INDIVISIBILITY OF HEEGNER POINTS AND ARITHMETIC APPLICATIONS
ASHAY A. BURUNGALE, FRANCESC CASTELLA, AND CHAN-HO KIM

Abstract. We upgrade Howard’s divisibility towards Perrin-Riou’s Heegner point main conjecture to the predicted equality. Contrary to previous works in this direction, our main result allows for the classical Heegner hypothesis and non-squarefree conductors. The main ingredients we exploit are W. Zhang’s proof of Kolyvagin’s conjecture, Kolyvagin’s structure theorem for Shafarevich–Tate groups, and the explicit reciprocity law for Heegner points.

Contents
1. Introduction 1
2. Selmer structures 4
3. Heegner point Kolyvagin systems 5
4. Equivalent main conjectures 7
5. Equivalent special value formulas 7
6. Skinner–Urban lifting lemma 9
7. Proof of the main results 9
References 10

1. Introduction

Let \( E/\mathbb{Q} \) be an elliptic curve of conductor \( N \) and let \( K \) be an imaginary quadratic field of discriminant \( D_K \) with \((D_K, N) = 1\). Then \( K \) determines a factorization

\[ N = N^+ N^- \]

with \( N^+ \) (resp. \( N^- \)) divisible only by primes which are split (resp. inert) in \( K \). Throughout this paper, the following hypothesis will be in force:

Assumption 1.1 (Generalized Heegner hypothesis). \( N^- \) is the square-free product of an even number of primes.

Let \( p > 3 \) be a good ordinary prime for \( E \) with \((p, D_K) = 1\), and let \( K_\infty \) be the anticyclotomic \( \mathbb{Z}_p \)-extension of \( K \). Under Assumption 1.1, the theory of complex multiplication provides a collection of CM points on a Shimura curve with “\( \Gamma_0(N^+) \)-level structure” attached to the quaternion algebra \( B/\mathbb{Q} \) of discriminant \( N^- \) defined over ring class extensions of \( K \). By modularity, these points give rise to Heegner points on \( E \) defined over the ring class extensions, and exploiting the \( p \)-ordinarity assumption these can be turn into a norm-compatible system of Heegner points on \( E \) over the \( \mathbb{Z}_p \)-extension \( K_\infty/K \).

Let \( T \) be the \( p \)-adic Tate module of \( E \), and set \( V := T \otimes \mathbb{Q}_p \) and \( \Lambda := V/T \simeq E[p^\infty] \). Let \( \Lambda = \mathbb{Z}_p[\text{Gal}(K_\infty/K)] \) be the anticyclotomic Iwasawa algebra, and let \( T \) and \( \Lambda \) be the \( \Lambda \)-adic
versions of $T$ and $A$, respectively, recalled in Section 2. Let
\[
\text{Sel}_{\text{Gr}}(K, T) \subset \varprojlim \text{H}^1(K_n, T), \quad \text{Sel}_{\text{Gr}}(K, A) \subset \varprojlim \text{H}^1(K_n, A)
\]
be $\Lambda$-adic Greenberg ordinary Selmer groups defined in [How04a, How04b] (and recalled in Section 2 below), where $K_n$ is the unique subextension of $K_\infty$ with $[K_n : K] = p^n$. Letting $\text{Sel}_{p^n}(E/K_n) \subset \text{H}^1(K_n, E[p^n])$ be the $p^n$-th descent Selmer groups fitting into the fundamental exact sequence
\[
0 \rightarrow E(K_n) \otimes \mathbb{Z}/p^n\mathbb{Z} \rightarrow \text{Sel}_{p^n}(E/K_n) \rightarrow \text{III}(E/K_n)[p^n] \rightarrow 0,
\]
there are $\Lambda$-module pseudo-isomorphisms
\[
\text{Sel}_{\text{Gr}}(K, T) \sim \varprojlim \varinjlim \text{Sel}_{p^n}(E/K_n), \quad \text{Sel}_{\text{Gr}}(K, A) \sim \varprojlim \varinjlim \text{Sel}_{p^n}(E/K_n).
\]

Via the Kummer map, the norm-compatible sequence of Heegner points on $E$ along $K_\infty/K$ gives rise to a $\Lambda$-adic Heegner cohomology class $\kappa_1^{\infty} \in \text{Sel}_{\text{Gr}}(K, T)$ which was first shown to be non-torsion by Cornut–Vatsal [CV07]. After Kolyvagin [Kol88], the non-triviality of a Heegner point over a ring class field $H/K$ implies that the Mordell–Weil rank of the underlying abelian variety over $H$ being one and also the finiteness of the corresponding Tate–Shafarevich group, with the index of the Heegner point in the Mordell–Weil group being closely to the size of the Tate–Shafarevich group (essentially, the latter is the square of the former). After Perrin-Riou [PR87, Conj. B] and Howard [How04b], a $\Lambda$-adic analogue of this result takes the form of the following “Heegner point main conjecture”, where we let $\iota: \Lambda \rightarrow \Lambda$ be the involution induced by the inversion in $\text{Gal}(K_\infty/K)$.

**Conjecture 1.2** (Perrin-Riou, Howard). The $\Lambda$-modules $\text{Sel}_{\text{Gr}}(K, T)$ and $\text{Sel}_{\text{Gr}}(K, A)$ have rank 1 and corank 1, respectively. Letting
\[
X = \text{Hom}_{\mathbb{Z}_p}(\text{Sel}_{\text{Gr}}(K, A), \mathbb{Q}_p/\mathbb{Z}_p)
\]
be the Pontrjagin dual of $\text{Sel}_{\text{Gr}}(K, A)$, there is a torsion $\Lambda$-module $M_\infty$ with:

1. $\text{char}(M_\infty) = \text{char}(M_\infty)_\iota$,
2. $X \sim \Lambda \oplus M_\infty \oplus M_\infty$,
3. $\text{char}(M_\infty) = \text{char}\left(\frac{\text{Sel}_{\text{Gr}}(K, T)}{\Lambda M_1^{\infty}}\right)$.

The third statement is a form of Iwasawa main conjecture involving zeta elements which similarly appears in other settings, notably [Rub90, Thm. 5.1] and [Kat04, Conj. 12.10]. Here, we assume that the Manin constant is 1 and that $\mathcal{O}_K = \{\pm 1\}$ for notational simplicity.

1.1. **Main result.** Similarly as in [Zha14, Notations], we consider the following condition on the triple $(E, p, K)$:

**Assumption 1.3** (Condition $\heartsuit$). Denote by $\text{Ram}(\overline{p})$ the set of primes $\ell$ dividing exactly $N$ such that the $G_{\mathbb{Q}}$-module $E[p]$ is ramified at $\ell$. Then:

1. $\text{Ram}(\overline{p})$ contains all primes $\ell\|N^+$.
2. $\text{Ram}(\overline{p})$ contains all primes $\ell\|N^-$.
3. If $N$ is not square-free, then $\#\text{Ram}(\overline{p}) \geq 1$, and either $\text{Ram}(\overline{p})$ contains a prime $\ell\|N^-$ or there are at least two primes $\ell\|N^+$.
4. If $\ell^2\|N^+$, then $H^0(Q_{\ell}, \overline{p}) = 0$.

**Remark 1.4.** This is a slight strengthening of Condition $\heartsuit$ in [Zha14], where in part (2) $E[p]$ is only required to be ramified at the primes $\ell\|N^-$ with $\ell \equiv \pm 1 \pmod{p}$.

Under Condition $\heartsuit$ (and other hypotheses recalled in Theorem 3.2 below), W. Zhang [Zha14] has recently obtained a proof of Kolyvagin’s conjecture [Kol91a]. Concerning the nature of this conjecture, let us just mention here that it concerns the $p$-indivisibility of so-called derived Heegner classes on $E$, and as such it does not seem to have an Iwasawa-theoretic flavour.
In this note, we shall build on W. Zhang’s result to prove the following theorem towards Conjecture 1.2, where in addition to Assumptions 1.1 and 1.3, the following is in force:

**Assumption 1.5.**

(1) \( p = \mathfrak{p} \mathfrak{P} \) splits in \( K \).

(2) \( \overline{\mathfrak{p}} : G_K \to \text{Aut}_{\mathbb{F}_p}(E[\mathfrak{p}]) \) is surjective.

**Theorem 1.6** (Main result). Suppose that the triple \((E, K, p)\) satisfies Assumptions 1.1, 1.3, and 1.5, and assume in addition that \( \text{ord}_{\mathfrak{p}}(L(E/K, s)) = 1 \). Then Conjecture 1.2 holds.

1.2. **Outline of the proof.** After Perrin-Riou’s work, the first results towards Conjecture 1.2 were due to Bertolini [Ber95] and Howard [How04a, How04b], which under mild hypotheses established one of the divisibilities predicted by the third statement in the conjecture. More precisely, adapting to the anticyclotomic setting the Kolyvagin system machinery of Mazur–Rubin [MR04], Howard constructed a \( \Lambda \)-adic Kolyvagin system \( \kappa^\infty \) whose base class \( \kappa^\infty_1 \) could be shown to be non-trivial by Cornut–Vatsal [CV07], yielding a proof of all the statements in Conjecture 1.2 except for the divisibility \( \subseteq \) in the third part.

Later, the first cases of the full Conjecture 1.2 were obtained in [Wana, Thm. 1.2] and [Cas17, Thm. 3.4]. These were obtained by building on X. Wan’s work [Wanb], which when combined with the reciprocity law for Heegner points [CH18] yields a proof of the missing divisibility \( \subseteq \). However, these results excluded the case \( N^- = 1 \) (i.e. the “classical” Heegner hypothesis) and \( N \) is assumed to be square-free. In contrast, our proof of Theorem 1.6 is based on a different idea, dispensing with the use of [Wanb] and allowing for those excluded cases. Moreover, we expect the analytic rank 1 hypothesis made in Theorem 1.6 to not be essential to our method (see Remark 1.8).

As alluded to above, Howard’s results in [How04a,How04b] are based on the Mazur–Rubin machinery of Kolyvagin systems, suitably adapted to the anticyclotomic setting. As essentially known to Kolyvagin [Kol91a], the upper bound provided by this machinery can be shown to be sharp under a certain nonvanishing hypothesis; in the framework of [MR04], this corresponds to the Kolyvagin system being primitive [MR04, Def. 4.5.5 and 5.3.9].

Even though primitivity was not incorporated into Howard’s treatment [How04a,How04b], we shall upgrade his divisibility to an equality by building on W. Zhang’s proof of Kolyvagin’s main conjectures [Zha14]. In order to carry out this strategy, we consider a different anticyclotomic main conjecture. Under Assumption 1.5, Bertolini–Darmon–Prasanna [BDP13] (as extended by Brooks [HB15] for \( N^- \neq 1 \)) have constructed a \( p \)-adic \( L \)-function \( \mathcal{L}_p^{BDP} \in \Lambda^u := \mathbb{Z}_p^u \otimes \Lambda \), where \( \mathbb{Z}_p^u \) is the completion of the maximal unramified extension of \( \mathbb{Z}_p \), \( p \)-adically interpolating a square-root of certain Rankin–Selberg \( L \)-values. A variant of Greenberg’s main conjectures [Gre94] relates \( \mathcal{L}_p^{BDP} \) to the characteristic ideal of an \( “N^-\)-minimal” anticyclotomic Selmer group

\[
\text{Sel}_{N^-}^{\Lambda}(K, \Lambda) \subset \lim_{\to} H^1(K_n, \Lambda)
\]

defined in [JSW17, §2.3.4] (and recalled in Section 2 below) which differs from \( \text{Sel}_{\text{Gr}}(K, \Lambda) \) by the defining local conditions at the primes dividing \( p \) (and possibly \( N^- \)):

**Conjecture 1.7.** The Pontrjagin dual \( X_{v,0}^{N^-} \) of \( \text{Sel}_{v,0}^{N^-}(K, \Lambda) \) is \( \Lambda \)-torsion, and we have

\[
\text{char}(X_{v,0}^{N^-})\Lambda^u = (\mathcal{L}_p^{BDP})^2.
\]

As a key step in our proof, in Section 4 we establish the equivalence between Conjecture 1.2 and Conjecture 1.7. In particular, we show that Howard’s divisibility implies the divisibility \( \subseteq \) in Conjecture 1.7. In Section 5, assuming

\[
(1) \quad \text{rank}_\mathbb{Z} E(K) = 1,
\]

\[1\text{See }[\text{How06}] \text{ however, esp. Theorem 3.2.3, although we will have no use for any of the results in that paper.} \]
by a useful commutative algebra lemma from [SU14] and the “anticyclotomic control theorem” of [JSW17], we reduce the proof of the opposite divisibility to the proof of the equality
\begin{equation}
[E(K) : \mathbb{Z}P]^2 = \#\Pi(E/K)[p^\infty] \prod_{\ell | N^+} c_{\ell}^2
\end{equation}
up to a $p$-adic unit, where $P \in E(K)$ is a $p$-primitive generator of $E(K)$ up to torsion, and $c_{\ell}$ is the Tamagawa number of $E/Q_\ell$. Under the hypotheses of Theorem 1.6, equalities (1) and (2) follow from the Gross–Zagier formula [GZ86,YZZ13], and the work of Kolyvagin [Kol91a], and W. Zhang [Zha14], with $P \in E(K)$ given by the trace of a Heegner point defined over the Hilbert class field of $K$, yielding our main result.

**Remark 1.8.** By the work of Cornut–Vatsal [CV07], the Heegner points $y_n \in E(K_n)$ defined over the $n$-th layer of the anticyclotomic $\mathbb{Z}_p$-extension are non-torsion for $n$ sufficiently large. Taking one such $n$, and letting $y_{n,\chi} \in E(K_n)^{\chi} \subset E(K_n) \otimes \mathbb{Z}[\text{Gal}(K_n/K)] \mathbb{Z}[\chi]$
be the image of $y_n$ in the $\chi$-isotypical component of for a primitive character $\chi : \text{Gal}(K_n/K) \to \mathbb{Z}[\chi]^{\times}$, one can use Kolyvagin’s methods (as extended in [BD90]) to establish the rank one property of $E(K_n)^{\chi}$, and the Gross–Zagier formula [YZZ13] combined with a generalization of Kolyvagin’s structure theorem for Shafarevich–Tate groups [Kol91b] should yield an analogue of (2) in terms of the index of $y_{n,\chi}$.

2. Selmer structures

We keep the notations from the Introduction. In particular, $E/\mathbb{Q}$ is an elliptic curve of conductor $N$ with good ordinary reduction at a prime $p > 3$, and $K$ is an imaginary quadratic field of discriminant prime to $Np$ in which $p = p\overline{p}$ splits. Throughout the rest of this paper, we also fix once and for all a choice of complex and $p$-adic embeddings $\mathbb{C} \hookrightarrow \overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$.

Let $\Sigma$ be a finite set of places of $K$ including the places lying above $p$, $\infty$, and the primes dividing $N$. For a finite extension $F$ of $K$, let $F_\Sigma$ denote the maximal extension of $F$ unramified outside the places lying above $\Sigma$. Following [MR04], given a Selmer structure $\mathcal{F} = \{F_w\}_{w \mid v, v \in \Sigma}$ on a $G_K$-module $M$, we define the associated Selmer group $\text{Sel}_\mathcal{F}(F, M)$ by

\[
\text{Sel}_\mathcal{F}(F, M) := \ker \left( \bigoplus_{w \mid v, v \in \Sigma} \text{Ind}_{F_w/F} H^1(F_w/F, M) \to \prod_{w \mid v, v \in \Sigma} \text{Ind}_{F_w/F} H^1(F_w, M) \right).
\]

If $M$ is a $G_K$-module and $L/K$ a finite Galois extension, we have the induced representation

\[
\text{Ind}_{L/K} M := \{f : G_K \to M : f(\sigma x) = f(x)^{\sigma} \text{ for all } x \in G_K, \sigma \in G_L\},
\]

which is equipped with commuting actions of $G_K$ and $\text{Gal}(L/K)$. Consider the modules

\[
T := \varprojlim (\text{Ind}_{K_n/K} T), \quad A := \varprojlim (\text{Ind}_{K_n/K} A) \simeq \text{Hom}(T, \mu_{p^\infty}),
\]

where the limits are with respect to the corestriction and restriction maps, respectively. These are finitely and cofinitely generated over $\Lambda$, respectively.

We recall the ordinary filtrations at $p$. Let $G_{Q_p} := \text{Gal}(\overline{\mathbb{Q}}_p/Q_p)$, viewed as a decomposition group at $p$ inside $G_{\mathbb{Q}}$ via $\iota_p$. By $p$-ordinarity, there is a one-dimensional $G_{Q_p}$-stable subspace $\text{Fil}^+ V \subset V$ such that the $G_{Q_p}$-action on the quotient $\text{Fil}^- V := V/\text{Fil}^+ V$ is unramified. Set

\[
\text{Fil}^+ T := T \cap \text{Fil}^+ V, \quad \text{Fil}^- T := T/\text{Fil}^+ T, \quad \text{Fil}^+ A := \text{Fil}^+ V/\text{Fil}^+ T, \quad \text{Fil}^- A := A/\text{Fil}^+ A,
\]

and define the submodules $\text{Fil}^+ T \subset T$ and $\text{Fil}^+ A \subset A$ by

\[
\text{Fil}^+ T := \varprojlim (\text{Ind}_{K_n/K} \text{Fil}^+ T), \quad \text{Fil}^+ A := \varprojlim (\text{Ind}_{K_n/K} \text{Fil}^+ A),
\]

and set $\text{Fil}^- T := T/\text{Fil}^+ T$ and $\text{Fil}^- A := A/\text{Fil}^+ A$. 

4
Following the terminology introduced in [Cas17, §2], if $M$ denotes any of the $G_K$-modules above, we consider the following three local conditions at a place $v$ lying above $p$:

\[
\begin{align*}
H^1_0(F_v, M) &:= H^1(F_v, M), \\
H^1_{Gr}(F_v, M) &:= \ker \left( H^1(F_v, M) \rightarrow H^1(F_v, \Fil^{-} M) \right), \\
H^1_0(F_v, M) &:= 0.
\end{align*}
\]

We also recall two local conditions at a place $v$ not lying above $p$:

\[
\begin{align*}
H^1_{\text{triv}}(F_v, M) &:= 0, \\
H^1_{\text{ur}}(F_v, M) &:= H^1(F_v/I_v, M^{I_v}).
\end{align*}
\]

If $F = K$ and $M = A$, then $H^1_{\text{triv}}(F_v, M) = H^1_{\text{ur}}(F_v, M)$ unless $v$ divides $N^{-}$ and $\p$ is unramified at $v$ as in [PW11, Page 1362].

Using these local conditions, for $a, b \in \{0, \Gr, 0\}$ we define

\[
\group{Sel}_{a,b}(K, T) := \ker\left( H^1(K_{\Sigma}/K, T) \rightarrow \frac{H^1(K_p, T)}{H^1_a(K_p, T)} \times \frac{H^1(K_{\p}, T)}{H^1_b(K_{\p}, T)} \times \prod_{v \in \Sigma, v \neq p} H^1(K_v, T) \right).
\]

In particular, $\group{Sel}_{Gr}(K, T) := \group{Sel}_{Gr,Gr}(K, T)$ coincides with the $\Lambda$-adic Selmer group of [How04a, Def. 2.2.6], which we shall denote by $H^1_{\Sigma}(K, T)$ following the notation in [How04a]. The same definitions and notational convention applies to $A$. Putting the trivial local condition at primes dividing $N^{-}$, we can also define the $N^{-}$-minimal variant of discrete Selmer group by

\[
\group{Sel}_{a,b}^{N^{-}}(K, A) := \ker\left( \group{Sel}_{a,b}(K, A) \rightarrow \prod_{v \mid N^{-}} H^1_{\text{ur}}(K_v, A) \right).
\]

**Remark 2.1.** If $v$ divides $N^{-}$ and $\p$ is unramified at $v$, then $H^1_{\text{triv}}(K_v, A) \neq H^1_{\text{ur}}(K_v, A)$ since $v$ splits completely in $K_{\infty}/K$. See [PW11, Lem. 3.4] for the exact difference. Indeed, the $N^{-}$-minimal Selmer groups are practically preferred in the anticyclotomic Iwasawa theory for modular forms since the mod $p^n$ Selmer groups with the $N^{-}$-ordinary local condition [PW11, §3.2], which is used in the Euler system argument à la Bertolini-Darmon [BD05], becomes the minimal Selmer group after taking the limit with respect to $n$ under the tame ramification condition described in Remark 1.4. See [PW11, Prop. 3.6] for detail.

3. **Heegner point Kolyvagin systems**

In this section we briefly recall the statement of Howard’s theorems towards Conjecture 1.2, as well as the results from Wei Zhang’s proof of Kolyvagin’s conjecture that we shall use to upgrade Howard’s divisibility to an equality.

Let

\[
X := \text{Hom}_{\mathbb{Z}_p}(\group{Sel}_{Gr}(K, A), \mathbb{Q}_p/\mathbb{Z}_p)
\]

be the Pontrjagin dual of the $\Lambda$-adic Greenberg Selmer group. Since we shall not directly need it here, we refer the reader to [How04a, §1.2] for the definition of a Kolyvagin system $\kappa_{\infty} = \{\kappa_n\}_{n \in \mathbb{N}}$ (attached to a $G_K$-module $M$ together with a Selmer structure $\mathcal{F}$), where $n$ runs over the set of square-free products of certain primes inert in $K$, with the convention that $1 \in \mathcal{N}$.

**Theorem 3.1.** Assume that $p > 3$ is a good ordinary prime for $E$, $D_K$ is coprime to $pN$, and $\mathcal{P}$ is surjective. Let $\mathcal{F}_\Lambda$ be the Selmer structure for the Greenberg Selmer group. Then:

1. There exists a $\Lambda$-adic Kolyvagin system $\kappa_{\infty}$ for $(T, \mathcal{F}_\Lambda)$ with $\kappa_{\infty}^+ \neq 0$.
2. $\group{Sel}_{Gr}(K, T)$ is a torsion-free, rank one $\Lambda$-module.
3. There is a torsion $\Lambda$-module $M_{\infty}$ such that $\text{char}(M_{\infty}) = \text{char}(M_{\infty})^t$ and a pseudo-isomorphism $X \sim \Lambda \oplus M_{\infty} \oplus M_{\infty}$.
4. $\text{char}(M_{\infty})$ divides $\text{char}(\group{Sel}_{Gr}(K, T)/\Lambda \kappa_{\infty}^+)$. 


Proof. This is [How04a, Thm. 2.2.10], as extended in [How04b, Thm. 3.4.2] to the case \( N^− \neq 1 \). The non-triviality of \( \kappa^∞ \) follows from the work of Cornut–Vatsal [CV07]. □

Following [Zha14], we say that a prime \( \ell \) is called a Kolyvagin prime if \( \ell \) is prime to \( pND_K \), inert in \( K \), and the index

\[
M(\ell) := \min_p \{ v_p(\ell + 1), v_p(a_\ell) \}
\]

is strictly positive, where \( a_\ell = \ell + 1 - \#E(F_\ell) \). Let

\[
\delta_w : E(F_w) \otimes \mathbb{Z}_p \rightarrow H^1(F_w, T)
\]

be the local Kummer map, and let \( F \) be the Selmer structure on \( T \) given by \( H^1_F(F_w, T) := \text{im}(\delta_w) \). As explained in [How04a, §1.7] (and its extension in [How04b, §2.3] to \( N^− \neq 1 \)), Heegner points give rise to a (mod \( p^M \)) Kolyvagin system

\[
\kappa = \{ \kappa_n = c_M(n) \in H^1(K, E[p^M]) : 0 < M \leq M(n), n \in \mathcal{N} \}
\]

for \( (T/p^MT, \mathcal{F}) \), where \( \mathcal{N} \) denotes the set of square-free products of Kolyvagin primes, and for \( n \in \mathcal{N} \) we set \( M(n) := \min \{ M(\ell) : \ell|n \} \), with \( M(1) = \infty \) by convention.

**Theorem 3.2.** Assume that:

- \( p > 3 \) is a good ordinary prime for \( E \),
- \( D_K \) is coprime to \( pN \),
- Condition \( \heartsuit \) holds for \( (E, p, K) \),
- \( G_K \rightarrow \text{Aut}_{F_p}[E[p]] \) is surjective.

Then the collection of mod \( p \) cohomology classes

\[
(3) \quad \kappa = \{ \kappa_n = c_1(n) \in H^1(K, E[p]) : n \in \mathcal{N} \}
\]

is nonzero. In particular, \( \kappa_n \neq 0 \) for some \( n \).

**Proof.** This is [Zha14, Thm. 9.3]. □

**Remark 3.3.** In the terminology of [MR04], Wei Zhang’s Theorem 3.2 may be interpreted as establishing the primitivity of the system \( \kappa \). Mazur–Rubin also introduced the (weaker) notion of \( \Lambda \)-primitivity for the cyclotomic analogue of \( \kappa^∞ \) (see [MR04, Def. 5.3.9]), and in some sense our main result in this paper may be seen as a realization of the implications

\[
\kappa \text{ is primitive} \implies \kappa^∞ \text{ is } \Lambda\text{-primitive} \implies \text{Conjecture 1.2 holds},
\]

where \( \kappa^∞ \) is Howard’s Heegner point \( \Lambda \)-adic Kolyvagin system from Theorem 3.1.

Combined with Kolyvagin’s work, Theorem 3.2 yields the following exact formula the order of \( \#\text{III}(E/K)[p^∞] \) that we shall need.

**Corollary 3.4.** Let the hypotheses be as in Theorem 3.2. If \( \text{ord}_s=1L(E/K, s) = 1 \), then

\[
\text{ord}_p(\#\text{III}(E/K)[p^∞]) = 2 \cdot \text{ord}_p[E(K) : \mathbb{Z}.y_K]
\]

where \( y_K \in E(K) \) is a Heegner point.

**Proof.** After Theorem 3.2 (more precisely, the non-vanishing of (3)), this follows from Kolyvagin’s structure theorem from \( \text{III}(E/K) \) [Kol91b] (see also [McC91]), using that \( y_K \) has infinite order by the Gross–Zagier formula [GZ86, YZZ13] (cf. [Zha14, Thm. 10.2]). □
4. Equivalent main conjectures

In this section we establish the equivalence between Conjecture 1.2 (the Heegner point main conjecture) and Conjecture 1.7 (the Iwawa–Greenberg main conjecture for \( \mathscr{L}^{BDP} \)) in the Introduction.

To ease the notation, for \( a, b \in \{0, \text{Gr}, 0\} \) we let \( X_{a,b} \) denote the Pontryagin dual of the generalized Selmer group \( \text{Sel}_{a,b}(K, A) \), keeping the earlier convention that \( X := X_{\text{Gr}, \text{Gr}} \).

**Theorem 4.1.** Suppose \( E[p] \) is ramified at all primes \( \ell | N^- \). Then Conjectures 1.2 and 1.7 are equivalent. More precisely, \( X \) has \( \Lambda \)-rank 1 if and only if \( X_{\text{Gr}, 0} \) is \( \Lambda \)-torsion, and one-sided divisibility holds in Conjecture 1.2(3) if and only if the same divisibility holds in Conjecture 1.7.

**Proof.** This is essentially shown in the Appendix of [Cas17] (cf. [Wana, §3.3]); all the references in the proof that follows are to results in that paper. First, note that \( \text{Sel}_{a,b}(K, A) = \text{Sel}_{a,b}^N(K, A) \) by assumption. If \( X \) has \( \Lambda \)-rank 1, then \( \text{Sel}_{\text{Gr}}(K, T) \) has \( \Lambda \)-rank 1 by Lemma 2.3(1), and hence \( X_{\text{Gr}, 0} \) is \( \Lambda \)-torsion by Lemma A.4. Conversely, assume that \( X_{\text{Gr}, 0} \) is \( \Lambda \)-torsion. Then \( X_{\text{Gr}, 0} \) is also \( \Lambda \)-torsion (see eq. (A.7)), and so \( X_{\text{Gr}, 0} \) has \( \Lambda \)-rank 1 by Lemma 2.3(2). Now, global duality yields the exact sequence

\[
0 \to \text{coker}(\text{loc}_p) \to X_{\text{Gr}, 0} \to X \to 0,
\]

where \( \text{loc}_p : \text{Sel}_{\text{Gr}}(K, T) \to H^1_{\text{Gr}}(K, T) \) is the restriction map. Since \( H^1_{\text{Gr}}(K, T) \) has \( \Lambda \)-rank 1, the leftmost term in (4) is \( \Lambda \)-torsion by Theorem A.1 and the nonvanishing of \( \mathscr{L}^{BDP} \) (see Theorem 1.5); since \( X_{\text{Gr}, 0} \simeq X_{\text{Gr}, \text{Gr}} \) by the action of complex conjugation, we conclude from (4) that \( X \) has \( \Lambda \)-rank 1.

Next, assume that \( X \) has \( \Lambda \)-rank 1. By Lemma 2.3(1), this amounts to the assumption that \( \text{Sel}_{\text{Gr}}(K, T) \) has \( \Lambda \)-rank 1, and so by Lemmas A.3 and A.4 for every height one prime \( \mathfrak{p} \) of \( \Lambda \) we have

\[
\text{length}_{\mathfrak{p}}(X_{\text{Gr}, 0}) = \text{length}_{\mathfrak{p}}(X_{\text{tors}}) + 2 \text{length}_{\mathfrak{p}}(\text{coker}(\text{loc}_p)),
\]

where \( X_{\text{tors}} \) denotes the \( \Lambda \)-torsion submodule of \( X \), and for every height one prime \( \mathfrak{p}' \) of \( \Lambda' \)

\[
\text{ord}_{\mathfrak{p}'}(\mathscr{L}^{BDP}) = \text{length}_{\mathfrak{p}'}(\text{coker}(\text{loc}_p)\Lambda') + \text{length}_{\mathfrak{p}'}\left( \frac{\text{Sel}_{\text{Gr}}(K, T)\Lambda'}{\Lambda'\kappa_1^\infty} \right).
\]

Thus for any height one prime \( \mathfrak{p} \) of \( \Lambda \), letting \( \mathfrak{p}' \) denote its extension to \( \Lambda' \), we see from (5) and (6) that

\[
\text{length}_{\mathfrak{p}}(X_{\text{tors}}) \leq 2 \text{length}_{\mathfrak{p}}\left( \frac{\text{Sel}_{\text{Gr}}(K, T)}{\Lambda\kappa_1^\infty} \right) \iff \text{length}_{\mathfrak{p}}(X_{\text{Gr}, 0}) \leq 2 \text{ord}_{\mathfrak{p}}(\mathscr{L}^{BDP}),
\]

and similarly for the opposite inequalities. The result follows.

**Remark 4.2.** Accounting for the difference between the unramified (as implicitly used here) and the strict local conditions in \( H^1(F_w, A) \) for \( w | \ell | N^- \) in terms of \( p \)-parts of the corresponding Tamagawa numbers (see e.g. [PW11, §3]), it is possible to prove an analogue of Theorem 4.1 without the above ramification hypothesis on \( E[p] \). Indeed, the difference will only affect the \( \mu \)-invariants of both sides due to [PW11, Lem. 3.4].

5. Equivalent special value formulas

The goal of this section is to establish Corollary 5.4 below, which is a manifestation of the equivalence of Theorem 4.1 after specialization at the trivial character.

**Theorem 5.1.** Assume that \( \text{rank}_{\mathbb{Z}} E(K) = 1 \), \( \# \text{III}(E/K) < \infty \), and \( E[p] \) is irreducible as \( G_{\mathbb{Q}} \)-module. Then \( X_{\text{Gr}, 0}^N \) is \( \Lambda \)-torsion, and letting \( f_{\text{Gr}, 0}(T) \in \mathbb{Z}_p[T] \) be a generator of its
The characteristic ideal, the following equivalence holds:

\[ f_{\emptyset,0}(0) \sim_p \left( 1 - \frac{a_p + p}{p} \right)^2 \cdot \log_{\omega_E} P^2 \iff [E(K) : \mathbb{Z}.P]^2 \sim_p \# \text{III}(E/K)[p^\infty] \prod_{\ell \mid N^+} c_\ell^2, \]

where \( P \in E(K) \) is any generator of \( E(K) \otimes_{\mathbb{Z}} \mathbb{Q} \), \( c_\ell \) is the Tamagawa number of \( E/\mathbb{Q}_{\ell} \), and \( \sim_p \) denotes equality up to a \( p \)-adic unit.

**Remark 5.2.** Note that no Tamagawa defect at the primes dividing \( N^- \) is assigned in the RHS due to the \( N^- \)-minimal local condition of the Selmer group. Indeed, \( c_\ell \) for \( \ell \) dividing \( N^- \) becomes trivial in our setting due to Condition \( \heartsuit \) (Condition 1.3.(2)). See [PW11, Prop. 3.7] for the definite case.

**Proof.** As shown in [JSW17, p. 395-6], our assumptions imply hypotheses (corank 1), (sur), and (irred\( _K \)) of [JSW17, §3.1], and so by [loc. cit., Thm. 3.31] (with \( S = S_p \) the set of primes dividing \( N \) and \( \Sigma = \emptyset \)) the module \( X_{\emptyset,0}^{N^-} \) is \( A \)-torsion, and

\[ \#Z_p/f_{\emptyset,0}(0) = \# \text{Sel}_{\emptyset,0}^{N^-}(K, E[p^\infty]) \cdot C(E[p^\infty]), \]

where

\[ C(E[p^\infty]) := \# \text{II}(K_p, E[p^\infty]) \cdot \# \text{II}(K_\infty, E[p^\infty]) \cdot \prod_{w|N^+} \# \text{II}_w(K_w, E[p^\infty]). \]

On the other hand, from [JSW17, (3.5.d)] we have

\[ \# \text{Sel}_{\emptyset,0}^{N^-}(K, E[p^\infty]) = \# \text{III}(E/K)[p^\infty] \cdot \left( \frac{\#(Z_p/(1-a_p+p) \cdot \log_{\omega_E} P)}{[E(K) : \mathbb{Z}.P]_p \cdot \# \text{II}(K_p, E[p^\infty])} \right)^2, \]

where \( P \in E(K) \) is any generator of \( E(K) \otimes_{\mathbb{Z}} \mathbb{Q} \), and \( [E(K) : \mathbb{Z}.P]_p \) denotes the \( p \)-part of the index \( [E(K) : \mathbb{Z}.P] \). Combining (7) and (8) we thus arrive at

\[ \#Z_p/f_{\emptyset,0}(0) = \# \text{III}(E/K)[p^\infty] \cdot \left( \frac{\#(Z_p/(1-a_p+p) \cdot \log_{\omega_E} P)}{[E(K) : \mathbb{Z}.P]_p} \right)^2 \prod_{w|N^+} \# \text{II}_w(K_w, E[p^\infty]). \]

Since the order of \( \# \text{II}_w(K_w, E[p^\infty]) \) is the \( p \)-part of the Tamagawa number of \( E/K_w \), the result follows.

The fundamental \( p \)-adic Waldspurger formula due to Bertolini–Darmon–Prasanna [BDP13] will allow us to relate the left-hand side of Theorem 5.1 to the anticyclotomic main conjecture.

**Theorem 5.3** (Bertolini–Darmon–Prasanna). The following special value formula holds:

\[ \mathcal{L}^{BDP}_p(0) = \left( 1 - \frac{a_p + p}{p} \right) \cdot (\log_{\omega_E} y_K), \]

where \( y_K \in E(K) \) is a Heegner point.

**Proof.** This is a special case of [BDP13, Theorem 5.13] (cf. [BDP12, Theorem 3.12]) and [HB15, Theorem 1.1].

**Corollary 5.4.** With notations and hypotheses as in Theorem 5.1, assume in addition that \( (E, p, K) \) satisfies Condition \( \heartsuit \). Then the following equivalence holds:

\[ f_{\emptyset,0}(0) \sim_p \mathcal{L}^{BDP}_p(0)^2 \iff [E(K) : \mathbb{Z}.P]^2 \sim_p \# \text{III}(E/K)[p^\infty] \]

for \( P \) a \( p \)-unit multiple of the Heegner point \( y_K \in E(K) \).

**Proof.** Since Condition \( \heartsuit \) forces all the Tamagawa numbers \( c_\ell \) for the primes \( \ell \mid N^+ \) to be \( p \)-adic units, the result follows from Theorem 5.1 and Theorem 5.3.

**Remark 5.5.** Here we require \( P \) to be a \( p \)-unit multiple of the Heegner point \( y_K \), as otherwise the logarithm \( \log_{\omega_E} P \) and the index \( [E(K) : \mathbb{Z}.P] \) can be divisible by an extra power of \( p \).
6. Skinner–Urban lifting lemma

We recall the following “easy lemma” in [SU14].

**Lemma 6.1.** Let $A$ be a ring and $a$ be a proper ideal contained in the Jacobson radical of $A$. Assume that $A/a$ is a domain. Let $L \subseteq A$ be such that its reduction modulo $a$ is non-zero. Let $I \subseteq (L)$ be an ideal of $A$ and $I$ be the image of $I$ in $A/a$. If $L \mod a \in I$, then $I = (L)$.

**Proof.** This is [SU14, Lem. 3.2].

For our application, we shall set $A := \Lambda$, $a := (\gamma - 1)$ the augmentation ideal of $\Lambda$, $L := f_{0,0}(T)$ a generator of the characteristic ideal of $X_{0,0}$, and $I$ the ideal generated by $\mathcal{L}_p^{BDP}$. The divisibility $I \subseteq (L)$ will be a consequence of Theorem 3.1 and Theorem 4.1, and (assuming analytic rank 1) the relations $0 \neq f_{0,0}(0) \sim_p \mathcal{L}_p^{BDP}(0)$ will be deduced from Corollary 3.4 and Corollary 5.4; the equality $I = (L)$ will then follow.

**Remark 6.2.** Note that the roles of algebraic and analytic $p$-adic $L$-functions are switched in our setting comparing with those of [SU14]. This is possible since $\Lambda$ is a UFD, and so the characteristic ideal of a finitely generated $\Lambda$-module is principal.

7. Proof of the main results

We are now ready to prove our main results.

**Theorem 7.1.** Let $E/\mathbb{Q}$ be an elliptic curve of conductor $N$, let $p > 3$ be a good ordinary prime for $E$, and let $K$ be an imaginary quadratic field of discriminant $D_K$ with $(D_K, Np) = 1$. Assume that:

- $N^-$ is the square-free product of an even number of primes.
- $(E, p, K)$ satisfies Condition $\nabla$.
- $G_K \to \text{Aut}_{\mathbb{F}_p}(E[p])$ is surjective.
- $p = \mathfrak{p}\mathfrak{p}$ splits in $K$.

In addition, assume that $\text{ord}_{s=1}L(E/K, s) = 1$. Then Conjecture 1.2 holds.

**Proof.** By Theorem 3.1, the Pontryagin dual $X$ of $\text{Sel}_{G_1}(K, \Lambda)$ has $\Lambda$-rank 1, and its $\Lambda$-torsion submodule $X_{\text{tors}}$ is such that

$$\text{char}(X_{\text{tors}}) \cong \text{char}\left(\frac{\text{Sel}_{G_1}(K, \mathbb{T})}{\Lambda_{K_1^\infty}}\right)^2.$$

By Theorem 4.1, it follows that the Pontrjagin dual $X_{N,0}^N$ of $\text{Sel}_{N,0}^N(K, A)$ is $\Lambda$-torsion, and we have

$$f_{0,0} \cong (\mathcal{L}_p^{BDP})^2,$$

where $f_{0,0} \in \Lambda$ is a generator of the characteristic ideal $\text{char}(X_{N,0}^N)$. On the other hand, by the work of Gross–Zagier and Kolyvagin, the assumption that $\text{ord}_{s=1}L(E/K, s) = 1$ implies the Heegner point $y_K \in E(K)$ is non-torsion, and we have $\text{rank}_Z E(K) = 1$ and $\#\text{III}(E/K) < \infty$; while by Corollary 3.4 we have

$$[E(K) : \mathbb{Z}.y_K]^2 \sim_p \#\text{III}(E/K)[p^\infty].$$

In light of Corollary 5.4, the last equality (up to a $p$-adic units) amounts to the equality

$$f_{0,0}(0) \sim_p \mathcal{L}_p^{BDP}(0)^2,$$

and given (9) and (10), the result follows from Lemma 6.1. □

**Corollary 7.2.** Let the hypotheses be as in Theorem 7.1. Then Conjecture 1.7 holds.

**Proof.** Since $E[p]$ is ramified at all primes $\ell | N^-$ by hypothesis, the result follows from Theorem 4.1 and Theorem 7.1. □
Lan90

[BD90] Massimo Bertolini and Henri Darmon, *Kolyvagin’s descent and Mordell-Weil groups over ring class fields*, J. Reine Angew. Math. **412** (1990), 63–74.

[BD05] ______, *Iwasawa’s main conjectures for elliptic curves over anticyclotomic $\mathbb{Z}_p$-extensions*, Ann. of Math. (2) **162** (2005), no. 1, 1–64.

[BDP12] Massimo Bertolini, Henri Darmon, and Kartik Prasanna, *$p$-adic Rankin $L$-series and rational points on CM elliptic curves*, Pacific J. Math. **260** (2012), no. 2, 261–303, Jonathan Rogawski Memorial Issue.

[BDP13] ______, *Generalized Heegner cycles and $p$-adic Rankin $L$-series*, Duke Math. J. **162** (2013), no. 6, 1033–1148, Appendix by Brian Conrad.

[Ber95] Massimo Bertolini, *Selmer groups and Heegner points in anticyclotomic $\mathbb{Z}_p$-extensions*, Compos. Math. **99** (1995), no. 2, 153–182.

[Cas17] Francesc Castella, *$p$-adic heights of Heegner points and Beilinson-Flach classes*, J. Lond. Math. Soc. (2) **96** (2017), no. 1, 156–180.

[CH18] Francesc Castella and Ming-Lun Hsieh, *Heegner cycles and $p$-adic $L$-functions*, Math. Ann. **370** (2018), no. 1-2, 567–628.

[CV07] Christophe Cornut and Vinayak Vatsal, *Nontriviality of Rankin-Selberg $L$-functions and CM points*, $L$-functions and Galois representations (Cambridge) (David Burns, Kevin Buzzard, and Jan Nekovář, eds.), London Math. Soc. Lecture Note Ser., vol. 320, Cambridge University Press, 2007, pp. 121–186.

[Gre94] Ralph Greenberg, *Iwasawa theory and $p$-adic deformations of motives*, Motives (Seattle, WA, 1991), Proc. Sympos. Pure Math., vol. 55, Amer. Math. Soc., Providence, RI, 1994, pp. 193–223.

[GZ86] Benedict Gross and Don Zagier, *Heegner points and derivatives of $L$-series*, Invent. Math. **84** (1986), no. 2, 225–320.

[HB15] Ernest Hunter Brooks, *Shimura curves and special values of $p$-adic $L$-functions*, Int. Math. Res. Not. IMRN (2015), no. 12, 4177–4241.

[How04a] Benjamin Howard, *The Heegner point Kolyvagin system*, Compos. Math. **140** (2004), no. 6, 1439–1472.

[How04b] ______, *Iwasawa theory of Heegner points on abelian varieties of $GL_2$ type*, Duke Math. J. **124** (2004), no. 1, 1–45.

[How06] ______, *Bipartite Euler systems*, J. Reine Angew. Math. **597** (2006), 1–25.

[JSW17] Dimitar Jetchev, Christopher Skinner, and Xin Wan, *The Birch and Swinnerton-Dyer formula for elliptic curves of analytic rank one*, Camb. J. Math. **5** (2017), no. 3, 369–434.

[Kat04] Kazuya Kato, *$p$-adic Hodge theory and values of zeta functions of modular forms*, Astérisque **295** (2004), 117–290.

[Kol88] Victor Kolyvagin, *On the Mordell-Weil and Shafarevich-Tate groups for Weil elliptic curves (Russian)*, Izv. Akad. Nauk SSSR Ser. Mat. **52** (1988), no. 6, 1154–1180, 1327, Math. USSR-Izv. **33** (1989), no. 3, 473–499.

[Kol91a] ______, *On the structure of Selmer groups*, Math. Ann. **291** (1991), no. 2, 253–259.

[Kol91b] ______, *On the structure of Shafarevich-Tate groups*, Algebraic Geometry (Spencer Bloch, Igor Dolgachev, and William Fulton, eds.), Lecture Notes in Math., vol. 1479, Springer, 1991, Proceedings of the US-USSR Symposium held in Chicago, June 20–July 14, 1989, pp. 94–121.

[Lang90] Serge Lang, *Cyclotomic Fields I and II*, combined 2nd ed., Grad. Texts in Math., vol. 121, Springer-Verlag, 1990.

[McC91] William McCallum, *Kolyvagin’s work on Shafarevich-Tate groups*, $L$-functions and Arithmetic (John Coates and M.J. Taylor, eds.), London Math. Soc. Lecture Note Ser., vol. 153, Cambridge University Press, 1991, Proceedings of the Durham Symposium, July, 1989, pp. 295–316.

[MR04] Barry Mazur and Karl Rubin, *Kolyvagin Systems*, Mem. Amer. Math. Soc., vol. 168, American Mathematical Society, March 2004.

[PR87] Bernadette Perrin-Riou, *Fonctions $L$ $p$-adiques, théorie d’Iwasawa et points de Heegner*, Bull. Soc. Math. France **115** (1987), no. 4, 399–456.

[PW11] Robert Pollack and Tim Weston, *On anticyclotomic $\mu$-invariants of modular forms*, Compos. Math. **147** (2011), 1353–1381.

[Rub90] Karl Rubin, *The Main Conjecture*, combined 2nd ed., Grad. Texts in Math., vol. 121, ch. Appendix, Springer-Verlag, 1990, Appendix to [Lang90].

[SU14] Christopher Skinner and Eric Urban, *The Iwasawa main conjectures for $GL_2$*, Invent. Math. **195** (2014), no. 1, 1–277.

[Wana] Xin Wan, *Heegner point Kolyvagin system and Iwasawa main conjecture*, preprint.

[Wanb] ______, *Iwasawa main conjecture for Rankin-Selberg $p$-adic $L$-functions*, preprint.

[YZZ13] Xinyi Yuan, Shou-Wu Zhang, and Wei Zhang, *The Gross-Zagier formula on Shimura curves*, Ann. of Math. Stud., vol. 184, Princeton University Press, 2013.
[Zha14] Wei Zhang, *Selmer groups and the indivisibility of Heegner points*, Camb. J. Math. 2 (2014), no. 2, 191–253.

(Burungale) **School of Mathematics, Institute for Advanced Study, Einstein Drive, Princeton, NJ 08540, USA**  
*E-mail address:* ashayburungale@gmail.com

(Castella) **Department of Mathematics, Princeton University, Washington Road, Princeton, NJ 08544-1000, USA**  
*E-mail address:* fcabello@math.princeton.edu

(Kim) **School of Mathematics, Korea Institute for Advanced Study, 85 Hoegi-ro, Dongdaemun-gu, Seoul 02455, Republic of Korea**  
*E-mail address:* chanho.math@gmail.com