{if } \ell \nmid m \text{ and is inert in } E \\ T_\ell(h[m]) - h[m]^{\sigma_\ell} - h[m]^{\sigma_\ell^*} & \text{if } \ell \nmid m \text{ and is split in } E \\ T_\ell(h[m]) - h[m/\ell] & \text{if } \ell \mid m \end{cases} \end{aligned}$$

as divisors on $X(\mathbf{C})$, where σ_ℓ and σ_ℓ^* are the Frobenius automorphisms of the primes of E above ℓ .

The existence of a canonical model for the complex curve $X(\mathbf{C})$ is due to Shimura:

Theorem 1.2.2. *There is a smooth projective variety X , defined and connected over F , whose complex points are isomorphic to $X(\mathbf{C})$ as a Riemann surface. The action of $\text{Gal}(\bar{F}/F)$ on the geometric components factors through $\text{Gal}(F_X/F)$ and agrees with the action determined by (2). If $x \in X(\mathbf{C})$ is a CM-point then x is defined over E^{ab} and the action of $\text{Gal}(E^{\text{ab}}/E)$ agrees with the action (4).*

Proof. This is Theorem 9.6 of [22]. \square

1.3. Abelian varieties associated to newforms. Fix an integral ideal $N \subset \mathcal{O}_F$, and assume that either $[F : \mathbf{Q}]$ is odd or that $\text{ord}_v(N)$ is odd for some finite prime v of F . Then we may fix a CM extension E/F of relative discriminant $D_{E/F}$ which satisfies the weak Heegner hypothesis $\epsilon(N) = (-1)^{g-1}$, where ϵ is the quadratic character associated to E/F . Abbreviate $\mathbb{T} = \mathbb{T}_2(K_0(N))$. If ϕ is a Hilbert modular newform of weight 2 and level N on \mathbf{A} , we let $\alpha_\phi : \mathbb{T} \rightarrow \mathbf{C}$ be the character giving the action of \mathbb{T} on $\mathbf{C} \cdot \phi$. We denote by F_ϕ the totally real field generated by $\alpha_\phi(T_m)$ with $(m, N) = 1$.

Let X be the canonical model over F of the complex curve $X(\mathbf{C})$ described in Section 1.2. The curve X splits into its geometric components over the field F_X defined in the previous section, i.e. $X \times_F F_X = \coprod X_i$ with each X_i geometrically irreducible, and any extension L/F for which $X(L) \neq \emptyset$ must contain F_X . Define J_X to be the abelian variety over F obtained by the restriction of scalars of $\text{Jac}(X_0)$ (for some fixed component X_0) from F_X to F . Then J_X has good reduction away from N , and for any algebraic extension L/F with $X(L) \neq \emptyset$,

$$J_X(L) = \prod_i \text{Jac}(X_i)(L) = \prod_i \text{Pic}^0(X_i \times_{F_X} L).$$

We denote by \mathbb{T}_X the \mathbf{Q} -algebra generated by the Hecke correspondences (3) acting on J_X .

By the Jacquet-Langlands correspondence, for every algebra homomorphism $\alpha : \mathbb{T}_X \rightarrow \mathbf{C}$ there exists a weight 2 level N newform ϕ such that (slightly abusing notation) $\alpha(T_m) = \alpha_\phi(T_m)$. This associates to every maximal ideal of \mathbb{T}_X a unique Galois conjugacy class of newforms and also gives a surjective algebra map $\mathbb{T} \rightarrow \mathbb{T}_X$, thus endowing the Lie algebra of J_X with an action of \mathbb{T} .

Theorem 1.3.1. (Zhang) *There is an isogeny $J_X \xrightarrow{\sim} \bigoplus_\phi A_\phi$ such that the induced map on Lie algebras is \mathbb{T} -equivariant, where the sum is over all Galois conjugacy classes of newforms of weight 2 and level dividing N . If ϕ is new of level N , the*

Lie algebra of A_ϕ is free of rank one over $F_\phi \otimes_{\mathbf{Q}} \mathbf{C}$. Furthermore, for each ϕ there is an equality of L -functions

$$L_N(s, A_\phi) = \prod_{\sigma: F_\phi \hookrightarrow \mathbf{C}} L_N(s, \phi^\sigma)$$

where the subscript N indicates that the Euler factors at primes dividing N have been removed.

Fix a newform ϕ . In order to obtain Heegner points on A_ϕ it suffices to exhibit embedding $X \rightarrow J_X$ which is defined over F and is compatible with the action of the Hecke operators. Since the curve X typically has no cusps, there is no natural choice of F -rational point on X to provide such an embedding. Instead, one uses the *Hodge class* $\xi \in \text{Pic}(X)$: the unique (up to constant multiple) class whose degree is constant on each geometric component and which satisfies

$$T_m \xi = \deg(T_m) \xi$$

for every Hecke correspondence with m prime to $D_{E/F}N$. In the absence of cusps and elliptic fixed points, the Hodge class is simply the canonical divisor on each geometric component. Write $X(\mathbf{C}) = \cup_i X_i(\mathbf{C})$ as a disjoint union of connected components, and let ξ_i be the restriction of $\xi \in \text{Pic}(X(\mathbf{C}))$ to the i^{th} component. Denote by d the degree of ξ_i . There is a unique morphism $X \rightarrow J_X$, defined over F , which on complex points takes $p_i \in X_i(\mathbf{C})$ to the divisor $dp_i - \xi_i \in J_X(\mathbf{C})$.

Applying the composition $X \rightarrow J_X \rightarrow A_\phi$ to the Heegner points described in the previous section yields the following.

Proposition 1.3.2. *There is a family of points $h[m] \in A_\phi(E^{\text{ab}})$, where m runs over all positive integers prime to $D_{E/F}N$, such that $h[m]$ is defined over $E[m]$, and*

$$\begin{aligned} & [\mathcal{O}_m^\times : \mathcal{O}_{m\ell}^\times] \cdot \text{Norm}_{E[m\ell]/E[m]}(h[m\ell]) \\ &= \begin{cases} a_\phi(\ell)h[m] & \text{if } \ell \nmid m \text{ and is inert in } E \\ a_\phi(\ell)h[m] - h[m]^{\sigma_\ell} - h[m]^{\sigma_{\bar{\ell}}} & \text{if } \ell \nmid m \text{ and is split in } E \\ a_\phi(\ell)h[m] - h[m/\ell] & \text{if } \ell \mid m \end{cases} \end{aligned}$$

Theorem 1.3.3. *(Zhang) Let $L(s, \phi, E) = L(s, \phi)L(s, \epsilon, \phi)$. Then $L(s, \phi, E)$ has analytic continuation and a functional equation equation in $s \mapsto 2 - s$ with sign $\epsilon(N)(-1)^{g-1} = -1$. In particular $L(s, \phi, E)$ vanishes at $s = 1$. Assume that a prime \mathfrak{p} of F is split in E if either \mathfrak{p} divides 2 or $\text{ord}_{\mathfrak{p}}(N) > 1$. Then*

$$L'(1, \phi, E) \neq 0 \iff \text{Norm}_{E[1]/E}(h[1]) \text{ has infinite order.}$$

Proof. This is Theorem C of [26]. □

One expects that the requirement that \mathfrak{p} splits when $\text{ord}_{\mathfrak{p}}(N) > 1$ is unnecessary.

2. BOUNDING THE SELMER GROUP

In Section 2 we prove Theorem A. The Heegner points having been constructed, the remainder of the proof is essentially identical to arguments of [9], and makes fundamental use of the observation of [13] that Kolyvagin's derivative classes κ_m satisfy certain ‘‘transverse’’ local conditions at primes dividing m .

Throughout Section 2 we work with a fixed CM field E , and denote by F its maximal real subfield. Fix a complex conjugation $\tau \in G_F$ and a rational prime p which does not divide 2, the class number of E , or the index $[\mathcal{O}_E^\times : \mathcal{O}_F^\times]$.

2.1. Kolyvagin systems. In preparation for the Iwasawa theory of Section 3, we work in greater generality than is need for the proof of Theorem A. By a coefficient ring we mean a complete, Noetherian, local ring with finite residue field of characteristic p . Let R be such a ring, and suppose that T is any topological R -module equipped with a continuous R -linear action of G_E , unramified outside a finite set of primes.

Definition 2.1.1. A *Selmer structure* on T is a pair (\mathcal{F}, Σ) where Σ is a finite set of places of E containing the archimedean places, the primes at which T is ramified, and all primes above p ; and \mathcal{F} is a collection of *local conditions* at the places of Σ . That is, for each $v \in \Sigma$ we have a choice of R -submodule

$$H_{\mathcal{F}}^1(E_v, T) \subset H^1(E_v, T).$$

If E^Σ denotes the maximal extension of E unramified outside of Σ , then we define the *Selmer module* $H_{\mathcal{F}}^1(E, T)$ to be the kernel of the localization

$$H^1(E^\Sigma/E, T) \xrightarrow{\oplus \text{loc}_v} \bigoplus_{v \in \Sigma} H^1(E_v, T)/H_{\mathcal{F}}^1(E_v, T).$$

Remark 2.1.2. Equivalently, one may define a Selmer structure to be a family of local conditions $H_{\mathcal{F}}^1(E_v, T) \subset H^1(E_v, T)$, one for *every* place v , such that almost all local conditions are equal to the unramified condition. We usually take this point of view, so that the set Σ does not need to be specified.

Remark 2.1.3. Since E is totally complex, $H^1(E_v, T) = 0$ at every archimedean place v .

If S is a submodule (resp. quotient) of T then a Selmer structure on T induces a Selmer structure on S by taking the preimages (resp. images) of the local conditions on T under the natural maps on local cohomology. We refer to this as *propagation* of Selmer structures.

The most important example of a local condition is the *unramified* condition: let v be a finite place of E , and denote by E_v^{unr} the maximal unramified extension of E_v . The unramified condition $H_{\text{unr}}^1(E_v, T)$ is defined as the kernel of restriction

$$H^1(E_v, T) \rightarrow H^1(E_v^{\text{unr}}, T).$$

For the remainder of this section we fix a Selmer structure (\mathcal{F}, Σ) on T , and assume that T is finitely generated over R .

Definition 2.1.4. A prime ideal ℓ of \mathcal{O}_F is *k-admissible* if it satisfies

- (a) ℓ does not divide $D_{E/F}$, is inert in E , and is not in Σ ,
- (b) $\mathbf{N}(\ell) + 1 \equiv 0 \pmod{p^k}$,
- (c) the Frobenius of the prime of E above ℓ acts trivially on $T/p^k T$.

A 1-admissible prime will simply be called *admissible*.

We will routinely confuse an admissible prime of F with the unique prime of E above it. To avoid confusion, the Frobenius of the unique prime of E above an admissible ℓ will be denoted $\text{Fr}_E(\ell)$. The set of k -admissible primes is denoted \mathcal{L}_k , and \mathcal{M}_k denotes the set of squarefree products of primes of \mathcal{L}_k . If ℓ is admissible let $G(\ell)$ be the p -Sylow subgroup of the cokernel of

$$(\mathcal{O}_F/\ell\mathcal{O}_F)^\times \rightarrow (\mathcal{O}_E/\ell\mathcal{O}_E)^\times.$$

This is a cyclic group of order equal to the maximal power of p dividing $\mathbf{N}(\ell) + 1$, and is the same as the p -Sylow subgroup of $(\mathcal{O}_E/\ell\mathcal{O}_E)^\times$, since we assume that p does not divide $\mathbf{N}(\ell) - 1$. For any $m \in \mathcal{M}_1$, let $E(m)$ be the p -ring class field of conductor m , i.e. the maximal p -power subextension of $E[m]/E$, and note that $E(1) = E$ since we assume that p does not divide the class number of E .

Lemma 2.1.5. *For any $m \in \mathcal{M}_1$,*

(a) *there is a canonical isomorphism*

$$G(m) \stackrel{\text{def}}{=} \text{Gal}(E(m)/E) \cong \prod_{\ell|m} G(\ell)$$

- (b) *if ℓ is a prime of F not dividing $mD_{E/F}$ which is inert in E (in particular if ℓ is admissible and prime to m), then the unique prime of E above ℓ splits completely in $E(m)$,*
- (c) *if ℓ is a prime divisor of m and λ is a prime of $E(m)$ above ℓ , then $E(m)_\lambda$ is a totally tamely ramified abelian p -extension of E_ℓ , and is a maximal such extension,*
- (d) *$\text{Gal}(E(m)/F)$ is a generalized dihedral group: for any $\sigma \in \text{Gal}(E(m)/E)$ and any complex conjugation $\tau \in \text{Gal}(E(m)/F)$, one has $\tau\sigma\tau = \sigma^{-1}$.*

Proof. Elementary class field theory. \square

Definition 2.1.6. Let $\ell \in \mathcal{L}_1$, and let λ be the unique prime of $E(\ell)$ above ℓ . We define the *transverse* local condition at ℓ , $H_{\text{tr}}^1(E_\ell, T)$, to be the kernel of restriction

$$H^1(E_\ell, T) \rightarrow H^1(E(\ell)_\lambda, T).$$

If \mathcal{F} is any Selmer structure on T and $m \in \mathcal{M}_1$, we define a new Selmer structure $\mathcal{F}(m)$ on T by

$$H_{\mathcal{F}(m)}^1(E_\ell, T) = \begin{cases} H_{\text{tr}}^1(E_\ell, T) & \text{if } \ell \mid m \\ H_{\mathcal{F}}^1(E_\ell, T) & \text{else.} \end{cases}$$

In practice, we only define the transverse condition when T is annihilated by $|G(\ell)|$ and $\text{Fr}_E(\ell) - 1$. Accordingly, for any admissible ℓ , we let $I_\ell = p^k R$ where k is the largest integer for which ℓ is k -admissible. If $m \in \mathcal{M}_1$ set

$$I_m = \sum_{\ell|m} I_\ell \quad \Delta_m = \bigotimes_{\ell|m} G(\ell)$$

so that $T/I_m T$ is annihilated both by $|G(\ell)|$ and by $\text{Fr}_E(\ell) - 1$ for any ℓ dividing m . By Lemma 1.2.4 of [13], if $\ell \in \mathcal{L}_1$ and $I \subset R$ is any ideal containing I_ℓ , there is a decomposition

$$H^1(E_\ell, T/IT) \cong H_{\text{unr}}^1(E_\ell, T/IT) \oplus H_{\text{tr}}^1(E_\ell, T/IT).$$

Furthermore, Lemma 1.2.1 of [13] gives canonical isomorphisms

$$H_{\text{unr}}^1(E_\ell, T/IT) \cong T/IT \quad H_{\text{tr}}^1(E_\ell, T/IT) \otimes G(\ell) \cong T/IT,$$

both of which are given by evaluation of cocycles: the first is evaluation at the Frobenius automorphism, and the second sends $c \otimes \sigma_\ell \mapsto c(\sigma_\ell)$ where σ_ℓ is a generator of Δ_ℓ . If $\ell \in \mathcal{L}_1$ and I contains I_ℓ , we define the *edge map* (or finite-singular comparison map) at ℓ to be the isomorphism

$$e_\ell : H_{\text{unr}}^1(E_\ell, T/IT) \cong T/IT \cong H_{\text{tr}}^1(E_\ell, T/IT) \otimes G(\ell).$$

For every $m\ell \in \mathcal{M}_1$, consider the maps

$$(5) \quad \begin{array}{ccc} H_{\mathcal{F}(m)}^1(E, T/I_m T) \otimes \Delta_m & & \\ & \downarrow \text{loc}_\ell & \\ & H_{\text{unr}}^1(E_\ell, T/I_{m\ell} T) \otimes \Delta_m & \\ & \downarrow e_{m,\ell} \otimes 1 & \\ H_{\mathcal{F}(m\ell)}^1(E, T/I_{m\ell} T) \otimes \Delta_{m\ell} & \xrightarrow{\text{loc}_\ell} & H_{\text{tr}}^1(E_\ell, T/I_{m\ell} T) \otimes \Delta_{m\ell}. \end{array}$$

Definition 2.1.7. Let $\mathcal{L} \subset \mathcal{L}_1$, and denote by \mathcal{M} the set of squarefree products of primes in \mathcal{L} . We define a *Kolyvagin system* κ for $(T, \mathcal{F}, \mathcal{L})$ to be a collection of cohomology classes

$$\kappa_m \in H_{\mathcal{F}(m)}^1(E, T/I_m T) \otimes \Delta_m$$

one for each $m \in \mathcal{M}$, such that for any $m\ell \in \mathcal{M}$ the images of κ_m and $\kappa_{m\ell}$ in $H_{\text{tr}}^1(E_\ell, T/I_{m\ell} T) \otimes \Delta_{m\ell}$ under the maps of (5) agree. We denote the R -module of all Kolyvagin systems for $(T, \mathcal{F}, \mathcal{L})$ by $\mathbf{KS}(T, \mathcal{F}, \mathcal{L})$.

2.2. The main bound. Let S be the ring of integers of a finite extension Φ/\mathbf{Q}_p , and let T be a free S -module of rank 2 equipped with a continuous S -linear action of G_E . Let Σ be a finite set of primes of E containing the infinite places, the primes above p , and all primes at which T is ramified. Let \mathfrak{m} be the maximal ideal of S , and fix a uniformizer $\pi \in \mathfrak{m}$. We set $\mathcal{D} = \Phi/S$, $V = T \otimes_S \Phi$, $W = V/T$.

Fix a Selmer structure (\mathcal{F}, Σ) on V , and propagate this to Selmer structures, still denoted \mathcal{F} , on T and W . The fact that the Selmer structure on T is propagated from V implies that the local conditions $H_{\mathcal{F}}^1(E_v, T)$ are *cartesian* on the category of quotients of T (see Definition 1.1.4 and Lemma 3.7.1 of [13]). Consequently, the isomorphism $T/\mathfrak{m}^k \cong W[\mathfrak{m}^k]$ identifies the Selmer structure on T/\mathfrak{m}^k propagated from T with the Selmer structure on $W[\mathfrak{m}^k]$ propagated from W .

We assume throughout this section that the module T satisfies the following hypotheses:

- H1:** there is an extension L/E which is Galois over F , such that G_L acts trivially on T and $H^1(L(\mu_{p^\infty})/E, T/\mathfrak{m}T) = 0$,
- H2:** $T/\mathfrak{m}T$ is an absolutely irreducible representation of $(S/\mathfrak{m})[[G_E]]$, and the action of G_E extends to an action of G_F . Furthermore, the action of τ splits $T/\mathfrak{m}T$ into two one-dimensional eigenspaces,
- H3:** there is a perfect, symmetric, S -bilinear pairing

$$(\ , \) : T \times T \rightarrow S(1)$$

such that $(a^\sigma, b^{\tau\sigma\tau}) = (a, b)^\sigma$ for all $a, b \in T$ and $\sigma \in G_E$. The induced pairing $T/\mathfrak{m}T \times T/\mathfrak{m}T \rightarrow (S/\mathfrak{m})(1)$ on the residual representation satisfies $(a^\tau, b^\tau) = (a, b)^\tau$,

The pairing of **H3** can be thought of as a G_E -equivariant pairing $T \times \text{Tw}(T) \rightarrow S(1)$ where $\text{Tw}(T)$ is the Galois module whose underlying S -module is T , but on which G_E acts through the automorphism $\sigma \mapsto \tau\sigma\tau$. This automorphism, together with the map $T \rightarrow \text{Tw}(T)$ which is the identity on underlying S -modules, induces a “change of group” $(G_E, T) \rightarrow (G_E, \text{Tw}(T))$, and hence an isomorphism

$$H^i(E, T) \cong H^i(E, \text{Tw}(T)).$$

At every prime v of E , there is a similar isomorphism $H^i(E_{v\tau}, T) \cong H^i(E_v, \text{Tw}(T))$, and similar remarks hold with T replaced by W or V . Tate local duality therefore gives perfect pairings

$$(6) \quad \begin{aligned} H^1(E_v, T) \times H^1(E_{v\tau}, W) &\rightarrow \mathcal{D} \\ H^1(E_v, V) \times H^1(E_{v\tau}, V) &\rightarrow \Phi \end{aligned}$$

at every place v . We assume that the Selmer structure \mathcal{F} on T satisfies

H4: at every place v , the local conditions $H_{\mathcal{F}}^1(E_v, V)$ and $H_{\mathcal{F}}^1(E_{v\tau}, V)$ are exact orthogonal complements under the pairing (6),

H5: at every place v of F , the module $\oplus_{w|v} H_{\mathcal{F}}^1(E_w, T/\mathfrak{m}T)$ is stable under the action of $\text{Gal}(E/F)$.

Proposition 2.2.1. *There is an integer r and a finite S -module M such that*

$$H_{\mathcal{F}}^1(E, W) \cong \mathcal{D}^r \oplus M \oplus M.$$

Proof. Define a Selmer structure \mathcal{F} on $\text{Tw}(W)$ by identifying

$$H^1(E_{v\tau}, W) \cong H^1(E_v, \text{Tw}(W))$$

everywhere locally. By the main result of [6], there is a generalized Cassels pairing

$$H_{\mathcal{F}}^1(E, W) \times H_{\mathcal{F}}^1(E, \text{Tw}(W)) \rightarrow \mathcal{D}$$

whose kernels on the left and right are exactly the submodules of S -divisible elements. The global change of group isomorphism identifies $H_{\mathcal{F}}^1(E, W)$ with $H_{\mathcal{F}}^1(E, \text{Tw}(W))$, and under this identification the pairing above yields a pairing

$$H_{\mathcal{F}}^1(E, W) \times H_{\mathcal{F}}^1(E, W) \rightarrow \mathcal{D}.$$

A straightforward (if tedious) modification of the methods of [6] shows that the resulting pairing is alternating; a similar calculation is done in Theorem 1.4.3 of [9]. \square

Theorem 2.2.2. *Suppose we have a set of primes $\mathcal{L} \subset \mathcal{L}_1$ with $\mathcal{L}_e \subset \mathcal{L}$ for $e \gg 0$. Let \mathcal{M} denote the set of squarefree products of primes in \mathcal{L} . Suppose that there is a collection of cohomology classes*

$$\{\kappa_m \in H^1(E, T/I_m T) \otimes \Delta_m \mid m \in \mathcal{M}\}$$

such that $\kappa_1 \neq 0$ and there exists an integer $d \geq 0$, independent of m , such that the family $p^d \kappa_m$ is a Kolyvagin system for $(T, \mathcal{F}, \mathcal{L})$. Then $\kappa_1 \in H_{\mathcal{F}}^1(E, T)$ and $H_{\mathcal{F}}^1(E, T)$ is free of rank one over S . Furthermore, there is an isomorphism

$$H_{\mathcal{F}}^1(E, W) \cong \mathcal{D} \oplus M \oplus M$$

with $\text{length}_S(M) \leq \text{length}_S(H_{\mathcal{F}}^1(E, T)/S \cdot \kappa_1)$.

Proof. The case $F = \mathbf{Q}$ and $d = 0$ is Theorem 1.6.1 of [9]. The only nontrivial modifications needed are to deal with $d > 0$, and these are essentially contained in the proof of Corollary 4.6.5 of [20].

Fix some integer e large enough that κ_1 has nontrivial image in $H^1(E, T/IT)$, where $I = p^e S$, and such that $\tilde{\mathcal{L}} \stackrel{\text{def}}{=} \mathcal{L}_{e+d}$ is contained in \mathcal{L} . Let $\tilde{\kappa}_m$ denote the image of κ_m in $H^1(E, T/IT) \otimes \Delta_m$. The claim is that the family $\tilde{\kappa}_m$ is a Kolyvagin system for $(T/IT, \mathcal{F}, \tilde{\mathcal{L}})$ (over the ring S/I). Let $\tilde{\mathcal{M}}$ denote the set of squarefree products of primes in $\tilde{\mathcal{L}}$. We must show that if $m \in \tilde{\mathcal{M}}$ then $\tilde{\kappa}_m$ lies in $H_{\mathcal{F}(m)}^1(E, T/IT) \otimes \Delta_m$. If $m = 1$ this follows from the fact that $H^1(E, T)/H_{\mathcal{F}}^1(E, T)$ is torsion free (as the

Selmer structure \mathcal{F} was assumed to be propagated from a Selmer structure on V and the hypothesis that $p^d \kappa_1 \in H_{\mathcal{F}}^1(E, T)$. If $m \neq 1$ then I_m is generated by (say) p^k with $e + d \leq k$. Set $I' = p^{e+d} S \supset I_m$. Multiplication by p^d on T induces a map

$$(7) \quad H^1(E, T/IT) \otimes \Delta_m \rightarrow H^1(E, T/I'T) \otimes \Delta_m$$

taking $\tilde{\kappa}_m$ to the image of $p^d \kappa_m$ modulo I' , and this image lies in $H_{\mathcal{F}(m)}^1(E, T/I'T) \otimes \Delta_m$ by hypothesis. By the cartesian property of $\mathcal{F}(m)$ (see the remarks at the beginning of this subsection and Lemma 3.7.4 of [13]) it follows that

$$\tilde{\kappa}_m \in H_{\mathcal{F}(m)}^1(E, T/IT) \otimes \Delta_m.$$

It is easily seen that the maps on local cohomology analogous to (7) are compatible with the edge maps of Section 2.1 and so the classes $\tilde{\kappa}_m$ form a Kolyvagin system.

The remainder of the proof is now [9] Theorem 1.6.1 almost verbatim. For every $m \in \tilde{\mathcal{M}}$ one has a (noncanonical) decomposition

$$H_{\mathcal{F}(m)}^1(E, W)[I] \cong H_{\mathcal{F}(m)}^1(E, T/IT) \cong (S/I)^\epsilon \oplus M_m \oplus M_m$$

where $\epsilon \in \{0, 1\}$ is independent of m , and the first isomorphism is given by [13] Lemma 3.5.3. For $m \in \tilde{\mathcal{M}}$, we define the *stub Selmer module* at m to be

$$\text{Stub}(m) = \mathfrak{m}^{\text{length}_S(M_m)} \cdot H_{\mathcal{F}(m)}^1(E, T/IT) \otimes \Delta_m.$$

By further shrinking $\tilde{\mathcal{L}}$ we may assume that $\tilde{\mathcal{L}} \subset \mathcal{L}_{2e+d}$, and the key point is that for every $m \in \tilde{\mathcal{M}}$ the class $\tilde{\kappa}_m$ belongs to the stub Selmer module at m . In particular, $\text{Stub}(1)$ is nonzero and M_1 has length strictly less than that of S/I . This implies that $\epsilon = 1$ and that the module M of the statement of the theorem is finite. Furthermore, the image of κ_1 in $H_{\mathcal{F}}^1(E, T/IT)$ actually lies in $\mathfrak{m}^{\text{length}_S(M_1)} H_{\mathcal{F}}^1(E, T/IT)$. Taking limits as $e \rightarrow \infty$ shows that $\kappa_1 \in \mathfrak{m}^{\text{length}_S(M)} H_{\mathcal{F}}^1(E, T)$. \square

2.3. Application to Heegner points. Now let N be an integral ideal of F , and let A/F be an abelian variety associated to a Hilbert modular form, ϕ , of level N . Fix an embedding $\mathcal{O} \hookrightarrow \text{End}_F(A)$ for some order \mathcal{O} of F_ϕ , and an \mathcal{O} -linear polarization of A . Fix a prime \mathfrak{P} of the ring of integers of F_ϕ , let p be the rational prime below \mathfrak{P} , and assume that conditions (1) and (2) of the introduction hold. Denote by $\mathcal{O}_{\mathfrak{P}}$ the completion of \mathcal{O} at \mathfrak{P} , let $\Phi_{\mathfrak{P}}$ be the field of fractions of $\mathcal{O}_{\mathfrak{P}}$, and set $\mathcal{D}_{\mathfrak{P}} = \Phi_{\mathfrak{P}}/\mathcal{O}_{\mathfrak{P}}$. We let Σ be any finite set of places of E containing the archimedean places, the primes above p , and the divisors of $N\mathcal{O}_E$. Let $T = T_{\mathfrak{P}}(A)$, $V = T \otimes_{\mathcal{O}_{\mathfrak{P}}} \Phi_{\mathfrak{P}}$, and $W = V/T \cong A[\mathfrak{P}^\infty]$. For any ideal m of \mathcal{O}_F we abbreviate $a_m = a_\phi(m) \in \mathcal{O}_{\mathfrak{P}}$.

Our choice of polarization of A gives a perfect, skew-symmetric, G_F -equivariant pairing

$$(8) \quad T_{\mathfrak{P}}(A) \times T_{\mathfrak{P}}(A) \rightarrow \mathbf{Z}_p(1)$$

under which the action of $\mathcal{O}_{\mathfrak{P}}$ is self-adjoint.

Lemma 2.3.1. *Let $\text{Tr} : \mathcal{O}_{\mathfrak{P}}(1) \rightarrow \mathbf{Z}_p(1)$ be the map induced by the trace from $\mathcal{O}_{\mathfrak{P}}$ to \mathbf{Z}_p .*

- (a) *The module $T_{\mathfrak{P}}(A)$ is free of rank 2 over $\mathcal{O}_{\mathfrak{P}}$,*
- (b) *there is a perfect, skew-symmetric, $\mathcal{O}_{\mathfrak{P}}$ -bilinear, G_F -equivariant pairing*

$$e_{\mathfrak{P}} : T_{\mathfrak{P}}(A) \times T_{\mathfrak{P}}(A) \rightarrow \mathcal{O}_{\mathfrak{P}}(1)$$

such that the pairing (8) factors as $\text{Tr} \circ e_{\mathfrak{P}}$,

- (c) the action of any complex conjugation in G_F splits $T_{\mathfrak{p}}(A)$ into two rank-one eigenspaces,
- (d) for any admissible ℓ , the Frobenius of ℓ (over F) acts as a conjugate of complex conjugation on $T_{\mathfrak{p}}(A)/I_{\ell}T_{\mathfrak{p}}(A)$, and $a_{\ell} \in I_{\ell}$.

Proof. Fix a complex parametrization $\mathbf{C}^d/L \cong A(\mathbf{C})$. Then $T_{\mathfrak{p}}(A) \cong L \otimes_{\mathcal{O}_{\mathfrak{p}}} \mathcal{O}_{\mathfrak{p}}$ is free of rank 2 over $\mathcal{O}_{\mathfrak{p}}$. If $\mathfrak{d} \in \Phi_{\mathfrak{p}}$ is a generator for the (absolute) inverse different of $\mathcal{O}_{\mathfrak{p}}$, then the map

$$\mathrm{Hom}_{\mathcal{O}_{\mathfrak{p}}}(T_{\mathfrak{p}}(A), \mathcal{O}_{\mathfrak{p}}) \rightarrow \mathrm{Hom}_{\mathbf{Z}_p}(T_{\mathfrak{p}}(A), \mathbf{Z}_p)$$

defined by $f \mapsto \mathrm{Tr} \circ (\mathfrak{d} \cdot f)$ is an isomorphism. For any $s \in T_{\mathfrak{p}}(A)$, let f_s denote the image of s under $T_{\mathfrak{p}}(A) \rightarrow \mathrm{Hom}_{\mathbf{Z}_p}(T_{\mathfrak{p}}(A), \mathbf{Z}_p(1))$, and let g_s be the unique lift of f_s to $\mathrm{Hom}_{\mathcal{O}_{\mathfrak{p}}}(T_{\mathfrak{p}}(A), \mathcal{O}_{\mathfrak{p}}(1))$. The pairing $e_{\mathfrak{p}}(s, t) = g_s(t)$ now has the desired properties of (b). Part (c) follows from the Galois equivariance of this pairing. The claims of (d) follow from the fact that the Frobenius of ℓ over E acts trivially on $T_{\mathfrak{p}}(A)/I_{\ell}T_{\mathfrak{p}}(A)$, and the Frobenius relative to F acts on $T_{\mathfrak{p}}(A)$ with characteristic polynomial $1 - a_{\ell}X + \mathbf{N}(\ell)X^2$. \square

Definition 2.3.2. We define the *canonical* Selmer structure $(\mathcal{F}^{\mathrm{can}}, \Sigma)$ on V by taking the unramified local condition at any place v of E not dividing p , and taking the image of the local Kummer map

$$A(E_v) \otimes_{\mathcal{O}} F_{\phi} \rightarrow H^1(E_v, V)$$

if v does divide p . We also denote by $\mathcal{F}^{\mathrm{can}}$ the Selmer structures on T and W obtained by propagation.

Proposition 2.3.3. *At every place v of E , the sequence*

$$0 \rightarrow H_{\mathcal{F}^{\mathrm{can}}}^1(E_v, W) \rightarrow H^1(E_v, W) \rightarrow H^1(E_v, A)[\mathfrak{p}^{\infty}] \rightarrow 0$$

is exact. Consequently, there is an exact sequence

$$0 \rightarrow A(E) \otimes_{\mathcal{O}} (\Phi_{\mathfrak{p}}/\mathcal{O}_{\mathfrak{p}}) \rightarrow H_{\mathcal{F}^{\mathrm{can}}}^1(E, W) \rightarrow \mathrm{III}(A/E)[\mathfrak{p}^{\infty}] \rightarrow 0.$$

Proof. This is Proposition 1.6.8 of [20]. \square

Lemma 2.3.4. *For any prime v of E not dividing p ,*

$$H_{\mathcal{F}^{\mathrm{can}}}^1(E_v, V) = H_{\mathcal{F}^{\mathrm{can}}}^1(E_v, W) = 0.$$

Proof. This follows from Corollary 1.3.3 of [20]. \square

For $\ell \in \mathcal{L}_1$ set $u_{\ell} = (\mathbf{N}(\ell) + 1)/|G(\ell)| \in \mathbf{Z}_p^{\times}$. If $m \in \mathcal{M}_1$, set $u_m = \prod_{\ell|m} u_{\ell}$ and define

$$h(m) = u_m^{-1}[\mathcal{O}_E^{\times} : \mathcal{O}_m^{\times}] \cdot \mathrm{Norm}_{E[m]/E(m)} h[m] \in A(E(m)) \otimes_{\mathcal{O}} \mathcal{O}_{\mathfrak{p}},$$

where $h[m]$ is the Heegner point of Section 1.3, and let c_m be the image of $h(m)$ under the Kummer map $A(E(m)) \otimes_{\mathcal{O}} \mathcal{O}_{\mathfrak{p}} \rightarrow H^1(E(m), T)$. The collection

$$\{c_m \in H^1(E(m), T) \mid m \in \mathcal{M}_1\}$$

is the *Heegner point Euler system*, and satisfies the relation

$$\mathrm{Norm}_{E(m\ell)/E(m)} c_{m\ell} = u_{\ell}^{-1} a_{\ell} \cdot c_m.$$

For each admissible ℓ we fix a generator $\sigma_\ell \in G(\ell)$ and define Kolyvagin's *derivative operator* $D_\ell \in \mathcal{O}_{\mathfrak{p}}[G(\ell)]$ by

$$D_\ell = \sum_{i=1}^{|G(\ell)|-1} i\sigma_\ell^i.$$

The derivative operator satisfies the telescoping identity $(\sigma_\ell - 1)D_\ell = |G(\ell)| - N_\ell$, where $N_\ell \in \mathcal{O}_{\mathfrak{p}}[G(\ell)]$ is the norm element. If $m \in \mathcal{M}_1$ let $D_m \in \mathcal{O}_{\mathfrak{p}}[G(m)]$ be defined by $D_m = \prod_{\ell|m} D_\ell$. Exactly as in [9], the class

$$D_m c_m \in H^1(E(m), T/I_m T)$$

is fixed by the action of $G(m)$, and there is a unique class $\kappa'_m \in H^1(E, T/I_m T)$ mapping to $D_m c_m$ under restriction. In order to remove the dependence on the choices of σ_ℓ , set

$$\kappa_m = \kappa'_m \otimes_{\ell|m} \sigma_\ell \in H^1(E, T/I_m T) \otimes \Delta_m.$$

The collection $\{\kappa_m \mid m \in \mathcal{M}_1\}$ (or at least some multiple of it) is the *Heegner point Kolyvagin system*.

Lemma 2.3.5. *Let c^{tam} be the product of the local Tamagawa factors of A/E . For every $m \in \mathcal{M}_1$, $c^{\text{tam}} \cdot \kappa'_m \in H^1_{\mathcal{F}(m)}(E, T/I_m T)$.*

Proof. We identify $T/I_m T \cong W[I_m]$. Suppose v is a prime of E not dividing mp . We must show that $\text{loc}_v(c^{\text{tam}} \cdot \kappa'_m) \in H^1_{\mathcal{F}^{\text{can}}}(E_v, W[I_m])$. If v is archimedean, then by Remark 2.1.3 there is nothing to prove, and so we assume v is nonarchimedean. Let w be a prime of $E(m)$ above v . It follows from Lemma 2.3.4 and Proposition 2.3.3 (which hold with E replaced by $E(m)$) that the image of $h(m)$ under the composition

$$A(E(m)) \rightarrow A(E(m)_w) \rightarrow H^1(E(m)_w, W[I_m]) \rightarrow H^1(E(m)_w, W)$$

is trivial for every w above v , and so the image of $D_m c_m$ under

$$H^1(E(m), W[I_m]) \rightarrow H^1(E(m)_w, W)$$

is trivial. Since v is unramified in $E(m)$, this shows that κ'_m lies in $H^1_{\text{unr}}(E_v, W)$ and hence (since the order of $H^1_{\text{unr}}(E_v, W)$ is the p -part of the local Tamagawa factor at v by Proposition I.3.8 of [15] and the Herbrand quotient) $c^{\text{tam}} \kappa'_m$ has trivial image in $H^1(E_v, W)$. By Lemma 2.3.4 and the definition of propagation of Selmer structures, this shows that the localization of $c^{\text{tam}} \kappa'_m$ at v lies in $H^1_{\mathcal{F}}(E_v, W[I_m])$.

Suppose that $v = \ell$ is a divisor of m , and let λ be the unique prime of $E(\ell)$ above ℓ . It suffices to show that κ'_m has trivial image in $H^1(E(\ell)_\lambda, W[I_m])$, and since λ splits completely in $E(m)$ it suffices to check that $D_m c_m$ is trivial in the semilocalization

$$H^1(E(m)_\ell, W[I_m]) \stackrel{\text{def}}{=} \bigoplus_{w|\ell} H^1(E(m)_w, W[I_m]).$$

Since the image of the Kummer map in $H^1(E(m)_w, W[I_m])$ is unramified for every choice of w , it follows that $\text{loc}_\ell(c_m) \in H^1_{\text{unr}}(E(m)_\ell, W[I_m])$. Evaluation at Frobenius gives an isomorphism of $G(m)$ -modules

$$H^1_{\text{unr}}(E(m)_\ell, W[I_m]) \cong \bigoplus_{w|\ell} W[I_m],$$

where $G(m)$ acts on the right hand side by permuting the summands. In particular $G(\ell) \subset G(m)$ acts trivially, since every prime of $E(m/\ell)$ above ℓ is totally ramified in $E(m)$. The action of D_ℓ on $H_{\text{unr}}^1(E(m)_\ell, W[I_m])$ is therefore multiplication by $\frac{|G(\ell)| \cdot (|G(\ell)| - 1)}{2} \in I_\ell$. This shows that $D_m c_m = D_\ell D_{m/\ell} c_m$ is trivial in $H^1(E(m)_\ell, W[I_m])$.

Suppose v divides p . By Proposition 2.3.3 it suffices to show that the image of κ'_m under the composition

$$H^1(E, W[I_m]) \rightarrow H^1(E_v, W) \rightarrow H^1(E_v, A)$$

is trivial. Consider the commutative diagram

$$\begin{array}{ccc} H^1(E_v, W[I_m]) & \longrightarrow & \bigoplus_{w|v} H^1(E(m)_w, W[I_m]) \\ \downarrow & & \downarrow \\ H^1(E_v, A) & \longrightarrow & \bigoplus_{w|v} H^1(E(m)_w, A). \end{array}$$

The image of $\text{loc}_v(\kappa_m)$ under the top horizontal arrow is $\bigoplus \text{loc}_w(D_m c_m)$, and the image of this under the right vertical arrow is trivial, since c_m is in the image of the global Kummer map. Since A has good reduction at v , Proposition I.3.8 of [15] implies that the restriction map

$$H^1(E_v, A) \rightarrow H^1(E_v^{\text{unr}}, A)$$

is injective, and so the bottom horizontal arrow of the diagram is also injective. This proves the claim. \square

Lemma 2.3.6. *For every $\ell \in \mathcal{M}_1$ there is an $\mathcal{O}_{\mathfrak{p}}$ -automorphism χ_ℓ of $T/I_\ell T$ such that the isomorphism*

$$\phi : H_{\text{unr}}^1(E_\ell, T/I_{m\ell}T) \cong T/I_{m\ell}T \xrightarrow{\chi_\ell} T/I_{m\ell}T \cong H_{\text{tr}}^1(E_\ell, T/I_{m\ell}T) \otimes \Delta_\ell$$

satisfies $\phi(\text{loc}_\ell(c^{\text{tam}} \cdot \kappa'_m)) = \text{loc}_\ell(c^{\text{tam}} \cdot \kappa'_{m\ell}) \otimes \sigma_\ell$ for every m such that $m\ell \in \mathcal{M}_1$. Furthermore, if $m \in \mathcal{M}_1$ then the maps $\chi_\ell : T/I_m T \rightarrow T/I_m T$ with $\ell|m$ pairwise commute.

Proof. This is exactly as in Proposition 4.4 of [14]. \square

Theorem 2.3.7. *Suppose $h(1) \neq 0$. Then*

- (a) *the $\mathcal{O}_{\mathfrak{p}}$ -modules $A(E) \otimes_{\mathcal{O}} \mathcal{O}_{\mathfrak{p}}$ and $H_{\mathcal{F}^{\text{can}}}^1(E, T)$ are free of rank one,*
- (b) *the \mathfrak{P} -primary component of $\text{III}(A/E)$ is finite,*
- (c) *there is a finite $\mathcal{O}_{\mathfrak{p}}$ -module M such that*

$$H_{\mathcal{F}^{\text{can}}}^1(E, W) \cong \mathcal{D}_{\mathfrak{p}} \oplus M \oplus M$$

$$\text{and } \text{length}_{\mathcal{O}_{\mathfrak{p}}}(M) \leq \text{length}_{\mathcal{O}_{\mathfrak{p}}}(H_{\mathcal{F}^{\text{can}}}^1(E, T)/\mathcal{O}_{\mathfrak{p}} \cdot h(1)).$$

Proof. For each $m \in \mathcal{M}_1$ and $\ell|m$, the automorphism χ_ℓ of the preceding Lemma induces an automorphism of $H^1(E, T/I_m T)$ which we still denote by χ_ℓ . Setting χ_m equal to the composition of χ_ℓ as ℓ runs over all divisors of m , the collection

$$c^{\text{tam}} \chi_m^{-1}(\kappa_m) \in H_{\mathcal{F}(m)}^1(E, T/I_m T) \otimes \Delta_m$$

is a Kolyvagin system for $(T, \mathcal{F}, \mathcal{L}_1)$. Furthermore, κ_1 is equal to the image of $h(1)$ under the Kummer map $A(E) \otimes \mathcal{O}_{\mathfrak{p}} \rightarrow H_{\mathcal{F}}^1(E, T)$.

By Theorem 2.2.2 (applied to the family $\chi_m^{-1}(\kappa_m)$ with $p^d \mathbf{Z}_p = c^{\text{tam}} \mathbf{Z}_p$) we need only check that the hypotheses **H1–H5** are satisfied. Recall our assumption that the image of $G_E \rightarrow \text{Aut}_{\mathcal{O}_{\mathfrak{p}}}(T_{\mathfrak{p}}(A))$ is equal to $G_{\mathfrak{p}}$, the subgroup of automorphisms whose determinant lies in \mathbf{Z}_p^\times . Taking $L = E(A[\mathfrak{P}^\infty])$, we have $H^1(L/E, A[\mathfrak{P}]) \cong H^1(G_{\mathfrak{p}}, A[\mathfrak{P}])$ which is trivial (apply the inflation-restriction sequence to the subgroup $\mathbf{Z}_p^\times \hookrightarrow G_{\mathfrak{p}}$ imbedded along the diagonal), showing that **H1** holds. Hypothesis **H2** follows from Lemma 2.3.1 and the fact that $G_{\mathfrak{p}}$ acts transitively on the nontrivial elements of $A[\mathfrak{P}]$. If $e_{\mathfrak{p}}$ denotes the pairing of Lemma 2.3.1, then the pairing $(s, t) = e_{\mathfrak{p}}(s, t^\tau)$ satisfies the properties of **H3**. Hypothesis **H4** is Tate local duality, and **H5** is trivially verified. \square

3. IWASAWA THEORY

Let $\phi, A, E/F, \mathcal{O} \subset F_\phi, p, \mathfrak{P}, \mathcal{O}_{\mathfrak{p}}, \Phi_{\mathfrak{p}}$, and $\mathcal{D}_{\mathfrak{p}}$ be as in Section 2.3. In addition to conditions (1) and (2) of the Introduction, we assume that

- (a) there is a unique prime $\mathfrak{p} = p\mathcal{O}$ of F above p ,
- (b) A has good ordinary reduction at \mathfrak{p} .

It can be deduced from the results of Section 3.6.2 of [7] that the ordinary hypothesis implies that $a_{\mathfrak{p}} \in \mathcal{O}_{\mathfrak{p}}^\times$. Recall that $\Phi_{\mathfrak{p}}$ denotes the field of fractions of $\mathcal{O}_{\mathfrak{p}}$, and $\mathcal{D}_{\mathfrak{p}} = \Phi_{\mathfrak{p}}/\mathcal{O}_{\mathfrak{p}}$. Let Σ be a finite set of places of E consisting of the archimedean places and the divisors of $\mathfrak{p}N\mathcal{O}_E$, and define E^Σ to be the maximal extension of E unramified outside Σ .

Our main tool for studying the cohomology of the Λ -modules \mathbf{T} and \mathbf{W} (defined in the next section) is to consider, following [13], the cohomology of $\mathbf{T} \otimes_\Lambda S$ as S runs over discrete valuation rings with Λ -algebra structures. The added complication of working over an Iwasawa algebra in several variables presents several new technical hurdles, but apart from that point the arguments follow [9] very closely.

3.1. Heegner points in anti-cyclotomic extensions. As before, for any ideal c of \mathcal{O}_F we let $E[c]$ denote the ring class field of conductor c , and $E(c)$ the maximal p -power subextension. The field $E[\mathfrak{p}^\infty] = \cup E[\mathfrak{p}^k]$ has

$$\text{Gal}(E[\mathfrak{p}^\infty]/E[1]) \cong \mathcal{O}_{E, \mathfrak{p}}^\times / \mathcal{O}_{F, \mathfrak{p}}^\times$$

and so $E[\mathfrak{p}^\infty]$ contains a unique subfield, E_∞ , with $\Gamma \stackrel{\text{def}}{=} \text{Gal}(E_\infty/E) \cong \mathbf{Z}_p^g$. We call this the anti-cyclotomic extension of E . Our running assumptions on p imply that each prime of E above \mathfrak{p} is totally ramified in E_∞ , that $E_k = E(\mathfrak{p}^{k+1})$ is the fixed field of Γ^{p^k} , and that E_k and $E(m)$ are linearly disjoint over E for any $m \in \mathcal{M}_1$. Define $E_k(m) = E_k E(m) = E(m\mathfrak{p}^{k+1})$, and set $E_\infty(m) = \cup E_k(m)$. Exactly as in Lemma 2.1.5, one may easily check the following facts:

- (a) for any $m \in \mathcal{M}_1$, $E_\infty(m)/F$ is of dihedral type,
- (b) if $m\ell \in \mathcal{M}_1$ then the unique prime of E above ℓ splits completely in $E_\infty(m)$.

Let $\Lambda = \mathcal{O}_{\mathfrak{p}}[[\Gamma]]$ be the Iwasawa algebra, and let $\iota : \Lambda \rightarrow \Lambda$ be the involution which is inversion on group-like elements.

As in Section 2.2 of [9], we define G_E and Λ -modules

$$\mathbf{T} = \varprojlim \text{Ind}_{E_k/E} T_{\mathfrak{p}}(A) \quad \mathbf{W} = \varinjlim \text{Ind}_{E_k/E} A[\mathfrak{P}^\infty],$$

where $\text{Ind}_{E_k/E}$ is the induction functor from G_{E_k} -modules to G_E -modules, and the limits are with respect to the natural corestriction and restriction maps. There is

an isomorphism $\mathbf{T} = T_{\mathfrak{p}}(A) \otimes_{\mathcal{O}_{\mathfrak{p}}} \Lambda$ with G_E acting on the second factor through $G_E \rightarrow \Lambda^\times \xrightarrow{t} \Lambda^\times$, and Shapiro's lemma gives canonical isomorphisms

$$\begin{aligned} H^1(E(m), \mathbf{T}) &\cong \varprojlim H^1(E_k(m), T_{\mathfrak{p}}(A)) \\ H^1(E(m), \mathbf{W}) &\cong \varinjlim H^1(E_k(m), A[\mathfrak{P}^\infty]), \end{aligned}$$

and similar isomorphisms on semi-local cohomology. Furthermore, as in Proposition 2.2.4 of [9], there is a perfect, G_E -equivariant pairing

$$(9) \quad e_\Lambda : \mathbf{T} \times \mathbf{W} \rightarrow \mathcal{D}_{\mathfrak{p}}(1)$$

satisfying $e_\Lambda(\lambda t, a) = e_\Lambda(t, \lambda^t a)$ for all $t \in \mathbf{T}$, $a \in \mathbf{W}$, and $\lambda \in \Lambda$. The action of G_E on \mathbf{T} and \mathbf{W} factors through $\text{Gal}(E^\Sigma/E)$.

For each integer $k \geq 0$ we define the Heegner point $h_k(m) \in A(E_k(m)) \otimes_{\mathcal{O}} \mathcal{O}_{\mathfrak{p}}$ by

$$h_k(m) = u_m^{-1} [\mathcal{O}_E^\times : \mathcal{O}_m^\times] \cdot \text{Norm}_{E[m\mathfrak{p}^{k+1}]/E_k(m)} h[m\mathfrak{p}^{k+1}],$$

with $u_m \in \mathbf{Z}_p^\times$ as in Section 2.3. For $m \in \mathcal{M}_1$ and $k \geq 0$, let

$$H_k(m) \subset A(E_k(m)) \otimes_{\mathcal{O}} \mathcal{O}_{\mathfrak{p}}$$

be the $\mathcal{O}_{\mathfrak{p}}[\text{Gal}(E_k(m))/E(m)]$ -module generated by $h_j(m)$ for $0 \leq j \leq k$, and set $H_\infty(m) = \varprojlim H_k(m)$. Define $\Phi \in \mathcal{O}_{\mathfrak{p}}[\text{Gal}(E(m)/E)]$ by the formula

$$\Phi = \begin{cases} (N(\mathfrak{p}) + 1)^2 - a_{\mathfrak{p}}^2 & \text{inert case} \\ (N(\mathfrak{p}) - a_{\mathfrak{p}}\sigma + \sigma^2)(N(\mathfrak{p}) - a_{\mathfrak{p}}\sigma^* + \sigma^{*2}) & \text{split case,} \end{cases}$$

in which split and inert refer to the behavior of \mathfrak{p} in E , and σ and σ^* are the Frobenius elements in $\text{Gal}(E(m)/E)$ of the primes above \mathfrak{p} . As k varies, the points $h_k(m)$ are almost norm compatible, and can be modified to give elements of $H_\infty(m)$:

Proposition 3.1.1. *There is a family $\{c_m \in H_\infty(m) \mid m \in \mathcal{M}_1\}$ satisfying*

- (a) c_m generates the torsion-free Λ -module $H_\infty(m)$, and is nonzero if and only if $h_k(m)$ has infinite order for some k ,
- (b) for $m\ell \in \mathcal{M}_1$, $\text{Norm}_{E_\infty(m\ell)/E_\infty(m)} c_{m\ell} = u_\ell^{-1} a_\ell \cdot c_m$,
- (c) the image of c_m under $H_\infty(m) \rightarrow H_0(m)$ is $\Phi h(m)$, where $h(m)$ is the Heegner point of Section 2.3.

Proof. This is proven exactly as in Section 2.3 of [9]. \square

3.2. Ordinary Selmer modules. For each prime \mathfrak{q} dividing $\mathfrak{p}\mathcal{O}_E$, define $\mathcal{O}_{\mathfrak{p}}$ -modules $A[\mathfrak{P}^\infty]^\pm$ by taking $A[\mathfrak{P}^\infty]^+$ to be the kernel of reduction

$$A[\mathfrak{P}^\infty] \rightarrow \tilde{A}[\mathfrak{P}^\infty],$$

where \tilde{A} is the reduction of A at \mathfrak{q} , and $A[\mathfrak{P}^\infty]^- = \tilde{A}[\mathfrak{P}^\infty]$. Define $T_{\mathfrak{p}}(A)^\pm$ similarly, and note that although we suppress it from the notation, these modules depend on \mathfrak{q} . In fact, they depend on fixing a place of \bar{E} above \mathfrak{q} , as does the localization map $H^i(E, A[\mathfrak{P}^\infty]) \rightarrow H^i(E_{\mathfrak{q}}, A[\mathfrak{P}^\infty])$. We will always assume, without further comment, that consistent choices are made. By definition, there are exact sequences

$$\begin{aligned} 0 &\rightarrow T_{\mathfrak{p}}(A)^+ \rightarrow T_{\mathfrak{p}}(A) \rightarrow T_{\mathfrak{p}}(A)^- \rightarrow 0 \\ 0 &\rightarrow A[\mathfrak{P}^\infty]^+ \rightarrow A[\mathfrak{P}^\infty] \rightarrow A[\mathfrak{P}^\infty]^- \rightarrow 0. \end{aligned}$$

The pairing of Lemma 2.3.1 induces perfect pairings

$$T_{\mathfrak{p}}(A)^\pm \times A[\mathfrak{P}^\infty]^\mp \rightarrow \mathcal{D}_{\mathfrak{p}}(1).$$

For each prime of E dividing \mathfrak{p} , the exact sequences above induce exact sequences

$$\begin{aligned} 0 &\rightarrow \mathbf{T}^+ \rightarrow \mathbf{T} \rightarrow \mathbf{T}^- \rightarrow 0 \\ 0 &\rightarrow \mathbf{W}^+ \rightarrow \mathbf{W} \rightarrow \mathbf{W}^- \rightarrow 0 \end{aligned}$$

together with perfect pairings $\mathbf{T}^\pm \times \mathbf{W}^\mp \rightarrow \mathcal{D}_{\mathfrak{p}}(1)$.

Lemma 3.2.1. *For every place v of E not dividing \mathfrak{p} , the groups*

$$H^1(E_v, \mathbf{T})/H_{\text{unr}}^1(E_v, \mathbf{T}) \quad H_{\text{unr}}^1(E_v, \mathbf{W})$$

have finite exponent. If $v \notin \Sigma$ these groups are trivial.

Proof. All references in this proof are to [20]. Let L be an unramified finite extension of E_v . By Corollary 1.3.3 and local Tate duality,

$$H^1(L, T_{\mathfrak{p}}(A) \otimes \Phi_{\mathfrak{p}}) = H_{\text{unr}}^1(L, T_{\mathfrak{p}}(A) \otimes \Phi_{\mathfrak{p}}) = 0,$$

and so Lemma 1.3.5 (iii) implies that

$$H^1(L, T_{\mathfrak{p}}(A))/H_{\text{unr}}^1(L, T_{\mathfrak{p}}(A)) \cong \mathcal{W}^{\text{Fr}=1}$$

where \mathcal{W} is $A(E_v^{\text{unr}})[\mathfrak{p}^\infty]$ modulo its maximal divisible subgroup. Note that \mathcal{W} is finite of order independent of L , and is trivial if $v \notin \Sigma$. The claim now follows from the identification

$$H^1(E_v, \mathbf{T})/H_{\text{unr}}^1(E_v, \mathbf{T}) \cong \varprojlim_{w|v} \bigoplus H^1(E_{k,w}, T_{\mathfrak{p}}(A))/H_{\text{unr}}^1(E_{k,w}, T_{\mathfrak{p}}(A))$$

of Shapiro's lemma, together with the perfect pairing

$$H^1(E_v, \mathbf{T})/H_{\text{unr}}^1(E_v, \mathbf{T}) \times H_{\text{unr}}^1(E_v, \mathbf{W}) \rightarrow \mathcal{D}_{\mathfrak{p}}$$

of Tate local duality. \square

Definition 3.2.2. Following [4], we define the *ordinary* Selmer structures \mathcal{F}_{ord} on \mathbf{T} and \mathbf{W} by

$$\begin{aligned} H_{\mathcal{F}_{\text{ord}}}^1(E_v, \mathbf{T}) &= \begin{cases} H^1(E_v, \mathbf{T}^+) & \text{if } v \mid \mathfrak{p} \\ H^1(E_v, \mathbf{T}) & \text{else} \end{cases} \\ H_{\mathcal{F}_{\text{ord}}}^1(E_v, \mathbf{W}) &= \begin{cases} H^1(E_v, \mathbf{W}^+) & \text{if } v \mid \mathfrak{p} \\ 0 & \text{else} \end{cases} \end{aligned}$$

and remark that these local conditions are everywhere exact orthogonal complements under the local Tate pairing $H^1(E_v, \mathbf{T}) \times H^1(E_v, \mathbf{W}) \rightarrow \mathcal{D}_{\mathfrak{p}}$.

By standard results, the Selmer groups $H_{\mathcal{F}_{\text{ord}}}^1(E, \mathbf{T})$ and $H_{\mathcal{F}_{\text{ord}}}^1(E, \mathbf{W})$ are finitely and cofinitely generated, respectively, as Λ -modules. Let

$$X = \text{Hom}_{\mathcal{O}_{\mathfrak{p}}} (H_{\mathcal{F}_{\text{ord}}}^1(E, \mathbf{W}), \mathcal{D}_{\mathfrak{p}}),$$

and let $X_{\text{tors}} \subset X$ be the Λ -torsion submodule.

Remark 3.2.3. By the main result of [4], Shapiro's lemma identifies the module X with the X defined in the Introduction (exactly, not just up to pseudo-isomorphism!). Similarly, $H_{\mathcal{F}_{\text{ord}}}^1(E, \mathbf{T})$ is identified with the module $S_{\mathfrak{p}, \infty}$ of the Introduction.

Proposition 3.2.4. *The Λ -module $H_{\mathcal{F}_{\text{ord}}}^1(E, \mathbf{T})$ is torsion-free.*

Proof. It suffices to show that $H^1(E^\Sigma/E, \mathbf{T})$ is torsion-free, and we imitate the method of [18]. Let $\Lambda_n = \mathcal{O}_{\mathfrak{p}}[\text{Gal}(E_n/E)]$ and set

$$X_n = \text{Hom}_{\mathcal{O}_{\mathfrak{p}}}(H^1(E^\Sigma/E_n, A[\mathfrak{P}^\infty]), \mathcal{D}_{\mathfrak{p}}).$$

Using $A(E_\infty)[\mathfrak{P}] = 0$ we have a canonical isomorphism

$$H^1(E^\Sigma/E_n, T_{\mathfrak{p}}(A)) \cong \text{Hom}_{\mathcal{O}_{\mathfrak{p}}}(X_n, \mathcal{O}_{\mathfrak{p}}),$$

and the map $\Lambda_n \rightarrow \mathcal{O}_{\mathfrak{p}}$ defined by extracting the coefficient of the neutral element of $\text{Gal}(E_n/E)$ induces an isomorphism

$$\text{Hom}_{\Lambda_n}(X_n, \Lambda_n) \cong \text{Hom}_{\mathcal{O}_{\mathfrak{p}}}(X_n, \mathcal{O}_{\mathfrak{p}}).$$

Using Shapiro's lemma, we obtain in the limit an isomorphism

$$H^1(E^\Sigma/E, \mathbf{T}) \cong \text{Hom}_{\Lambda}(\varprojlim X_n, \Lambda),$$

which proves the claim. \square

Definition 3.2.5. By a *specialization* of Λ , we mean the ring of integers S of a finite extension of $\mathcal{O}_{\mathfrak{p}}$, together with a homomorphism of $\mathcal{O}_{\mathfrak{p}}$ -algebras $\phi : \Lambda \rightarrow S$ with finite cokernel. If $\phi : \Lambda \rightarrow S$ is a specialization, we define the *dual specialization* $\phi^* : \Lambda \rightarrow S^*$ by $S^* = S$ and $\phi^* = \phi \circ \iota$. The maximal ideal of S is denoted $\mathfrak{m} = \mathfrak{m}_S$.

We view all specializations as taking values in a fixed algebraic closure of $\Phi_{\mathfrak{p}}$. For any specialization $\phi : \Lambda \rightarrow S$, we let Φ_S be the field of fractions of S , and set $\mathcal{D}_S = \Phi_S/S$. Furthermore, we define S -modules

$$T_S = \mathbf{T} \otimes_{\Lambda} S \quad V_S = T_S \otimes_S \Phi_S \quad W_S = V_S/T_S,$$

and for each prime of E above \mathfrak{p} ,

$$T_S^\pm = \mathbf{T}^\pm \otimes_{\Lambda} S \quad V_S^\pm = T_S^\pm \otimes_S \Phi_S \quad W_S^\pm = V_S^\pm/T_S^\pm.$$

We regard T_S as a G_E module, with G_E acting trivially on S . Alternatively, we may identify $T_S \cong T_{\mathfrak{p}}(A) \otimes_{\mathcal{O}_{\mathfrak{p}}} S$ with G_E acting on the second factor by $s^\sigma = \phi(\sigma^{-1})s$.

If we let $e_{\mathfrak{p}}$ denote the pairing of Lemma 2.3.1 and identify both T_S and T_{S^*} with $T_{\mathfrak{p}}(A) \otimes_{\mathcal{O}_{\mathfrak{p}}} S$ as S -modules (which defines two distinct Λ and G_E -module structures on $T_{\mathfrak{p}}(A) \otimes_{\mathcal{O}_{\mathfrak{p}}} S$), then the pairing

$$(10) \quad T_S \times T_{S^*} \rightarrow S(1)$$

defined by $(t_0 \otimes s_0, t_1 \otimes s_1) \mapsto s_0 s_1 \cdot e_{\mathfrak{p}}(t_0, t_1)$ is perfect, S -bilinear, G_E -equivariant, and satisfies $(\lambda x, y) = (x, \lambda^t y)$ for $\lambda \in \Lambda$. If \mathfrak{d} is a generator for the inverse different of $\Phi_S/\Phi_{\mathfrak{p}}$, then the composition

$$S \xrightarrow{\mathfrak{d}} \mathfrak{d}S \xrightarrow{\text{Trace}} \mathcal{O}_{\mathfrak{p}},$$

together with the pairing (10), gives perfect pairings

$$T_S \times T_{S^*} \rightarrow \mathcal{O}_{\mathfrak{p}}(1) \quad T_S \times W_{S^*} \rightarrow \mathcal{D}_{\mathfrak{p}}(1).$$

Dualizing the map $\mathbf{T} \rightarrow T_{S^*}$, and using the pairing (9), we obtain a G_E -equivariant map of Λ -modules $W_S \rightarrow \mathbf{W}$.

Definition 3.2.6. If S is a specialization of Λ , we define a Selmer structure \mathcal{F}_S on V_S by

$$H_{\mathcal{F}_S}^1(E_v, V_S) = \begin{cases} H^1(E_v, V_S^+) & \text{if } v \mid \mathfrak{p} \\ H_{\text{unr}}^1(E_v, V_S) & \text{else} \end{cases}$$

and propagate this to Selmer structures on T_S and W_S .

Proposition 3.2.7. *For every specialization S of Λ , there is an S -bilinear pairing*

$$H_{\mathcal{F}_S}^1(E, W_S) \times H_{\mathcal{F}_{S^*}}^1(E, W_{S^*}) \rightarrow \mathcal{D}_S$$

whose kernels on either side are the submodules of S -divisible elements.

Proof. This follows from the main result of [6], the construction of a generalized Cassels-Tate pairing. \square

Lemma 3.2.8. *For any specialization $\phi : S \rightarrow \Lambda$, the module T_S and the Selmer structure \mathcal{F}_S on T_S satisfy hypotheses **H1**–**H5** of Section 2.2.*

Proof. Let $L = E(A[\mathfrak{P}^\infty])$ and $L_\infty = LE_\infty$ and consider the inflation-restriction sequence

$$0 \rightarrow H^1(L/E, A[\mathfrak{P}]) \rightarrow H^1(L_\infty/E, A[\mathfrak{P}]) \rightarrow \text{Hom}(\text{Gal}(L_\infty/L), A[\mathfrak{P}])^{\text{Gal}(L/E)}.$$

The final term is 0, since we are assuming condition (2) of the Introduction. The term $H^1(L/E, A[\mathfrak{P}])$ is also zero, by the proof of Theorem 2.3.7, and so **H1** holds. For **H2**, we may identify $T_S \cong T_{\mathfrak{P}}(A) \otimes_{\mathcal{O}_{\mathfrak{P}}} S$ with G_E acting on S via $G_E \rightarrow \Lambda^\times \xrightarrow{\iota} \Lambda^\times \rightarrow S^\times$. In particular, the action of G_E on the residual representation of S is trivial. The residual representation of T_S is therefore isomorphic to $A[\mathfrak{P}] \otimes S$, with G_E now acting only on the first factor.

For hypothesis **H3**, we again identify T_S with $T_{\mathfrak{P}}(A) \otimes_{\mathcal{O}_{\mathfrak{P}}} S$. Let $e_{\mathfrak{P}}$ be the pairing of Lemma 2.3.1, and define a pairing

$$T_{\mathfrak{P}}(A) \otimes_{\mathcal{O}_{\mathfrak{P}}} S \times T_{\mathfrak{P}}(A) \otimes_{\mathcal{O}_{\mathfrak{P}}} S \rightarrow S(1)$$

by $(t_0 \otimes s_0, t_1 \otimes s_1) \mapsto s_0 s_1 \cdot e_{\mathfrak{P}}(t_0, t_1)$. It is trivial to verify that this pairing has the desired properties. Hypotheses **H4** and **H5** follow easily from the definition of \mathcal{F}_S . \square

In the remainder of this section we prove some technical lemmas needed in the next section.

Lemma 3.2.9. *Let $\phi : \Lambda \rightarrow S$ be a specialization with kernel I , and let \mathfrak{q} be a prime of E above \mathfrak{p} . The cokernel of the natural map*

$$H^1(E_{\mathfrak{q}}, \mathbf{T}^+) \rightarrow H^1(E_{\mathfrak{q}}, \mathbf{T}^+/I\mathbf{T}^+)$$

is finite with order bounded by a constant which depends only on $\text{rank}_{\mathcal{O}_{\mathfrak{P}}}(S)$.

Proof. We extend scalars to S : let $\Lambda' = \Lambda \otimes_{\mathcal{O}_{\mathfrak{P}}} S$ and extend ϕ to a surjective S -module map $\phi' : \Lambda' \rightarrow S$. Fix an identification $\Lambda' \cong S[[s_1, \dots, s_g]]$ and define $\alpha_i = \phi(s_i) \in S$. Let I be the ideal of Λ' generated by all $(s_i - \alpha_i)$. Consider the map

$$(11) \quad H^1(E_{\mathfrak{q}}, T_{\mathfrak{P}}(A)^+ \otimes \Lambda') \rightarrow H^1(E_{\mathfrak{q}}, T_{\mathfrak{P}}(A)^+ \otimes (\Lambda'/I)).$$

If $I_r \subset \Lambda'$ is the ideal generated by $s_i - \alpha_i$ for $1 \leq i \leq r$, then the cohomology of

$$0 \rightarrow \Lambda'/I_r \xrightarrow{s_{r+1} - \alpha_{r+1}} \Lambda'/I_r \rightarrow \Lambda'/I_{r+1} \rightarrow 0$$

tensored (over $\mathcal{O}_{\mathfrak{p}}$) with $T_{\mathfrak{p}}(A)^+$, yields exactness of

$$\begin{aligned} H^1(E_{\mathfrak{q}}, T_{\mathfrak{p}}(A)^+ \otimes (\Lambda'/I_r)) &\rightarrow H^1(E_{\mathfrak{q}}, T_{\mathfrak{p}}(A)^+ \otimes (\Lambda'/I_{r+1})) \\ &\rightarrow H^2(E_{\mathfrak{q}}, T_{\mathfrak{p}}(A)^+ \otimes (\Lambda'/I_r)). \end{aligned}$$

By local duality and Shapiro's lemma the final term is dual to the I_r -torsion submodule of

$$\varinjlim \oplus_{w|\mathfrak{q}} H^0(E_{k,w}, \tilde{A}[\mathfrak{P}^\infty]) \otimes_{\mathcal{O}_{\mathfrak{p}}} S.$$

Since \mathfrak{q} is totally ramified in E_∞ , this is equal to the \mathfrak{P} -power-torsion of \tilde{A} rational over the residue field of E at \mathfrak{q} (tensored with S), which is clearly finite. It follows that the cokernel of (11) is finite and bounded by a constant depending only on $\text{rank}_{\mathcal{O}_{\mathfrak{p}}}(S)$. This map, however, is exactly the map obtained by tensoring the map in the statement of the lemma (over $\mathcal{O}_{\mathfrak{p}}$) with S , and the claim follows. \square

Lemma 3.2.10. *Let $\phi : \Lambda \rightarrow S$ be a specialization with kernel I . For every place v of E the maps $\mathbf{T}/I\mathbf{T} \rightarrow T_S$ and $W_S \rightarrow \mathbf{W}[I]$ induce Λ -module maps*

$$\begin{aligned} H_{\mathcal{F}_{\text{ord}}}^1(E_v, \mathbf{T}/I\mathbf{T}) &\rightarrow H_{\mathcal{F}_S}^1(E_v, T_S) \\ H_{\mathcal{F}_S}^1(E_v, W_S) &\rightarrow H_{\mathcal{F}_{\text{ord}}}^1(E_v, \mathbf{W}[I]), \end{aligned}$$

where the Selmer structure \mathcal{F}_{ord} on $\mathbf{T}/I\mathbf{T}$ is propagated from \mathbf{T} , and similarly for $\mathbf{W}[I]$. The kernels and cokernels of these maps are finite and bounded by constants depending only $\text{rank}_{\mathcal{O}_{\mathfrak{p}}}(S)$ and $[S : \phi(\Lambda)]$.

Proof. Bounds on the kernel and cokernel of the first map, in the case in which v is a divisor of \mathfrak{p} , are exactly as in the proof of Lemma 2.2.7 of [9], together with Lemma 3.2.9 above.

Consider the case where v does not divide \mathfrak{p} . We first show that the natural map $H_{\text{unr}}^1(E_v, \mathbf{T}) \rightarrow H_{\text{unr}}^1(E_v, \mathbf{T}/I\mathbf{T})$ is surjective. Indeed, as $\text{Gal}(E_v^{\text{unr}}/E_v)$ has cohomological dimension one, it suffices to show that $\mathbf{T}^{\mathcal{I}} \rightarrow (\mathbf{T}/I\mathbf{T})^{\mathcal{I}}$ is surjective, where \mathcal{I} is the inertia subgroup of G_{E_v} . Identifying $\mathbf{T} \cong T_{\mathfrak{p}}(A) \otimes \Lambda$, and using the fact that $T_{\mathfrak{p}}(A)$ is a flat $\mathcal{O}_{\mathfrak{p}}$ -module and that \mathcal{I} acts trivially on Λ , this is equivalent to the surjectivity of $T_{\mathfrak{p}}(A)^{\mathcal{I}} \otimes \Lambda \rightarrow T_{\mathfrak{p}}(A)^{\mathcal{I}} \otimes \Lambda/I$, which is clear.

Now applying Lemma 3.2.1, we see that

$$(12) \quad H_{\text{unr}}^1(E_v, \mathbf{T}/I\mathbf{T}) \subset H_{\mathcal{F}_{\text{ord}}}^1(E_v, \mathbf{T}/I\mathbf{T})$$

with finite index, and equality holds if $v \notin \Sigma$. Furthermore, the index depends only on $\text{rank}_{\mathcal{O}_{\mathfrak{p}}}(S)$ and not on ϕ . The quotient of $H^1(E_v, T_S)$ by $H_{\mathcal{F}_S}^1(E_v, T_S)$ is torsion free, and it follows that the image of

$$H_{\mathcal{F}_{\text{ord}}}^1(E_v, \mathbf{T}/I\mathbf{T}) \rightarrow H^1(E_v, T_S)$$

is contained in $H_{\mathcal{F}_S}^1(E_v, T_S)$.

Exactly as in the proof of Lemma 5.3.13 of [13], the kernel and cokernel of the composition

$$H_{\text{unr}}^1(E_v, \mathbf{T}/I\mathbf{T}) \rightarrow H_{\text{unr}}^1(E_v, T_S) \hookrightarrow H_{\mathcal{F}_S}^1(E_v, T_S)$$

are finite with bounds of the desired sort. The claims concerning the kernel and cokernel of first map of the lemma follow without difficulty. The claims concerning the second map of the statement of the lemma follow from Tate local duality. \square

Lemma 3.2.11. *Let $\phi : \Lambda \rightarrow S$ be a specialization with kernel I . The maps $\mathbf{T}/I\mathbf{T} \rightarrow T_S$ and $W_S \rightarrow \mathbf{W}[I]$ induce Λ -module maps on global cohomology*

$$\begin{aligned} H_{\mathcal{F}_{\text{ord}}}^1(E, \mathbf{T}/I\mathbf{T}) &\rightarrow H_{\mathcal{F}_S}^1(E, T_S) \\ H_{\mathcal{F}_S}^1(E, W_S) &\rightarrow H_{\mathcal{F}_{\text{ord}}}^1(E, \mathbf{W}[I]), \end{aligned}$$

where the Selmer structure \mathcal{F}_{ord} on $\mathbf{T}/I\mathbf{T}$ is propagated from \mathbf{T} , and similarly for $\mathbf{W}[I]$. The kernels and cokernels of these maps are finite and bounded by constants depending only on $\text{rank}_{\mathcal{O}_{\mathfrak{p}}}(S)$ and $[S : \phi(\Lambda)]$.

Proof. This can be deduced from the proof of Proposition 5.3.14 of [13], once we show that $H^1(E, \mathbf{T}) = H^1(E^\Sigma/E, \mathbf{T})$. If $v \notin \Sigma$ is a prime of E which does not split completely in E_∞ , then $H^1(E_v, \mathbf{T}) = H_{\text{unr}}^1(E_v, \mathbf{T})$ by [20] Proposition B.3.4, while if v does splits completely we have

$$H^1(E_v, \mathbf{T}) = H^1(E_v, T) \otimes_{\mathcal{O}_{\mathfrak{p}}} \Lambda = H_{\text{unr}}^1(E_v, T) \otimes_{\mathcal{O}_{\mathfrak{p}}} \Lambda = H_{\text{unr}}^1(E_v, \mathbf{T}).$$

By the proof of [20] Proposition 1.6.8, $H_{\text{unr}}^1(E_v, T \otimes \mathbf{Q}_p) = 0$, and so local Tate duality and the Weil pairing force $H^1(E_v, T \otimes \mathbf{Q}_p) = 0$. From [20] Lemma 1.3.5 it then follows that $H^1(E_v, T) = H_{\text{unr}}^1(E_v, T)$. \square

Lemma 3.2.12. *For any ideal $I \subset \Lambda$, the inclusion $\mathbf{W}[I] \rightarrow \mathbf{W}$ induces an isomorphism*

$$H_{\mathcal{F}_{\text{ord}}}^1(E, \mathbf{W}[I]) \cong H_{\mathcal{F}_{\text{ord}}}^1(E, \mathbf{W})[I].$$

Proof. See Lemma 3.5.3 of [13]. \square

3.3. Choosing specializations. In this section we construct sequences of specializations with nice properties. The reader is advised to read the statements of Proposition 3.3.3 and Corollary 3.3.4, and proceed directly to Section 3.4.

Throughout this section we fix a height-one prime $\mathfrak{Q} \neq \mathfrak{P}\Lambda$ of Λ and some nonzero $c \in H_{\mathcal{F}_{\text{ord}}}^1(E, \mathbf{T})$. Set

$$\mathbf{L}_c = H_{\mathcal{F}_{\text{ord}}}^1(E, \mathbf{T})/\Lambda c.$$

By convention the characteristic ideal of a Λ -module of positive rank is zero, and the order at \mathfrak{Q} of the zero ideal is infinite. Let $\phi : \Lambda \rightarrow S$ be a specialization. By Lemma 3.2.11, the maps $\mathbf{T} \rightarrow T_S$ and $W_S \rightarrow \mathbf{W}$ induce maps, still denoted ϕ , on Selmer modules

$$H_{\mathcal{F}_{\text{ord}}}^1(E, \mathbf{T}) \rightarrow H_{\mathcal{F}_S}^1(E, T_S) \quad H_{\mathcal{F}_S}^1(E, W_S) \rightarrow H_{\mathcal{F}_{\text{ord}}}^1(E, \mathbf{W}).$$

Our goal is to exhibit many specializations for which we have careful control over the kernels and cokernels of these maps.

For any specialization S , Proposition 2.2.1 and Lemma 3.2.8 show that the quotient of $H_{\mathcal{F}_S}^1(E, W_S)$ by its maximal S -divisible submodule has the form $M_S \oplus M_S$.

Let $Q \in \Lambda$ generate the ideal \mathfrak{Q} , and consider the following properties:

Sp1: The Λ -rank of $H_{\mathcal{F}_{\text{ord}}}^1(E, \mathbf{T})$ is equal to the S -rank of $H_{\mathcal{F}_S}^1(E, T_S)$.

Sp2: The Λ -rank of X is equal to the S -corank of $H_{\mathcal{F}_S}^1(E, W_S)$.

Sp3: With M_S as above

$$2 \cdot \text{length}_S(M_S) = \text{ord}_{\mathfrak{Q}}(\text{char}(X_{\Lambda\text{-tors}})) \cdot \text{length}_S(S/\phi(Q)S).$$

Sp4: The equality

$$\text{length}_S(H_{\mathcal{F}_S}^1(E, T_S)/S \cdot \phi(c)) = \text{ord}_{\mathfrak{Q}}(\text{char}(\mathbf{L}_c)) \cdot \text{length}_S(S/\phi(Q)S)$$

holds (we include the case where both sides are infinite),

Sp5: the image of c in $H_{\mathcal{F}_S}^1(E, T_S)$ is nonzero.

Definition 3.3.1. A sequence of specializations $\phi_i : \Lambda \rightarrow S$ (with S independent of i) is said to converge to $\mathfrak{Q} = Q\Lambda$ if

- (a) $\phi_i(Q) \rightarrow 0$, but $\phi_i(Q) \neq 0$ for all i ,
- (b) **Sp1,2,5** hold for every i ,
- (c) the equalities **Sp3,4** hold up to $O(1)$ as i varies,
- (d) the maps $H_{\mathcal{F}_{\text{ord}}}^1(E, \mathbf{T}) \otimes_{\Lambda} S \rightarrow H_{\mathcal{F}_S}^1(E, T_S)$ have finite kernels and cokernels, bounded as i varies.

Remark 3.3.2. The reader should keep in mind that the notation $T_S, W_S, \mathcal{F}_S, ? \otimes_{\Lambda} S$, and so on is slightly abusive, since these objects depend not only on the ring S (which will typically remain fixed), but on its structure as a Λ -algebra (which will typically vary). We will continue to suppress this dependence from the notation.

This section is devoted to the proof of the following proposition:

Proposition 3.3.3. *There exists a sequence of specializations converging to \mathfrak{Q} .*

The following result can be deduced from Nekovář's general theory of Selmer complexes [17], (in particular the “duality diagram” of section 0.13), but is also a trivial consequence of the proposition above.

Corollary 3.3.4. *The modules $H_{\mathcal{F}_{\text{ord}}}^1(E, \mathbf{T})$ and X have the same Λ -rank.*

Proof. If S is a specialization with uniformizer π , the Selmer group $H_{\mathcal{F}_S}^1(E, T_S)$ is isomorphic to the π -adic Tate module of $H_{\mathcal{F}_S}^1(E, W_S)$ (using Lemmas 3.5.4 and 3.7.1 of [13]). The claim therefore follows from the existence of a single specialization for which properties **Sp1** and **Sp2** hold. \square

Definition 3.3.5. Let $J \subset \Lambda$ be an ideal, $\phi : \Lambda \rightarrow S$ a specialization, let

$$d(S, J) = \min(\{v(\phi(\lambda)) \mid \lambda \in J\}),$$

where v is the normalized valuation on S . We define the *distance* from S to J to be $p^{-d(S, J)}$ (including the case $d(S, J) = \infty$, in which case the distance is zero).

Remark 3.3.6. The geometric intuition behind the definition is as follows: if one were to replace Λ by a polynomial ring over \mathbf{Q}_p , then J cuts out an algebraic subset $V(J)$ of affine space. Geometrically, a specialization is a point in affine space, and the distance function defined above measures the p -adic distance from this point to $V(J)$.

Lemma 3.3.7. *There is a height-two ideal $J \subset \Lambda$ with the following property: if $\{\phi_i : \Lambda \rightarrow S\}$ is a sequence of specializations (with S fixed), such that as i varies*

- (a) $[S : \phi_i(\Lambda)]$ is bounded above,
- (b) the distance from \mathfrak{Q} to ϕ_i converges to (but is never equal to) zero,
- (c) the distance from J to ϕ_i is bounded away from zero,
- (d) the maps $H_{\mathcal{F}_{\text{ord}}}^1(E, \mathbf{T}) \otimes_{\Lambda} S \rightarrow H_{\mathcal{F}_S}^1(E, T_S)$ have finite and uniformly bounded kernels and cokernels,

then ϕ_i converges to \mathfrak{Q} .

Proof. Fix pseudo-isomorphisms

$$(13) \quad \begin{aligned} H_{\mathcal{F}_{\text{ord}}}^1(E, \mathbf{T}) &\rightarrow \Lambda^{r_1} \\ X &\rightarrow \Lambda^{r_0} \oplus B \oplus C \\ \mathbf{L}_c &\rightarrow \Lambda^{r_1-1} \oplus B' \oplus C' \end{aligned}$$

such that B and C are direct sums of torsion, cyclic Λ -modules, with the characteristic ideal of B a power of \mathfrak{Q} , the characteristic ideal of C prime to \mathfrak{Q} , and similarly for B' and C' .

Let $J \subset \Lambda$ be any height two ideal such that

- (a) J annihilates the kernels and cokernels of the above pseudo-isomorphisms
- (b) $J \subset \mathfrak{Q} + \text{char}(C)$
- (c) $J \subset \mathfrak{Q} + \text{char}(C')$

and let $\phi_i : \Lambda \rightarrow S$ be a sequence of specializations satisfying the hypotheses of the Lemma. The condition that the distance from ϕ_i to J is bounded below guarantees that the maps obtained by tensoring the maps of (13) with ϕ_i have finite kernels and cokernels, bounded as i varies. Indeed, if U and V denote the kernel and cokernel of any one of (13), the kernel and cokernel of the map tensored with S are controlled by $U \otimes S$, $V \otimes S$, and $\text{Tor}_\Lambda^1(V, S)$. The number of generators of these modules does not depend on the map ϕ_i , and the assumption that ϕ_i is bounded away from J gives a nonzero element of S , independent of i , which annihilates all of these modules.

It follows that the S -rank of $H_{\mathcal{F}_{\text{ord}}}^1(E, \mathbf{T}) \otimes S$ is equal to r_1 , the Λ -rank of $H_{\mathcal{F}_{\text{ord}}}^1(E, \mathbf{T})$. This, together with the fourth hypothesis of the Lemma, verifies property **Sp1**. The second condition defining J , together with the assumption that the distance from ϕ_i to \mathfrak{Q} goes to zero, implies that the distance from ϕ_i to $\text{char}(C)$ is bounded below. Therefore $C \otimes S$ is finite and bounded as i varies. Writing $B \cong \bigoplus \Lambda/\mathfrak{Q}^{e_k}$, we have that $B \otimes S \cong \bigoplus S/\phi_i(\mathfrak{Q})^{e_k} S$ is a torsion S -module and

$$\text{length}_S(B \otimes S) = \left(\sum e_k \right) \text{length}_S(S/\phi_i(\mathfrak{Q})S).$$

Thus $X \otimes S$ is an S -module of rank r_0 whose torsion submodule has length

$$\text{ord}_{\mathfrak{Q}}(\text{char}(X_{\Lambda\text{-tors}})) \cdot \text{length}_S(S/\phi_i(\mathfrak{Q})S)$$

up to $O(1)$ as i varies. Applying Lemmas 3.2.11 and 3.2.12 and dualizing, we see that **Sp2** holds, and that the equality **Sp3** holds up to $O(1)$ as i varies.

Exactly as above, $\mathbf{L}_c \otimes S$ is an S -module of rank $r_1 - 1$ and length

$$\text{ord}_{\mathfrak{Q}}(\text{char}(\mathbf{L}_c)) \cdot \text{length}_S(S/\phi_i(\mathfrak{Q})S)$$

up to $O(1)$ as i varies. In the exact sequence

$$(\Lambda \cdot c) \otimes S \rightarrow H_{\mathcal{F}_{\text{ord}}}^1(E, \mathbf{T}) \otimes S \rightarrow \mathbf{L}_c \otimes S \rightarrow 0$$

the second and third modules have S -rank r_1 and $r_1 - 1$, respectively, and so the first arrow must be an injection. The remaining properties now follow from the fourth hypothesis of the Lemma. \square

The difficulty lies in producing a sequence of specializations for which hypothesis (d) holds.

Lemma 3.3.8. *Let S be the ring of integers of a finite extension of $\Phi_{\mathfrak{p}}$, and let M be a finitely generated $S[[x_1, \dots, x_r]]$ -module. For all but finitely many $\alpha \in \mathfrak{m} = \mathfrak{m}_S$, $M[x_r - \alpha]$ is a torsion S -module and a pseudo-null $S[[x_1, \dots, x_r]]$ -module.*

Proof. The module $M[x_r - \alpha]$ is pseudo-null whenever $x_r - \alpha$ does not divide the characteristic ideal of the $S[[x_1, \dots, x_r]]$ -torsion submodule of M , and so this condition causes no difficulty.

For the S -torsion condition, first suppose that M has no S -torsion. Recall that a prime ideal of $S[[x_1, \dots, x_r]]$ is said to be an *associated prime* of M if it is the exact annihilator of some $m \in M$. By the theory of primary decomposition, M has only finitely many associated primes, and $M[x_r - \alpha]$ is trivial unless $x_r - \alpha$ is contained in some associated prime. If \mathfrak{Q} is an associated prime of M with $(x_r - \alpha)$ and $(x_r - \beta)$ both contained in \mathfrak{Q} , then $\alpha - \beta$ is contained in \mathfrak{Q} . By the definition of an associated prime, M has a submodule isomorphic to $S[[x_1, \dots, x_r]]/\mathfrak{Q}$, and so $S[[x_1, \dots, x_r]]/\mathfrak{Q}$ can have no S -torsion. Therefore $\alpha = \beta$, and so for every associated prime there is at most one α for which $x_r - \alpha$ is contained in that prime.

The case of arbitrary M now follows easily from the exactness of

$$0 \rightarrow M_{S\text{-tors}}[x_r - \alpha] \rightarrow M[x_r - \alpha] \rightarrow (M/M_{S\text{-tors}})[x_r - \alpha].$$

□

We are now ready to begin the proof of Proposition 3.3.3. Let J be as in Lemma 3.3.7, and let $\phi : \Lambda \rightarrow S$ be a specialization such that $\phi(Q) = 0$ and such that the distance from S to J is nonzero. We fix an identification $\Lambda \cong \mathcal{O}_{\mathfrak{p}}[[x_1, \dots, x_g]]$ in such a way that $Q(x_1, b_2, \dots, b_g)$ is not identically zero as a power series in x_1 , where $b_i = \phi(x_i)$ for $1 \leq i \leq g$. By Hensel's lemma, for every i there is an open neighborhood $U_i \subset \mathfrak{m}$ of b_i , such that for any $\beta_i \in U_i$, the subring $\mathcal{O}_{\mathfrak{p}}[\beta_i] \subset S$ is equal to $\mathcal{O}_{\mathfrak{p}}[b_i]$. Hence if $\beta \in U_1 \times \dots \times U_g$, the map $\phi^\beta : \Lambda \rightarrow S$ taking $x_i \mapsto \beta_i$, determines a specialization of Λ .

For $0 \leq r \leq g$ define $\Lambda_r = S[[x_1, \dots, x_r]]$. For $\beta \in U$, sending $x_i \mapsto \beta_i$ for $r+1 \leq i \leq g$ determines a map $\Lambda \rightarrow \Lambda_r$. When we view Λ_r as a Λ -algebra in this way, we will write Λ_r^β to emphasize the dependence on β . Composing these maps with the character $G_E \rightarrow \Lambda^\times \xrightarrow{\iota} \Lambda^\times$, we obtain characters $\chi_r : \text{Gal}(E^\Sigma/E) \rightarrow (\Lambda_r^\beta)^\times$. Set

$$\mathbf{T}_r^\beta = T_{\mathfrak{p}}(A) \otimes_{\mathcal{O}_{\mathfrak{p}}} \Lambda_r^\beta$$

with $\text{Gal}(E^\Sigma/E)$ acting on both factors, and for each prime \mathfrak{q} dividing \mathfrak{p} define $\mathbf{T}_r^{\beta\pm} = T_{\mathfrak{p}}(A)^\pm \otimes \Lambda_r^\beta$. Sending $x_r \mapsto \beta_r$ determines a Λ -algebra map $\Lambda_r^\beta \rightarrow \Lambda_{r-1}^\beta$, which induces the exact sequence

$$0 \rightarrow \mathbf{T}_r^\beta \xrightarrow{x_r - \beta_r} \mathbf{T}_r^\beta \rightarrow \mathbf{T}_{r-1}^\beta \rightarrow 0$$

and similarly with \mathbf{T} replaced by \mathbf{T}^\pm . Set

$$L_r^\beta = \bigoplus_{\mathfrak{q}|\mathfrak{p}} H^1(E_{\mathfrak{q}}, \mathbf{T}_r^{\beta-}) \oplus \bigoplus_v H^1(\mathcal{I}_v, \mathbf{T}_r^\beta)$$

where the second sum is over all $v \in \Sigma$ not dividing \mathfrak{p} , and \mathcal{I}_v is the inertia subgroup of $\text{Gal}(\bar{E}_v/E_v)$. We define generalized Selmer groups H_r^β by the exactness of

$$0 \rightarrow H_r^\beta \rightarrow H^1(E^\Sigma/E, \mathbf{T}_r^\beta) \rightarrow L_r^\beta.$$

Remark 3.3.9. The Λ -algebra Λ_r^β depends only on the coordinates β_i with $i > r$, and similarly for \mathbf{T}_r^β and H_r^β .

Lemma 3.3.10. Fix $1 \leq r \leq g$, and suppose we are given $\beta_i \in \mathfrak{m}$ for $i > r$. For all but finitely many $\beta_r \in \mathfrak{m}$, the map $\mathbf{T}_r^\beta \rightarrow \mathbf{T}_{r-1}^\beta$ induces a map

$$H_r^\beta \otimes_{\Lambda_r^\beta} \Lambda_{r-1}^\beta \rightarrow H_{r-1}^\beta$$

with S -torsion kernel and cokernel. If $r = 1$, there is a subset $V \subset \mathfrak{m}$ of finite complement such that kernel and cokernel are finite and bounded as β_1 ranges over V .

Proof. Let M_r^β denote the image of $H^1(E^\Sigma/E, \mathbf{T}_r^\beta) \rightarrow L_r^\beta$ and consider the commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & H_r^\beta & \longrightarrow & H^1(E^\Sigma/E, \mathbf{T}_r^\beta) & \longrightarrow & M_r^\beta & \longrightarrow & 0 \\ & & \downarrow x_r - \beta_r & & \downarrow x_r - \beta_r & & \downarrow x_r - \beta_r & & \\ 0 & \longrightarrow & H_r^\beta & \longrightarrow & H^1(E^\Sigma/E, \mathbf{T}_r^\beta) & \longrightarrow & M_r^\beta & \longrightarrow & 0 \\ & & \downarrow \mu & & \downarrow \nu & & \downarrow \xi & & \\ 0 & \longrightarrow & H_{r-1}^\beta & \longrightarrow & H^1(E^\Sigma/E, \mathbf{T}_{r-1}^\beta) & \longrightarrow & M_{r-1}^\beta & \longrightarrow & 0 \end{array}$$

in which all rows and the middle column are exact. Viewing this as an exact sequence of vertical complexes and taking cohomology, the kernel of

$$H_r^\beta / (x_r - \beta_r) H_r^\beta \xrightarrow{\mu} H_{r-1}^\beta$$

is isomorphic to the cokernel of

$$H^1(E^\Sigma/E, \mathbf{T}_r^\beta)[x_r - \beta_r] \rightarrow M_r^\beta[x_r - \beta_r],$$

and so is S -torsion for all but finitely many choices of β_r by Lemma 3.3.8. Furthermore, in the case $r = 1$, $M_r^\beta[x_1 - \beta_1]$ is bounded by the order of the maximal pseudo-null (hence finite) submodule of M_r^β .

The cokernel of μ is bounded in terms of the cokernel of ν and the kernel of

$$(14) \quad M_r^\beta / (x_r - \beta_r) M_r^\beta \xrightarrow{\xi} M_{r-1}^\beta.$$

The cokernel of ν is isomorphic to the $x_r - \beta_r$ torsion in $H^2(E^\Sigma/E, \mathbf{T}_r^\beta)$, which is again controlled by Lemma 3.3.8. The middle column of

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M_r^\beta & \longrightarrow & L_r^\beta & \longrightarrow & M_r^\beta / L_r^\beta & \longrightarrow & 0 \\ & & \downarrow x_r - \beta_r & & \downarrow x_r - \beta_r & & \downarrow x_r - \beta_r & & \\ 0 & \longrightarrow & M_r^\beta & \longrightarrow & L_r^\beta & \longrightarrow & M_r^\beta / L_r^\beta & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & M_{r-1}^\beta & \longrightarrow & L_{r-1}^\beta & \longrightarrow & M_{r-1}^\beta / L_{r-1}^\beta & \longrightarrow & 0 \end{array}$$

is exact, and as above the kernel of (14) is isomorphic to the cokernel of

$$L_r^\beta[x_r - \beta_r] \rightarrow (M_r^\beta / L_r^\beta)[x_r - \beta_r],$$

Again this is controlled by Lemma 3.3.8. \square

Lemma 3.3.11. *For $0 \leq r \leq g$, there is a dense subset $\Delta_r \subset U_{r+1} \times \cdots \times U_g$ such that for $\beta \in U_1 \times \cdots \times U_r \times \Delta_r$, the map $\mathbf{T}_g^\beta \rightarrow \mathbf{T}_r^\beta$ induces a map*

$$H_g^\beta \otimes_{\Lambda_g^\beta} \Lambda_r^\beta \rightarrow H_r^\beta$$

with S -torsion kernel and cokernel.

Proof. An easy induction using the preceding lemma. \square

The power series $Q(x_1, b_2, \dots, b_g) \in S[[x_1]]$ is not identically zero by assumption and has a zero in \mathfrak{m} , namely b_1 . Using the Weierstrass preparation theorem and Hensel's lemma, we see that if we replace b_2, \dots, b_g by sufficiently nearby points β_2, \dots, β_g , then $Q(x_1, \beta_2, \dots, \beta_g)$ has a zero, β_1 , which is as close as we like to b_1 . Replacing b by a nearby solution to $Q(x_1, \dots, x_g) = 0$, we henceforth assume that $b \in U_1 \times \Delta_1$. Define a sequence of specializations $\phi_i : \Lambda \rightarrow S$ by

$$\phi_i(x_r) = \begin{cases} b_1 + p^i & \text{if } r = 1 \\ b_r & \text{if } r > 1. \end{cases}$$

We shall always assume that i is chosen large enough that $b_1 + p^i \in U_1$ and that $\phi_i(Q) \neq 0$, the second being possible since, by Weierstrass preparation, the function $Q(x_1, b_2, \dots, b_g)$ has only finitely many zeros in \mathfrak{m} . Also, the distance from ϕ_i to J converges to the (nonzero) distance from ϕ to J , and so the sequence satisfies conditions (a)–(c) of Lemma 3.3.7. We let $\beta(i) \in \mathfrak{m}^g$ be the point with coordinates $\phi_i(x_1), \dots, \phi_i(x_g)$, and set ourselves to the task of showing that the sequence ϕ_i satisfies condition (d) of Lemma 3.3.7.

Lemma 3.3.12. *Let $\beta = \beta(i)$ for $i \gg 0$. The map $\mathbf{T}_g^\beta \rightarrow \mathbf{T}_0^\beta$ induces a map*

$$H_g^\beta \otimes_{\Lambda_g^\beta} \Lambda_0^\beta \rightarrow H_0^\beta$$

with finite kernel and cokernel, bounded as i varies.

Proof. By choice of β_2, \dots, β_g (which do not vary with i), the map

$$H_g^\beta \otimes_{\Lambda_g^\beta} \Lambda_1^\beta \rightarrow H_1^\beta$$

has S -torsion kernel and cokernel. Furthermore, by Remark 3.3.9, the number of generators (as Λ_1^β -modules) and the annihilators (as S -modules) of the kernel and cokernel do not vary with i . Consequently, tensoring this map with $\Lambda_0^\beta \cong S$, the kernel and cokernel of

$$H_g^\beta \otimes_{\Lambda_g^\beta} \Lambda_0^\beta \rightarrow H_1^\beta \otimes_{\Lambda_1^\beta} \Lambda_0^\beta$$

are finite and bounded as i varies. By the final claim of Lemma 3.3.10, the map

$$H_1^\beta \otimes_{\Lambda_1^\beta} \Lambda_0^\beta \rightarrow H_0^\beta$$

has finite kernel and cokernel, bounded as i varies, and the claim is proven. \square

Lemma 3.3.13. *Let $\beta = \beta(i)$, and $\phi = \phi_i : \Lambda \rightarrow S$ the associated specialization. Identifying $\Lambda_0^\beta = S$, $H_0^\beta \subset H_{\mathcal{F}_S}^1(E, T_S)$ with finite index, bounded as i varies.*

Proof. Let

$$L_S = \bigoplus_{\mathfrak{q}|\mathfrak{p}} H^1(E_{\mathfrak{q}}, V_S^-) \oplus \bigoplus_v H^1(\mathcal{I}_v, V_S)$$

where the second sum is over all $v \in \Sigma$ not dividing \mathfrak{p} . The map $T_S \rightarrow V_S$ induces a map $L_0^\beta \rightarrow L_S$, and so from the definitions we have the commutative diagram with exact rows

$$\begin{array}{ccccccc} 0 & \longrightarrow & H_0^\beta & \longrightarrow & H^1(E^\Sigma/E, T_S) & \longrightarrow & L_0^\beta \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & H_{\mathcal{F}_S}^1(E, T_S) & \longrightarrow & H^1(E^\Sigma/E, T_S) & \longrightarrow & L_S \end{array}$$

and so it suffices to bound the kernel of $L_0^\beta \rightarrow L_S$. If \mathfrak{q} divides \mathfrak{p} , the kernel of $H^1(E_{\mathfrak{q}}, T_S^-) \rightarrow H^1(E_{\mathfrak{q}}, V_S^-)$ is bounded by the order of $H^0(E_{\mathfrak{q}}, W_S^-)$. Let w be a place of E_∞ above \mathfrak{q} . It clearly suffices to bound the order of $H^0(E_{\infty, w}, W_S^-)$, but as a module over the absolute Galois group of $E_{\infty, w}$ we have $W_S^- \cong \tilde{A}[\mathfrak{P}^\infty] \otimes_{\mathcal{O}_{\mathfrak{p}}} S$, where S has trivial Galois action and \tilde{A} is the reduction of A at \mathfrak{q} . It therefore suffices to show that $H^0(E_{\infty, w}, \tilde{A}[\mathfrak{P}^\infty])$ is finite. Since $\tilde{A}[\mathfrak{P}^\infty]$ is cofree of rank one over $\mathcal{O}_{\mathfrak{p}}$, if this is not the case then all of $\tilde{A}[\mathfrak{P}^\infty]$ is fixed by the Galois group of $E_{\infty, w}$. But since $\tilde{A}[\mathfrak{P}^\infty]$ is unramified over $E_{\mathfrak{q}}$ and $E_{\infty, w}/E_{\mathfrak{q}}$ is totally ramified, we must have

$$H^0(E_{\infty, w}, \tilde{A}[\mathfrak{P}^\infty]) = H^0(E_{\mathfrak{q}}, \tilde{A}[\mathfrak{P}^\infty]).$$

The right hand side is finite.

Similarly, the kernel of $H^1(\mathcal{I}_v, T_S) \rightarrow H^1(\mathcal{I}_v, V_S)$ is isomorphic to quotient of $H^0(\mathcal{I}_v, W_S)$ by its maximal S -divisible submodule, which is finite. Since \mathcal{I}_v acts trivially on Λ , it also acts trivially on $S \cong \Lambda_0^\beta$, regardless of the choice of β , and so the group $H^0(\mathcal{I}_v, W_S)$ does not vary with i . \square

Let $\beta = \beta(i)$ and $\phi : \Lambda \rightarrow S$ the associated specialization. Define $H_{\text{ord}}^{\text{unr}}(\mathbf{T})$ by exactness of

$$0 \rightarrow H_{\text{ord}}^{\text{unr}}(\mathbf{T}) \rightarrow H_{\mathcal{F}_{\text{ord}}}^1(E, \mathbf{T}) \rightarrow \bigoplus_v H^1(E_v, \mathbf{T})/H_{\text{unr}}^1(E_v, \mathbf{T}),$$

where the second sum is over all $v \in \Sigma$ not dividing \mathfrak{p} . By Lemma 3.2.1, the map

$$H_{\text{ord}}^{\text{unr}}(\mathbf{T}) \otimes_{\Lambda} S \rightarrow H_{\mathcal{F}_{\text{ord}}}^1(E, \mathbf{T}) \otimes_{\Lambda} S$$

has finite kernel and cokernel, bounded as i varies. We may identify $\mathbf{T} \otimes_{\mathcal{O}_{\mathfrak{p}}} S \cong \mathbf{T}_g^\beta$ (with G_E acting trivially on S in the left hand side), and this identification induces an isomorphism

$$H_{\text{ord}}^{\text{unr}}(\mathbf{T}) \otimes_{\mathcal{O}_{\mathfrak{p}}} S \cong H_g^\beta$$

(note that neither side depends on β , the right hand side by Remark 3.3.9). This identification, together with the preceding two lemmas, gives a commutative diagram

$$\begin{array}{ccc} H_{\text{ord}}^{\text{unr}}(\mathbf{T}) \otimes_{\Lambda} S & \longrightarrow & H_g^\beta \otimes_{\Lambda_g^\beta} \Lambda_0^\beta \\ \downarrow & & \downarrow \\ H_{\mathcal{F}_{\text{ord}}}^1(E, \mathbf{T}) \otimes_{\Lambda} S & \longrightarrow & H_{\mathcal{F}_S}^1(E, T_S) \end{array}$$

in which the upper horizontal arrow is an isomorphism, and the two vertical arrows have finite kernel and cokernel, bounded as i varies. It follows that the bottom horizontal arrow has finite kernel and cokernel, bounded as i varies.

This concludes the proof of Proposition 3.3.3.

Remark 3.3.14. In the construction of the sequence $\phi_i : \Lambda \rightarrow S$, if one replaces the ideal J by $J \cap J^t$ then the sequence ϕ_i still converges to Ω , and the sequence of dual specializations $\phi_i \circ \iota$ converges to Ω^t .

3.4. The Main Conjecture. We continue to abbreviate

$$X = \mathrm{Hom}_{\mathcal{O}_{\mathfrak{P}}}(H_{\mathcal{F}_{\mathrm{ord}}}^1(E, \mathbf{W}), \mathcal{D}_{\mathfrak{P}}),$$

and by X_{tors} the Λ -torsion submodule of X . Let $H_{\infty} = H_{\infty}(1) \subset H_{\mathcal{F}_{\mathrm{ord}}}^1(E, \mathbf{T})$ be the Λ -module of Section 3.1.

Proposition 3.4.1. *Let $\phi : \Lambda \rightarrow S$ be a specialization such that the image of H_{∞} under $H_{\mathcal{F}_{\mathrm{ord}}}^1(E, \mathbf{T}) \rightarrow H_{\mathcal{F}_S}^1(E, T_S)$ is nonzero. Then $H_{\mathcal{F}_S}^1(E, T_S)$ is a free rank one S -module, and there is an integer d (independent of ϕ) and a finite S -module M_S such that*

$$H_{\mathcal{F}_S}^1(E, W_S) \cong \mathcal{D}_S \oplus M_S \oplus M_S$$

with $\mathrm{length}_S(M_S) \leq \mathrm{length}_S(H_{\mathcal{F}_S}^1(E, T_S)/\phi(p^d H_{\infty}))$.

Proof. This is exactly as in [9], and so we only give a sketch. Fix a family $\{c_m \mid m \in \mathcal{M}_1\}$ as in Proposition 3.1.1. As in Section 2.3, one may apply Kolyvagin's derivative operators to obtain classes

$$\{\kappa'_m \in H^1(E, \mathbf{T}/I_m \mathbf{T}) \mid m \in \mathcal{M}_1\}.$$

Lemma 2.3.4 of [9] asserts that

$$(15) \quad \kappa'_m \in H_{\mathcal{F}_{\mathrm{ord}}(m)}^1(E_v, \mathbf{T}/I_m \mathbf{T}),$$

but the proof breaks down at primes of bad reduction which split completely in E_{∞} . This is corrected as follows: let v be a prime of bad reduction which splits completely in E_{∞} (so in particular v does not divide p or m). Choose d large enough that p^d annihilates the finite group $H^2(E_v, T)$ (for all such choices of v). By the exactness of

$$H^1(E_v, \mathbf{T}) \rightarrow H^1(E_v, \mathbf{T}/I_m \mathbf{T}) \rightarrow H^2(E_v, \mathbf{T})$$

and the fact that $H^2(E_v, \mathbf{T}) \cong H^2(E_v, T) \otimes \Lambda$, we have that $p^d \kappa'_m$ lifts to $H^1(E_v, \mathbf{T})$. By definition of $\mathcal{F}_{\mathrm{ord}}$, (15) now holds with κ'_m replaced by $p^d \kappa'_m$.

By Lemma 3.2.10 the map $\mathbf{T} \rightarrow T_S$ induces everywhere locally a map

$$H_{\mathcal{F}_{\mathrm{ord}}}^1(E_v, \mathbf{T}) \rightarrow H_{\mathcal{F}_S}^1(E_v, T_S),$$

and therefore a map on global cohomology

$$H_{\mathcal{F}_{\mathrm{ord}}(m)}^1(E, \mathbf{T}/I_m \mathbf{T}) \rightarrow H_{\mathcal{F}_S(m)}^1(E, T_S/I_m T_S).$$

The images of the classes $p^d \kappa'_m$ may be modified, as in Theorem 2.3.7, to form a Kolyvagin system for $(T_S, \mathcal{F}_S, \mathcal{L}_1)$, with κ_1 generating $\phi(p^d H_{\infty})$. The claim now follows from Theorem 2.2.2 and Lemma 3.2.8. \square

Theorem 3.4.2. *There are torsion Λ -modules M and $M_{\mathfrak{P}}$ such that \mathfrak{P} does not divide $\mathrm{char}(M)$, $\mathrm{char}(M_{\mathfrak{P}}) = \mathfrak{P}^k$ for some k , and*

$$X_{\mathrm{tors}} \sim M \oplus M \oplus M_{\mathfrak{P}}.$$

Furthermore, M satisfies the functional equation $\mathrm{char}(M) = \mathrm{char}(M)^t$.

Proof. Fix a height-one prime $\mathfrak{Q} \neq \mathfrak{P}\Lambda$ with generator Q and a pseudo-isomorphism

$$X \rightarrow \Lambda^r \oplus B \oplus C$$

with B of the form $\bigoplus \Lambda/\mathfrak{Q}^{e_k}$ and C of the form $\bigoplus_{\Lambda} / f_k \Lambda$ with each $f_k \notin \mathfrak{Q}$. Let $\phi_i : \Lambda \rightarrow S$ be the sequence of specializations converging to \mathfrak{Q} constructed in Section 3.3. In particular ϕ_i satisfy the hypotheses of Lemma 3.3.7, and so (by the proof of the lemma) the map

$$(16) \quad X \otimes_{\Lambda} S \rightarrow S^{r_0} \oplus (B \otimes_{\Lambda} S) \cong S^{r_0} \oplus \bigoplus S/\phi_i(Q)^{e_k} S$$

has finite kernel and cokernel, bounded as i varies. On the other hand, Lemmas 3.2.11 and 3.2.12 give maps

$$(17) \quad X \otimes_{\Lambda} S \rightarrow \text{Hom}_S(H_{\mathcal{F}_S}^1(E, W_S), \mathcal{D}_S)$$

with finite kernel and cokernel, bounded as i varies. The S -torsion submodule of this module has the form $M_S \oplus M_S$ by Proposition 2.2.1 (and Lemma 3.2.8). The maps (16) and (17), restricted to S -torsion, now give maps

$$\begin{aligned} (X \otimes_{\Lambda} S)_{S\text{-tors}} &\rightarrow \bigoplus S/\phi_i(Q)^{e_k} S \\ (X \otimes_{\Lambda} S)_{S\text{-tors}} &\rightarrow M_S \oplus M_S \end{aligned}$$

whose kernels and cokernels remain bounded as i varies. Letting $i \rightarrow \infty$, so that $\phi_i(Q) \rightarrow 0$, some elementary linear algebra shows that each e_k must occur as an exponent an even number of times.

For the functional equation, choose a sequence of specializations $\phi_i : \Lambda \rightarrow S$ converging to \mathfrak{Q} . By Remark 3.3.14 we may do this in such a way that the sequence of dual specializations $\phi^* = \phi_i \circ \iota$ converges to \mathfrak{Q}^t . Applying Proposition 3.2.7 and the definition of convergence (in particular hypothesis (c)), we have

$$\begin{aligned} \text{ord}_{\mathfrak{Q}}(\text{char}(X_{\Lambda\text{-tors}})) \cdot \text{length}_S(S/\phi_i(Q)S) \\ = \text{ord}_{\mathfrak{Q}^t}(\text{char}(X_{\Lambda\text{-tors}})) \cdot \text{length}_S(S/\phi_i^*(Q^t)S) \end{aligned}$$

up to $O(1)$ as i varies. Letting $i \rightarrow \infty$ gives the result. \square

Theorem 3.4.3. *Assume that $h_k(1) \in A(E_k(1))$ has infinite order for some k , then*

- (a) *the Λ -module $H_{\mathcal{F}_{\text{ord}}}^1(E, \mathbf{T})$ is torsion free of rank one,*
- (b) *$X \sim \Lambda \oplus X_{\text{tors}}$,*
- (c) *in the notation of Theorem 3.4.2, $\text{char}(M)$ divides $\text{char}(H_{\mathcal{F}_{\text{ord}}}^1(E, \mathbf{T})/H_{\infty})$.*

Proof. By Proposition 3.1.1, we are assuming that H_{∞} is a free rank one Λ -module. Let c be a generator. By Proposition 3.3.3, there is a specialization $\phi : \Lambda \rightarrow S$ satisfying hypotheses **Sp1,2,5**, and from Proposition 3.4.1 we conclude that $H_{\mathcal{F}_{\text{ord}}}^1(E, \mathbf{T})$ and X have Λ -rank one. Furthermore, $H_{\mathcal{F}_{\text{ord}}}^1(E, \mathbf{T})$ has no Λ -torsion by Proposition 3.2.4.

Now let $\mathfrak{Q} \neq \mathfrak{P}\Lambda$ be a height-one prime of Λ , and let Q generate \mathfrak{Q} . Using Proposition 3.3.3 we choose a sequence of specializations $\phi_i : \Lambda \rightarrow S$ converging to \mathfrak{Q} . Set $\sigma_i = \text{length}_S(S/\phi_i(Q)S)$. By Proposition 3.4.1 the inequality

$$\text{ord}_{\mathfrak{Q}}(\text{char}(X_{\Lambda\text{-tors}})) \cdot \sigma_i \leq 2 \cdot \text{ord}_{\mathfrak{Q}}(\text{char}(H_{\mathcal{F}_{\text{ord}}}^1(E, \mathbf{T})/p^d H_{\infty})) \cdot \sigma_i$$

holds up to $O(1)$ as i varies. As $i \rightarrow \infty$, $\sigma_i \rightarrow \infty$ and (since the factor of p^d does not affect the order of the characteristic ideal at \mathfrak{Q}) the result follows. \square

REFERENCES

- [1] M. Bertolini. Selmer groups and Heegner points in anticyclotomic \mathbf{Z}_p -extensions. *Compositio Mathematica*, 99:153–182, 1995.
- [2] M. Bertolini and H. Darmon. Iwasawa’s Main Conjecture for elliptic curves over anticyclotomic \mathbf{Z}_p -extensions. Preprint, 2001.
- [3] M. Bertolini and H. Darmon. p -adic L -functions of modular elliptic curves. In *Mathematics Unlimited- 2001 and Beyond*. Springer-Verlag, 2001.
- [4] J. Coates and R. Greenberg. Kummer theory for abelian varieties over local fields. *Invent. Math.*, 124:129–174, 1996.
- [5] C. Cornut. Mazur’s conjecture on higher Heegner points. *Invent. Math.*, 148:495–523, 2002.
- [6] M. Flach. A generalisation of the Cassels-Tate pairing. *J. Reine Angew. Math.*, 412:113–127, 1990.
- [7] E. Goren. *Lectures on Hilbert Modular Varieties and Modular Forms*. American Mathematical Society, 2001.
- [8] B. Gross. Kolyvagin’s work on modular elliptic curves. In J. Coates and M. Taylor, editors, *L-functions and Arithmetic*, pages 235–256, 1991.
- [9] B. Howard. The Heegner point Kolyvagin system. To appear in *Comp. Math.*
- [10] V. Kolyvagin. Euler systems. In *The Grothendieck Festschrift, vol. 2*, pages 435–483. Birkhäuser, 1990.
- [11] V. Kolyvagin and D. Logachev. Finiteness of the Shafarevich-Tate group and the group of rational points for some modular abelian varieties. *Leningrad Math. J.*, 1(5):1229–1253, 1990.
- [12] V. Kolyvagin and D. Logachev. Finiteness of III over totally real fields. *Math. USSR Izvestiya*, 39(2):829–853, 1992.
- [13] B. Mazur and K. Rubin. Kolyvagin systems. Memoirs of the AMS no. 799, 2004.
- [14] W. McCallum. Kolyvagin’s work on Shafarevich-Tate groups. In J. Coates and M. Taylor, editors, *L-functions and Arithmetic*, pages 296–316, 1991.
- [15] J. Milne. *Arithmetic Duality Theorems*. Academic Press, 1986.
- [16] J. Nekovář. On the parity of ranks of Selmer groups II. *C.R. Acad. Sci. Paris Sér.1 Math.*, 332:99–104, 2001.
- [17] J. Nekovář. Selmer complexes. *Preprint*.
- [18] B. Perrin-Riou. Fonctions L p -adiques, théorie d’Iwasawa et points de Heegner. *Bull. Soc. Math. France*, 115:399–456, 1987.
- [19] K. Ribet. Galois action on division points of abelian varieties with real multiplication. *American Journal of Mathematics*, 98(3):751–804, 1976.
- [20] K. Rubin. *Euler Systems*. Princeton University Press, 2000.
- [21] G. Shimura. Construction of class fields and zeta functions of algebraic curves. *Annals of Math.*, 85:58–159, 1967.
- [22] G. Shimura. *Introduction to the Arithmetic Theory of Automorphic Functions*. Princeton University Press, 1971.
- [23] G. van der Geer. *Hilbert Modular Surfaces*. Springer-Verlag, 1987.
- [24] M.-F. Vignéras. *Arithmétique des Algèbres de Quaternions*. Number 800 in Lecture Notes in Mathematics. Springer Verlag, 1980.
- [25] S. Zhang. Gross-Zagier formula for GL_2 . *Asia J. Math.* 5:183–290, 2001.
- [26] S. Zhang. Heights of Heegner points on Shimura curves. *Annals of Math.*, 153:27–147, 2001.