HEEGNER POINT KOLYVAGIN SYSTEM AND IWASAWA MAIN CONJECTURE

Xin Wan

Abstract

In this paper we prove an anticyclotomic Iwasawa main conjecture proposed by Perrin-Riou for Heegner points when the global sign is \(-1\), using a recent work of the author on one divisibility of Iwasawa-Greenberg main conjecture for Rankin-Selberg \(p\)-adic \(L\)-functions. As a byproduct we also prove the equality for the above mentioned main conjecture under some local conditions.

1 Introduction

Let \(p \geq 5\) be an odd prime. Let \(E\) be an elliptic curve over \(\mathbb{Q}\) with square free conductor \(N\). Let \(T\) be the \(p\)-adic Tate-module of \(E\) and \(V = T \otimes_{\mathbb{Z}} \mathbb{Q}_p\). Suppose \(E\) has good ordinary reduction at \(p\). Let \(K\) be a quadratic imaginary field where \(p\) and 2 are split. Let \(G_K\) and \(G_\mathbb{Q}\) be the absolute Galois group of \(K\) and \(\mathbb{Q}\). Consider either of the following assumptions:

1. there is at least one prime \(q|N\) non split in \(\mathcal{K}\) and that the global root number of \(E\) over \(\mathcal{K}\) is \(-1\);

2. for each \(q|N\) either \(q\) is split in \(\mathcal{K}\) or \(q\) is ramified and \(E\) has non-split multiplicative reduction at \(q\), and suppose we have at least one such ramified prime. This implies that the root number of \(E\) over \(\mathcal{K}\) is \(-1\).

We fix \(\iota_p : \mathbb{C} \simeq \mathbb{C}_p\) and let \(v\) be the prime of \(\mathcal{K}\) above \(p\) determined by \(\iota_p\). Let \(\bar{v}\) be its conjugation. It is well known that there is a Galois stable 1-dimensional subspace \(V^+ \subset V\) such that the Galois action of \(G_p\) on \(V^+\) is given by the cyclotomic character twisted by an unramified character. Let \(V^- = V/V^+\), \(T^+ = V^+ \cap T\), \(T^- = T/T^+\). By Taniyama-Shimura conjecture [20] we know that \(E\) is associated to a weight 2 cuspidal eigenform with the automorphic representation \(\pi = \pi_f\). Suppose that the representation \(T|_{G_{K}}\) contains \(GL_2(\mathbb{Z}_p)\) (This is needed for the Euler system argument).

Let \(\mathcal{K}_\infty\) be the unique \(\mathbb{Z}_p^2\)-extension of \(\mathcal{K}\) unramified outside \(p\). The complex conjugation \(c\) acts on \(\Gamma := \text{Gal}(\mathcal{K}_\infty/\mathcal{K})\). We let \(\Gamma^\pm\) be the 1-dimensional \(\mathbb{Z}_p\)-space on which \(c\) acts as \(\pm 1\). Let \(\mathcal{K}_\infty^+\) be the \(\mathbb{Z}_p\)-extension of \(\mathcal{K}\) such that \(\text{Gal}(\mathcal{K}_\infty^+/\mathcal{K}) = \Gamma^+\). Take topological generators \(\gamma^\pm\) of \(\Gamma^\pm\). We let \(\mathcal{K}_k\) be the unique subextension of \(\mathcal{K}_\infty^-\) with \(\text{Gal}(\mathcal{K}_k/\mathcal{K}) \simeq \mathbb{Z}/p^k\mathbb{Z}\). Define \(\Lambda_k := \mathbb{Z}_p[[\Gamma_k]],\) \(\Lambda = \Lambda^- = \mathbb{Z}_p[[\Gamma_k^-]]\), This \(\Lambda \simeq \mathbb{Z}_p[[W]]\) by the \(\mathbb{Z}_p\)-map sending \(\gamma^-\) to \(W + 1\). Let \(\Psi_k\) be the composition \(\leftarrow: \Gamma_k \twoheadrightarrow \Lambda_k^x\). Let \(\epsilon : \mathcal{K} \setminus \Lambda_k^x \rightarrow \Lambda_k^x\) be the composition of \(\Psi_k\) with the reciprocity map of class field theory (normalized by the geometric Frobenius). Let \(\mathcal{T}\) be the \(\Lambda\)-adic Galois representation \(\mathcal{T} \otimes_{\mathbb{Z}_p} \Lambda(\Psi)\). Here \(\Lambda(\Psi)\) means the \(\Lambda\)-adic character with Galois action given by \(\Psi\). We define in involution \(\iota : \Lambda \simeq \Lambda\) to be the \(\mathbb{Z}_p\)-morphism sending \((1 + W)\)
to \((1 + W)^{-1}\). Define \(A := \text{Hom}_{\mathbb{Z}_p}(T, \mathbb{Q}_p/\mathbb{Z}_p(1))\) (convention is slightly different from Howard’s). We also define \(\Lambda_K^* = \text{Hom}_{\mathbb{Z}_p}(\Lambda, \mathbb{Q}_p/\mathbb{Z}_p)\) and \(\Lambda^* = \text{Hom}_{\mathbb{Z}_p}(\Lambda, \mathbb{Q}_p/\mathbb{Z}_p)\).

**Selmer Conditions:**

We define some Selmer conditions \((\mathcal{F}, \mathcal{F}_w, \mathcal{F}_v, \mathcal{F}_\bar{v}, \mathcal{v}, \mathcal{v}, \text{str})\) for various Galois representations \(T, T, A\), etc (we write \(T\) for example in the following). Let:

\[
(\mathcal{F})_w = \begin{cases} 
\ker\{H^1(\mathcal{K}_w, T) \to H^1(I_w, T)\}, & w \nmid p \\
\ker\{H^1(\mathcal{K}_w, T) \to H^1(\mathcal{K}_w, T^-)\} & w|p 
\end{cases}
\]

\[
(\mathcal{F}_w)_w = \begin{cases} 
\mathcal{F}_w, & w \nmid \bar{v} \\
0 & w = \bar{v} 
\end{cases}
\]

\[
(\mathcal{F}_v)_w = \begin{cases} 
\mathcal{F}_w, & w \nmid v \\
0 & w = v 
\end{cases}
\]

\[
(\mathcal{F}_\bar{v})_w = \begin{cases} 
\mathcal{F}_w, & w \nmid \bar{v} \\
0 & w = \bar{v} 
\end{cases}
\]

\[
(\mathcal{v})_w = \begin{cases} 
\mathcal{F}_w, & w \nmid \bar{v} \\
0 & w = \bar{v} 
\end{cases}
\]

\[
(\bar{v})_w = \begin{cases} 
\mathcal{F}_w, & w \nmid \bar{v} \\
0 & w = \bar{v} 
\end{cases}
\]

\[
(\text{str})_w = \begin{cases} 
\mathcal{F}_w, & w \nmid \bar{v} \\
0 & w|p 
\end{cases}
\]

We define the local Selmer condition \(\mathcal{F}'\) by replacing the \(w|p\) local conditions for \(\mathcal{F}\) by \(\ker\{H^1(\mathcal{K}_w, T) \to H^1(I_w, T^-)\}\). We also define the local Selmer condition \(\mathcal{v}'\) by replacing the local condition at \(\bar{v}\) by \(\ker\{H^1(\mathcal{K}_{\bar{v}}, T) \to H^1(I_{\bar{v}}, T^-)\}\). We define \(\mathcal{v}'\) similarly.

We define the corresponding Selmer groups \(H^1_{\mathcal{F}}(\mathcal{K}, -)\) to be the inverse image in \(H^1(\mathcal{K}, -)\) of \(\prod_w \mathcal{F}_w\) under the localization map and \(X := H^1_{\mathcal{F}}(\mathcal{K}, A)^*\). We also define Selmer groups for other Selmer conditions in a similar way.

**1.1 Perrin-Riou’s Conjecture**

Let \(\Phi : X_0(N) \to E\) be a modular parameterization given by \([20]\). Let \(\mathcal{K}[n]\) be the ring class field of \(\mathcal{K}\) of conductor \(n\). In \([3]\) he constructed a Kolyvagin system \(\{\kappa_n^{Hg}\}_n\) with \(n\) running over a set of square-free products of degree two primes in \(\mathcal{K}\) and \(\kappa_n^{Hg} \subseteq H^1(\mathcal{K}, T)\). We also adopt Howard’s notation that \(\kappa_1\) being the image of \(\kappa_n^{Hg}\) in \(H^1(\mathcal{K}, T)\). These depend on the choice of \(\Phi\). We refer to \([3]\) for the definition of a Kolyvagin system. He proved the following theorem:

**Theorem 1.1.** \(H^1_{\mathcal{F}}(\mathcal{K}, T)\) is a torsion free rank one \(\Lambda\)-module. There is a torsion \(\Lambda\)-module \(M\) such that \(\text{char}(M) = \text{char}(M)^t\) and a pseudo-isomorphism:

\[
X \sim \Lambda \oplus M \oplus M.
\]

Also, under assumption (2) we have \(\text{char}(M) \supseteq \text{char}(H^1_{\mathcal{F}}(\mathcal{K}, T)/\Lambda \kappa_n^{Hg})\). Under assumption (1) we have the same containment but on as ideals of \(\Lambda \otimes_{\mathbb{Z}_p} \mathbb{Q}_p\).
Howard proved it under the assumption that all primes of $N$ are split in $\mathcal{K}$. However we will see in the next section that it is true under our assumptions as well.

We prove in this paper that it is the case.

**Theorem 1.2.** If assumption (2) is true then

\[
\text{char}_\Lambda(M) = \text{char}_\Lambda(H^1_F(\mathcal{K}, T)/\Lambda^n H^0).
\]

If assumption (1) is true then the above equality holds as ideals of $\Lambda \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$.

In general there should be a Manin constant showing up in the above identity. However by our assumption of square-free conductor such Manin constant is prime to $p$. There should also be a product of local Tamagawa numbers which is again a $p$-adic unit under assumption (2). Our theorem can be interpreted as a Gross-Zagier theoretic Iwasawa main conjecture: [9] proved a formula relating the right hand side with the quotient of the derivative of a two variable $p$-adic $L$-function and some $\Lambda$-adic regulator $R$. Thus our theorem simply states that the torsion part of the Selmer group is given by the derivatives of the $p$-adic $L$-function over $R$.

**Remark 1.3.** Assumption (2) actually implies the anti-cyclotomic $\mu$-invariant is 0 by results of M. Hirsch. Without this assumption there should be a product of local Tamagawa numbers showing up in the anti-cyclotomic main conjecture. In particular the Kolyvagin system argument does not give the sharp bound. We will treat these powers of $p$ in a future joint work with D. Jetchev and C. Skinner.

This conjecture can be proven under a different assumption (basically assuming some local Galois representations being ramified) by W. Zhang [21] combined with results of Howard [10].

### 1.2 Iwasawa Main Conjecture

We also prove a theorem of the 2-variable Iwasawa main conjecture as a byproduct. First we recall here the main result of [19]. As in loc.cit there is a $p$-adic $L$-function $\mathcal{L}_{f,K} \in \text{Frac}\Lambda_K$, such that for a Zariski dense set of arithmetic points $\phi \in \text{Spec}\Lambda_K$ such that $\phi \circ \varepsilon$ is the $p$-adic avatar of a Hecke character $\xi_\phi$ of $\mathcal{K}^\times \setminus \mathbb{A}_\mathcal{K}^\times$ of infinite type $(-\frac{8}{7}, \frac{8}{7})$ for some $k \geq 6$, of conductor $(p^t, p')$ ($t > 0$) at $p$, then:

\[
\phi(\mathcal{L}_{f,K}) = \frac{p^{(k-3)t} \xi_1 \varepsilon_1 \varepsilon_2 \varepsilon_1^{-1} (\varepsilon_2-p^{-t} \xi_1 \varepsilon_1^{-1}) \varepsilon_1 \varepsilon_2 \varepsilon_1^{-1} (\varepsilon_2-p^{-t} \xi_1 \varepsilon_1^{-1})}{(2\pi i)^{2k-1} \Omega_{\mathcal{K}}^{-1}}.
\]

Here $\xi$ is the Gauss sum and $\chi_1, \chi_2$ are characters such that $\pi(\chi_1, \chi_2) \simeq \pi_{f,p}$. We do not know if this $p$-adic $L$-function is in $\Lambda_K$. However we will prove it is the case under the assumptions (2).

On the arithmetic side the local Selmer condition in [19] is the $v'$-one defined here. We make some remarks about the slight difference between the Selmer condition $v$ and $v'$ above. We have the Hochschild-Serre spectral sequence:

\[
0 \to H^1(G_0/I_0, \mathbb{A}^{I_0}) \to H^1(\mathcal{K}, A) \to H^1(I_0, \mathbb{A})^{G_0}
\]

we have $0 \to H^1_{I_0}(\mathcal{K}_0, A) \to H^1_{I_0}(\mathcal{K}, A) \to H^1(G_0/I_0, \mathbb{A}^{I_0})$ where the last term is of finite cardinality. This implies that $\text{ord}_P(H^1_{I_0}(\mathcal{K}, A)^*) = \text{ord}_P(H^1_{I_0}(\mathcal{K}, A, v')^*)$ for all height one primes $P$ of $\Lambda$. 

3
The two variable main conjecture states that:

\[ \text{char}_{\Lambda_K}(X_{f,K,v}) = (\mathcal{L}_{f,K}) \]

Where \( X_{f,K,v} := H^1(K, T \otimes \Lambda_K(\Psi_K) \otimes_{\Lambda_K} \Lambda_K^*) \). The following is the part (ii) of the main theorem of [19].

**Theorem 1.4.** Under assumption (1) we have one containment

\[ \text{char}_{\Lambda_K \otimes \mathbb{Q}_p}(X_{f,K,v}) \subseteq (\mathcal{L}_{f,K}) \]

as fractional ideals of \( \Lambda_K \).

**Remark 1.5.** In loc.cit there is a CM character \( \xi \) of \( K^\times \backslash \mathbb{A}^\times \) showing up. In fact the assumption on \( \xi \) in that part (ii) there exactly means some specialization of the \( p \)-adic L-functions gives the “special value \( L(K,f,1) \)” but this is not an interpolation point since here the CM form is a weight one Eisenstein series which has weight less than \( f \).

Our second main theorem is the following

**Theorem 1.6.** Then under assumption (2) we have \( \mathcal{L}_{f,K} \in \Lambda_K \). Moreover: \( X_{f,K} \) is \( \Lambda_K \)-torsion and

\[ \text{char}_{\Lambda_K}(X_{f,K}) = (\mathcal{L}_{f,K}) \]

Finally we prove the following result which is a stronger form of a result of C.Skinner [17], which has been used as an important ingredient to prove that a majority of elliptic curves satisfy the BSD conjecture.

**Theorem 1.7.** Let \( E/\mathbb{Q} \) be an elliptic curve with square-free conductor \( N \) and \( K \) is an imaginary quadratic field such that \( p \) splits. Suppose the assumption (1) is true. If the Selmer group \( H^1_F(K,E[p^\infty]) \) has corank one. Then the Heegner point \( \kappa_1 \) is not torsion and thus the vanishing order of \( L_K(f,1) \) is exactly one.

**Remark 1.8.** Here by arguing Iwasawa theoretically we can remove the assumption put in [17] that certain localization map at \( p \) is injective.

One may also deduce some results over \( \mathbb{Q} \) by choosing the \( K \) properly as in [17]. We omit the details.

## 2 Known Results

### 2.1 Ben Howard’s Result

In [8] Howard constructed a Kolyvagin system \( \kappa_1^{Hg} \in H^1(K, T) \), and proved the following theorem:

**Theorem 2.1.** \( H^1_F(K, T) \) is a torsion free rank one \( \Lambda \)-module. There is a torsion \( \Lambda \)-module \( M \) such that \( \text{char}(M) = \text{char}(M)^t \) and a pseudo-isomorphism:

\[ X \sim \Lambda \oplus M \oplus M. \]

Also, \( \text{char}(M)|\text{char}(H^1_F(K, T)/\Lambda\kappa_1^{Hg}) \).
Proof. This is essentially [8, theorem 2.2.10] except that we did not assume that all primes dividing $N$ are split in $K$. However our local condition is enough to construct the Heegner points. We refer to [4] for the construction of the Heegner points $\kappa_1^{Hg}$ in the more general case. In [8] Howard used a result of Cornut [3] that the image of certain Heegner point under the trace map of the Galois group $G$ contains the maximal ideal of $L$ which is a multiple of the specialization of the field of $K$. Now Howard’s proof works throughout. The only difference is in lemma 2.3.4 of loc.cit case (ii) we need to take care of non-split primes $v|N$. But then any prime of $\mathcal{K}[n]$ above $v$ splits completely in $\mathcal{K}_k[n]$, the composition of $\mathcal{K}_k$ and $\mathcal{K}[n]$ where $\mathcal{K}[n]$ is the ring class field of conductor $n$ for $n$ a square-free product of inert primes. So the fact that $\kappa_1^{Hg}$ is in the unramified class follows from that the inertial group of $v$ is the same as that for any prime of $\mathcal{K}_\infty[n]$ above $v$. 

\[ \square \]

2.2 Castella’s Formula

Now we recall the result of [2] which generalizes a formula of [1]. There is a big logarithm map $\log_{\omega(E)} : H^1_F(K_v, T) \to \Lambda$ with finite cokernel ([2], note that by the construction there the image is in $\Lambda$ and contains the maximal ideal of $\Lambda$). Moreover there is a quasi-isomorphism $H^1(F_v, T)/H^1_F(K_v, T) \to \Lambda$ with finite cokernel. We write $\mathcal{L}_{f,K}^{BDP}$ for the $p$-adic $L$-function of Bertolini-Darmon-Prasanna [1], which is a multiple of the specialization of $\mathcal{L}_{f,K}$ to $\gamma^+ \to 1$.

**Definition 2.2.** Let $P$ be a height one prime of $\Lambda$. We consider the maps: $H^1_F(K_v, T)_P \to H^1_F(K_v, T)_P$ and $H^1_F(K_v, T)_P \to H^1_F(K_v, T)_P$. These are maps of free $\Lambda_P$-modules of rank 1. Moreover we are going to know that these maps are non-zero. We define the numbers $f_{v,P}$ and $f_{v,P}$ to be the orders of $P$ of the cokernels of the corresponding maps above.

The following proposition is proved in [2].

**Proposition 2.3.** Under assumption (2) we have

$$\mathcal{L}_{f,K}^{BDP} = \log^2_{\omega(E)}(\kappa_1^{Hg}).$$

Under assumption (1) the above is true up to multiplying by some powers of $p$.

In fact in [2] the result is not stated in such generality since he only uses Heegner points on modular curves. However if we use Heegner points on general indefinite Shimura curves the proof goes in the completely same way (in the proof in loc.cit the two ingredients are the Waldspurger formula and the big logarithm map deduced from [12]). There should also be a modular degree factor showing up. Under assumption (2) this degree is co-prime to $p$ by the square-free conductor assumption and that the Heegner points come from the modular form. But under assumption (1) the formula is only true up to scaling.

**Corollary 2.4.** For any height one prime $P$ of $\Lambda$, we have under assumption (2)

$$\text{ord}_P(\mathcal{L}_{p,f,K}^{BDP}) = 2f_{v,P} + 2\text{ord}_P(H^1_F(K_v, T)/\kappa_1^{Hg}).$$

Under assumption (1) the above is true for all $P \neq (p)$. 

5
Proof. We consider the map:

$$0 \to H^1_F(K, T)_P \to H^1_F(K_v, T)_P \to \Lambda_P$$

of $\Lambda_P$-modules. Here the last is the $\log_{\omega_E}$ map. The corollary is clear.

3 Proof of the Main Results

3.1 Tate Local Duality

Let $K$ be a finite extension of $\mathbb{Q}_p$. Let $V^* := \text{Hom}_{\mathbb{Q}_p}(V, \mathbb{Q}_p(1))$. The pairing $V \times V^* \to \mathbb{Q}_p(1)$ gives a perfect pairing (see [16, 1.4]):

$$H^1(K, V) \otimes H^1(K, V^*) \to H^2(K, \mathbb{Q}_p(1)) \simeq \mathbb{Q}_p.$$

We also have a perfect pairing:

$$H^1(K, T) \times H^1(K, T^* \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p) \to H^2(K, \mathbb{Q}_p/\mathbb{Z}_p(1)) \simeq \mathbb{Q}_p/\mathbb{Z}_p.$$

We usually write $F^*$ for the dual Selmer conditions by requiring $F^*_w$ is the orthogonal complement of $F_w$ under the local Tate pairing.

3.2 Control of Selmer Groups

We first recall some notion of Greenberg [6] about control theorems for Selmer groups. Let $F$ be an extension of $K$ ($K$ or $K_{\infty}$ in application) and $F_{\infty}$ is an extension of $F$ such that the Galois group is isomorphic to $\Gamma = \mathbb{Z}_p^d$ for some $d$. We have the following diagram:

$$
\begin{array}{cccccc}
0 & \to & H^1_v(F, E[p^\infty]) & \to & H^1(F, E[p^\infty]) & \to & \mathcal{G}_E(F) & \to & 0 \\
& & s \downarrow & & h \downarrow & & g \downarrow & & \\
0 & \to & H^1_v(F_{\infty}, E[p^\infty])^\Gamma & \to & H^1(F_{\infty}, E[p^\infty])^\Gamma & \to & \mathcal{G}_E(F_{\infty})^\Gamma & & \\
\end{array}
$$

Where

$$\mathcal{G}_E(M) = \text{Im}(H^1(M, E[p^\infty]) \to \mathcal{P}_E(M))$$

and

$$\mathcal{P}_E(M) = \prod_{\eta \nmid p} H^1(M_\eta, E[p^\infty])/H^1_v(M_\eta, E[p^\infty]) \prod_{\eta \nmid \bar{v}} H^1_v(G_\eta, E[p^\infty]).$$

For any prime $w$ of $F$ let $r_w$ be the map

$$H^1(F_w, E[p^\infty])^\Gamma / H^1_v(F_w, E[p^\infty]) \to H^1(F_{\infty,w}, E[p^\infty])^\Gamma / H^1_v(F_{\infty,w}, E[p^\infty]).$$

By the snake lemma we have

$$0 \to \ker s \to \ker h \to \ker g \to \coker s \to \coker h.$$
**Proposition 3.1.** Under assumption (1) there is an isomorphism $X_{f,K,v}/I \simeq X_{fK,v}^{anti}$ of $\Lambda$-modules. Under assumption (2) the above equality is true as ideals of $\Lambda$-modules.

**Proof.** We consider the above discussion with $F = K_\infty^-$ and $F = K_\infty$. We need to study the kernel and cokernel of $s$. First note that $\ker h = 0$ and $\coker h = 0$ (see [loc.cit] lemma 3.2]). So $\ker s = 0$. We need to study $\ker(g)$. For any prime $w$ of $K$ split in $K/\mathbb{Q}$ (allowed to divide $p$) and primes $w^-$ of $K^- \subset K$ and $w_\infty$ of $K_\infty$ above it, we have $K^-_{w^-} = K_{w_\infty}$, so the $\ker s = 0$.

At non-split primes $w$ and $w^-$ and $w_\infty$ as above, we have $K^-_{w^-} = K_v$. Since $\mathbb{Q}_\infty \subset K_\infty$. So by the [6 page 74], $\ker(r_{w^-}) \sim c_v^{(p)}$ where $c_v^{(p)}$ is the $p$-part of the Tamagawa number of $E$ at $v$. Under (2) by our assumption about non-split multiplicative reduction this is a $p$-adic unit.

These altogether shows that the two-variable main conjecture implies the one variable anticyclotomic main conjecture.

**Corollary 3.2.** We have under assumption (2)

$$(L_{f,K}^{BDP}) \simeq \mathrm{char}_\Lambda(X_{fK,v}^{anti}).$$

Under assumption (1) the above is true as ideals of $\Lambda \otimes \mathbb{Z}_p \mathbb{Q}_p$.

**Proof.** We already have the result after inverting $p$. The powers of $p$ can be taken care of by note that by [loc.cit] $L_{f,K}^{BDP}$ has $\mu$-invariant $0$.

### 3.3 Galois Cohomology Computations

We say a $\Lambda$-module $M$ is of rank $n$ if $M \otimes \Lambda F_\Lambda$ is dimension $n$ over $F_\Lambda$ ($F_\Lambda$ is the fraction field). As in [13] we define a set of height one primes of $\Lambda$

$$\Sigma_\Lambda := \{ P : \sharp H^2(K_{\Sigma}/K, T)[P] = \infty \} \cup \{ P : \sharp H^2(K_v, T)[P] = \infty \} \cup \{ P : \sharp H^2(K_{\Sigma}, T)[P] = \infty \} \cup \{ P \in \{ P \} \}.$$  

This is a finite set by [13] lemma 5.3.4].

**Proposition 3.3.** (Poitou-Tate exact sequence) We have the following long exact sequence:

$$0 \rightarrow H^1_f(K, T) \rightarrow H^1_G(K, T) \rightarrow H^1_f(K_v, T)/H^1_f(K_v, T) \rightarrow H^1_f(K, A)^* \rightarrow H^1_f(K, A)^* \rightarrow 0.$$  

**Proof.** It follows from [16] Theorem 1.7.3 in a similar way as corollary 1.7.5 in loc.cit.

**Lemma 3.4.**

$$H^1_{str}(K, T) = 0.$$  

**Proof.** We have

$$0 \rightarrow H^1_{str}(K, T) \rightarrow H^1_f(K, T) \rightarrow \oplus_v H^1_f(K_v, T)/H^1_{str}(K_v, T).$$  

We tensor it with $F_\Lambda$. By proposition 2.3 the image of $\kappa_{H^1} \in H^1_f(K_v, T)$ in $H^1_f(K_v, T)$ is the $p$-adic $L$-function of Bertolini-Darmon-Prasanna, which is non zero by the result of [loc.cit]. Since $H^1_f(K, T)$ is rank one, $H^1_{str}(K, T)$ must be of rank $0$. We know that $H^1(K, T)$ is torsion free as remarked in [8 lemma 2.2.9]. So $H^1_{str}(K, T)$ is $0$.  

\[ \square \]
Lemma 3.5. $H^1(\mathcal{K}, \mathbf{T})$ and $H^1(\mathcal{K}, \Lambda)^*$ have the same $\Lambda$-rank.

Proof. We need only to prove that for a generic set of height one prime $P$, $H^1(\mathcal{K}, \mathbf{T})/P$ and $H^1(\mathcal{K}, \Lambda)^*/P^\ast$ have the same $\mathbb{Z}_p$-rank. For any height one prime $\mathfrak{q}$ we define $S_{\mathfrak{q}}$ to be the integral closure of $\Lambda/\mathfrak{q}$ and $T_{\mathfrak{q}}$ to be the Galois representation obtained by $T/\mathfrak{q}T$ base changed to $S_{\mathfrak{q}}$. Let $\Phi_{\mathfrak{q}}$ be the fraction field of $S_{\mathfrak{q}}$ and $A_{\mathfrak{q}}$ the base change of $T_{\mathfrak{q}}$ to $\Phi_{\mathfrak{q}}/S_{\mathfrak{q}}$. Suppose $P \notin \Sigma_{\Lambda}$ and $g_P$ be a generator of $P$. From:

$$0 \to T \to T \to T/P \to 0$$

where the second arrow is given by multiplication by $g_P$. We have:

$$H^1(\mathcal{K}, T)/P \hookrightarrow H^1(\mathcal{K}, T/P) \to H^2(\mathcal{K}, T)[P].$$

From

$$0 \to \Lambda[P^\ast] \to \Lambda \to \Lambda \to 0$$

we have

$$H^0(\mathcal{K}, \Lambda) \to H^1(\mathcal{K}, \Lambda[P^\ast]) \to H^1(\mathcal{K}, \Lambda)[P^\ast].$$

Note that $H^0(\mathcal{K}, \Lambda)$ has finite cardinality. On the other hand we have:

$$H^1(\mathcal{K}, T/P) \to H^1(\mathcal{K}, T_P)$$

$$H^1(\mathcal{K}, \Lambda_{P^\ast}) \to H^1(\mathcal{K}, \Lambda[P^\ast])$$

both have finite kernel and cokernel since $P \notin \Sigma_{\Lambda}$, by [3] Lemma 2.2.7. Also $H^1(\mathcal{K}, T_P)$ is the $\mathfrak{m}_P$-adic Tate module of $H^1(\mathcal{K}, \Lambda_{P^\ast})$. So the $\mathbb{Z}_p$-rank of $H^1(\mathcal{K}, T)/P$ is the $\mathbb{Z}_p$-corank of $H^1(\mathcal{K}, \Lambda[P^\ast])$ and we are done.

Corollary 3.6. $H^1(\mathcal{K}, T)$ has rank 2 and $H^1_{str}(\mathcal{K}, \Lambda)^*$ is $\Lambda$-torsion.

Proof. This follows from the Poitou-Tate long exact sequence and the above lemma, by noting that $H^1_{str}(\mathcal{K}, \Lambda)^*$ is a quotient of $H^1_{\mathfrak{F}}(\mathcal{K}, \Lambda)^*$ and thus has rank not greater than one.

Lemma 3.7. We have exact sequence:

$$0 \to H^1_{\mathfrak{F}}(\mathcal{K}, T) \to H^1_{\mathfrak{F}}(\mathcal{K}, T) \to \text{coker} \to 0$$

where coker has finite cardinality.

Proof. We first claim that $H^1_{\mathfrak{F}}(\mathcal{K}, T)$ is a rank 1 $\Lambda$-module. This follows from a $\Lambda$-adic analogue of the argument [L7] lemma 2.3.2]. By the above lemma $H^1(\mathcal{K}, T)$ has rank 2. We consider the image of $H^1(\mathcal{K}, T)/H^1_{\mathfrak{F}}(\mathcal{K}, T) \hookrightarrow \oplus_v H^1(\mathcal{K}_v, T)/H^1_{\mathfrak{F}}(\mathcal{K}_v, T)$. It is of rank 1 over $\Lambda$, and is invariant under $\iota \circ c$ (c is the complex conjugation). If $H^1_{\mathfrak{F}}(\mathcal{K}, T)$ is rank 2 then we get that the above image is rank 2, a contradiction.

Recall we have $H^1(\mathcal{K}_v, T)/H^1_{\mathfrak{F}}(\mathcal{K}_v, T) \hookrightarrow H^1(\mathcal{K}_v, T') \to \Lambda$ with finite kernel. By the Poitou-Tate exact sequence, the coker is injected to the torsion part of $H^1(\mathcal{K}_v, T)/H^1_{\mathfrak{F}}(\mathcal{K}_v, T)$, which is finite.

Lemma 3.8. $H^1_{\mathfrak{F}}(\mathcal{K}, T)$ is 0.
Proof. Since $H^1(K, T)$ is torsion free we only need to show $H^1_{\mathcal{F}}(K, T)$ is torsion. Again this follows from a $\Lambda$-adic analogue of [17] [lemma 2.3.2] in a completely same way as the above lemma. □

**Proposition 3.9.** Consider the map $H^1(K_v, T)/H^1_{\mathcal{F}}(K_v, T) \to H^1_{\mathcal{F}^*}(K, A)^*$ which is the Pontryagin dual of the natural map

$$H^1_{\mathcal{F}^*}(K, A) \to H^1_{\mathcal{F}}(K_v, A).$$

Then for any height one prime $P$ of $\Lambda$ as above. We localize the above map at $P$ and compose it with projection to the free-$\Lambda_P$ part of $H^1_{\mathcal{F}}(K, A)_P$. We write this $\Lambda_P$-module map as $j_{P,v}$. Then:

$$\text{ord}_P(\text{coker } j_{P,v}) = f_{v,P}.$$ 

We can define $j_{P,v}$ similarly and have $\text{ord}_P(\text{coker } j_{P,v}) = f_{v,P}$.

The proposition follows from the following lemma:

**Lemma 3.10.** Let $v$ be a prime of $K$ above $p$. Then

$$\text{ord}_P \text{coker } \{H^1_{\mathcal{F}}(K_v, T)_P \to H^1_{\mathcal{F}}(K_v, T)_P\} = \text{ord}_P \text{coker } \{H^1_{\mathcal{F}}(K_v, A)_P \to X_P \to \Lambda_P\}$$

where the last arrow is defined as follows. Recall Howard proved the quasi-isomorphism: $X \to \Lambda \oplus M \oplus M$ with finite kernel and cokernel. That arrow is induced from composing this map with projection to $\Lambda$.

**Proof.** We claim that length$_{\mathbb{Z}_p} H^0(K_v, A)$ is bounded by a constant depending only on $T$. Take $\gamma \in I_v$ such that $\epsilon(\gamma) \not\equiv 1(\text{mod } m)$ take a basis $v_1, v_2$ of $T$ such that the action of $\gamma$ is diagonal

$$\begin{pmatrix} a_\gamma & d_\gamma \\ 0 & 1 \end{pmatrix}.$$ 

Suppose $d_\gamma \not\equiv 1(\text{mod } m)$. Then if $v \in H^0(K_v, A)$, then $v = a_1 v_1$ for some $a_1 \in \Lambda^*$. Moreover by considering the action of $I_v$ we get: $W a_1 = 0$. Also $(a_0 - 1)a_1 = 0$ by considering the action of an element in $H$ which induces the Frobenius modulo $I_v$. The claim is clear.

We follow the idea of [8] Theorem 2.2.10. For any height one prime $P$, if $P$ is not $(p)$ we take a generator $g$ of it. Let $f = g + p^m$ and $\mathfrak{D}$ be the ideal generated by $f$. Then if $m$ is large then we have $\Lambda/P \cong \Lambda/\mathfrak{D}$ as rings (not as $\Lambda$-modules). Thus $\mathfrak{D}$ is a height one prime as well. In the following we use $\approx$ to mean the difference is a contant not depending on $\mathfrak{D}$ and $m$. We write LHS and RHS for the left hand side and right hand side of the equality in the proposition. Then for $p = v\overline{v}$

$$\text{LHS \times } m d$$

$$\approx \text{length}_{\mathbb{Z}_p} \text{coker } \{H^1_{\mathcal{F}}(K_v, T)/\mathfrak{D} \to H^1_{\mathcal{F}}(K_v, T)/\mathfrak{D}\}$$

$$\approx \text{length}_{\mathbb{Z}_p} \text{coker } \{H^1_{\mathcal{F}}(K_v, T_\mathfrak{D}) \to H^1_{\mathcal{F}}(K_v, T_\mathfrak{D})\}$$

Here we used [8] lemma 2.2.7,lemma 2.2.8. We also used that $H^1(K_v, T)/\mathfrak{D} \cong H^1(K_v, T/\mathfrak{D}) \to H^2(K_v, T)/[\mathfrak{D}]$, and the last term is finite whose size is independent of $\mathfrak{D}$ and $m$ by the claim above and Tate duality.

$$\text{RHS \times } m d$$

$$\approx \text{length}_{\mathbb{Z}_p} \text{coker } \{H^1_{\mathcal{F}}(K_v, A)^*/\mathfrak{D}^i \to X/\mathfrak{D} \to \Lambda/\mathfrak{D}^i\}$$

$$\approx \text{length}_{\mathbb{Z}_p} \text{ker } \{\Lambda^*/[\mathfrak{D}^i] \to H^1_{\mathcal{F}}(K_v, A)[\mathfrak{D}^i] \to H^1_{\mathcal{F}}(K_v, A)[\mathfrak{D}^i]\}$$

$$\approx \text{length}_{\mathbb{Z}_p} \text{ker } \{H^1_{\mathcal{F}}(K_v, A)[\mathfrak{D}^i]_{\text{div}} \to H_{\mathcal{F}}(K_v, A)[\mathfrak{D}^i]\}$$

$$\approx \text{length}_{\mathbb{Z}_p} \text{ker } \{H^1_{\mathcal{F}}(K_v, A_\mathfrak{D}^i)_{\text{div}} \to H^1_{\mathcal{F}}(K_v, A_\mathfrak{D}^i)\}$$

9
Here again we used [8, lemma 2.2.7, lemma 2.2.8]. Moreover we need that the kernel of the map $H^1_F(K_v, A[\mathfrak{D}^i]) \to H^1_F(K_v, A)[\mathfrak{D}^i]$ is bounded by some constant depending only on $T$.

Notice that $T_{\mathfrak{D}}$ is the $m$-adic Tate module of $A_{\mathfrak{D}}$. We have $H^1_F(K, T_{\mathfrak{D}}) = \varprojlim H^1_F(K, T_{\mathfrak{D}}/m^i)$ and $H^1_F(K, A_{\mathfrak{D}}) = \varprojlim H^1_F(K, m^{-i}T_{\mathfrak{D}}/T_{\mathfrak{D}})$ (by [8, lemma 1.3.3]). The similar identities are true for the local cohomology groups. So the lemma follows by taking $m$ tends to infinity.

If $P$ is $(p)$, we take the height one prime $\mathfrak{D} = (p + T^m)$ and argue similarly. Although we do not have the isomorphism $\Lambda/P \simeq \Lambda/D$, we do have $S_{\mathfrak{D}} = \Lambda/D$. See [8, Theorem 2.2.10].

**Proposition 3.11.** For a height one prime $P$ of $\Lambda$, we have: $H^1_F(K_v, A)^*$ is $\Lambda$-torsion module and:

$$2\text{ord}_P M + f_{v,P} = \text{ord}_P(H^1_F(K_v, A)^*)$$

**Proof.** In the poitou-Tate exact sequence we take $G^* = F_v$ and $F^*$ to be our $F$. The proposition follows from lemma 3.7 and proposition 3.9.

**Proposition 3.12.** For a height one prime $P$ as above we have: $H^1_v(K, A)^*$ is $\Lambda$-torsion and:

$$2\text{ord}_P(M) + f_{v,P} = \text{ord}_P(H^1_v(K, A)^*)$$

**Proof.** In the Poitou-Tate exact sequence we take $F^*$ to be $v$ and $G^* = F_v$. The proposition follows from the last proposition, lemma 3.7 and lemma 3.8.

Note that we have $f_{v,P} = f_{v,P}$ by considering the complex conjugation of the Galois representation. Thus we in fact proved:

$$2\text{ord}_P(M) + 2f_{v,P} = \text{ord}_P(H^1_v(K, A)^*) \quad (1)$$

Before proving the main theorem, let us prove the following corollary:

**Corollary 3.13.** The 2-variable Selmer module $X_{f,K}$ defined in [19] is $\Lambda$-torsion.

**Proof.** Suppose it is not. Then by the control theorem for Selmer groups the anti-cyclotomic Selmer module with “$v$” Selmer condition at $p$ is not torsion, which contradicts the above proposition.

**Theorem 3.14.** Theorem [12] is true, i.e. under assumption (2) we have

$$\text{char}_\Lambda(M) = \text{char}_\Lambda(H^1_F(K, T)/\Lambda H^1_{Hg}).$$

Under assumption (1) this is true as ideals of $\Lambda \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$.

**Proof.** Fix a height one prime $P$. By [11], corollary 2.4 and corollary 5.2 we have:

$$2\text{ord}_P M + 2f_{v,P} \geq 2\text{ord}_P(H^1_F(K, T)/\Lambda H^1_{Hg}) + 2f_{v,P}.$$

The theorem follows.

Now let us prove the two variable main conjecture.
Theorem 3.15. Suppose assumption (2) is true. Then \( \mathcal{L}_{f, K} \in \Lambda_K \). Moreover:

\[
\text{char}_{\Lambda_K}(X_{f, K}) = (\mathcal{L}_{f, K}).
\]

Remark 3.16. After I finished the first draft B. Howard informed me that Francesc Castella obtained similar results in \([2]\) via a seemingly different proof.

Proof. Let \( \tilde{\mathcal{L}}_{f, K} \) be the \( \mathcal{L}_{f, K} \) multiplied by its denominator (note that \( \Lambda_K \) is uniquely factorable ring) and then remove all \( p \)-power divisors so that \( \tilde{\mathcal{L}}_{f, K} \in \Lambda_K \). By the main theorem of \([19]\) we have the two variable

\[
(\tilde{\mathcal{L}}_{f, K}) \supseteq \text{char}_{\Lambda_K}(X_{f, K})
\]

(note that \( \text{ord}_p(\tilde{\mathcal{L}}_{f, K}) = 0 \)).

Write \( \tilde{\mathcal{L}}^{\text{anti}}_{f, K} \) for \( \tilde{\mathcal{L}}_{f, K} \) evaluated at \( \gamma^+ = 1 \). By \([11]\) \( \mathcal{L}_{f, K}^{\text{BDP}} \) has \( \mu \)-invariant 0. So it is not hard to see from the construction that \( \mathcal{L}_{f, K}^{\text{BDP}} | \tilde{\mathcal{L}}^{\text{anti}}_{f, K} \). Then by Theorem 2.1, corollary 2.4, corollary 3.2 and (1) we already have:

\[
\text{char}_{\Lambda}(X_{f, K})^{\text{anti}} \supseteq (\mathcal{L}_{f, K}^{\text{BDP}}) \supseteq (\tilde{\mathcal{L}}^{\text{anti}}_{f, K})
\]

as ideals of \( \Lambda \). So we deduce that

\[
(\tilde{\mathcal{L}}_{f, K}) = \text{char}_{\Lambda_K}(X_{f, K})
\]

in the same way as \([18] \) Theorem 3.6.5] and all above \( \supseteq \) are \( = \). In particular \( \mathcal{L}_{f, K}^{\text{BDP}} = \tilde{\mathcal{L}}^{\text{anti}}_{f, K} \). By the interpolation property we have \( \tilde{\mathcal{L}}_{f, K} = \mathcal{L}_{f, K} \). This proves the theorem.

Finally we prove the following

Theorem 3.17. Let \( E/\mathbb{Q} \) be an elliptic curve with square-free conductor \( N \) and \( K \) is an imaginary quadratic field such that \( p \)-splits. Suppose moreover assumption (1) is true. If the Selmer group \( H^1_F(K, E[p^\infty]) \) has corank one. Then the Heegner point \( \kappa_1 \) is not torsion and thus the vanishing order of \( L_K(f, 1) \) is exactly one.

Proof. We consider the behavior of specialization of the Selmer group \( H^1_F \) from \( K_{\infty} \) to \( K \). By our discussion on Greenberg’s method in subsection 3.2 we know that the surjection

\[
X_{f, K}/IX_{f, K} \twoheadrightarrow H^1_F(K, E[p^\infty])^*
\]

has finite kernel. By theorem 1.1 and theorem 1.2 we have \( M \otimes \Lambda/I \) and thus \( \frac{H^1_F(K, T)}{\Lambda \kappa_1 H^1} \otimes \frac{\Lambda}{I} \) is torsion. Thus \( \frac{H^1_F(K, T)}{IH^1_F(K, T)} + \Lambda \kappa_1 H^1 \) is torsion. One can easily check that there is an injection

\[
H^1_F(K, T)/IH^1_F(K, T) \hookrightarrow H^1_F(K, T).
\]

Note that the image \( \kappa_1 \) of \( \kappa_1 H^1 \) is not torsion in \( H^1_F(K, T) \). So \( \kappa_1 \) is not torsion.

\[\Box\]
References

[1] Massimo Bertolini, Henri Darmon, and Kartik Prasanna. p-adic Rankin L-series and rational points on CM elliptic curves, Pacific Journal of Mathematics, Vol. 260, No. 2, 2012. pp. 261-303.

[2] Francesc Castella. p-adic L-functions and the p-adic variation of Heegner points, preprint.

[3] Cornut, Christophe. Mazur’s conjecture on higher Heegner points. Inventiones mathematicae 148.3 (2002): 495-523.

[4] Cornut, Christophe, and Vinayak Vatsal. “Nontriviality of Rankin-Selberg L-functions and CM points.” London Mathematical Society Lecture Note Series 320 (2007): 121.

[5] Eischen, M. Harris, J. Li, C. Skinner, p-adic L-functions for Unitary Shimura Varieties (II), preprint 2014.

[6] Greenberg, Ralph. "Iwasawa theory for elliptic curves." Arithmetic theory of elliptic curves. Springer Berlin Heidelberg, 1999. 51-144.

[7] Gross, Benedict H., and Don B. Zagier. “Heegner points and derivatives of L-series." Inventiones mathematicae 84.2 (1986): 225-320.

[8] Howard, B: The Heegner point Kolyvagin system. Compos. Math. 140, 1439C1472(2004)

[9] B. Howard. The Iwasawa theoretic Gross-Zagier theorem. Comp.Math.141, No. 4 (2005),811C846.

[10] B. Howard, Bipartite Euler systems, Journal-ref: J. Reine Angew. Math. 597, (2006), 1-25.

[11] M.-L. Hsieh, Special values of anticyclotomic Rankin-Selberg L-functions. Preprint as of 08/23/12

[12] Loeffler, David, and Sarah Livia Zerbes. “Iwasawa theory and p-adic L-functions over $\mathbb{Z}_p^2$-extensions.” arXiv preprint arXiv:1108.5954 (2011).

[13] B. Mazur and K. Rubin, Kolyvagin systems, Mem. Amer. Math. Soc., vol. 168, no. 799 (American Mathematical Society, Providence, RI, 2004).

[14] Perrin-Riou, Bernadette. “Fonctions $L$ p-adiques, theorie d’Iwasawa et points de Heegner.” Bulletin de la Societe Mathematique de France 115 (1987): 399-456.

[15] B. Perrin-Riou, p-adic $L$-functions and p-adic representations (American Mathematical Society, Providence, RI, 2000).

[16] K. Rubin, Euler systems. Annals of Mathematics Studies 147. Hermann Weyl Lectures. The Institute for Advanced Study. Princeton University Press, Princeton, NJ, 2000.

[17] C. Skinner, A converse of a theorem of Gross, Zagier and Kolyvagin, submitted, 2014.

[18] Skinner, Christopher, and Eric Urban. “The Iwasawa main conjectures for GL_2.” Inventiones mathematicae 195.1 (2014): 1-277.
[19] X. Wan, Iwasawa Main Conjecture for Rankin-Selberg $p$-adic $L$-functions, submitted, 2013.
[20] A. Wiles, Elliptic curves and Fermat’s Last Theorem Ann. of Math. 141, p. 443-551, 1995.
[21] W. Zhang, Selmer groups and the divisibility of Heegner points. preprint, 2013.

XIN WAN, DEPARTMENT OF MATHEMATICS, COLUMBIA UNIVERSITY, NEW YORK, NY, 10027, USA
E-mail Address: xw2295@math.columbia.edu