Cambridge Journal of Mathematics
Volume 2, Number 2, 191–253, 2014

Selmer groups and the indivisibility of Heegner points

Wei Zhang

For elliptic curves over $\mathbb{Q}$, we prove the p-indivisibility of derived Heegner points for certain prime numbers p, as conjectured by Kolyvagin in 1991. Applications include the refined Birch–Swinerton-Dyer conjecture in the analytic rank one case, and a converse to the theorem of Gross–Zagier and Kolyvagin. A slightly different version of the converse is also proved earlier by Skinner.

1. Introduction and main results

In this article we confirm a refined conjecture of Kolyvagin [24] on the p-indivisibility of some derived Heegner points on an elliptic curve E over $\mathbb{Q}$

for a good ordinary prime $p \geq 5$ that satisfies suitable local ramification hypothesis. When the analytic rank of $E/\mathbb{Q}$ is one, combining with the general Gross–Zagier formula on Shimura curves [17, 45, 46] and Kolyvagin's theorem [23], we are able to prove the p-part of the refined Birch–Swinnerton-Dyer conjecture. We also obtain a converse to the theorem of Gross–Zagier and Kolyvagin, first proved by Skinner for semistable elliptic curves [36]. When the analytic rank is higher than one, together with Kolyvagin's theorem [24], one may naturally construct all elements in the p^∞-Selmer group $\mathrm{Sel}_{p^\infty}(E/\mathbb{Q})$ from Heegner points defined over ring class fields. In a subsequent paper [49], we will apply the main result of this paper to prove a version of the Birch–Swinnerton-Dyer conjecture (for Selmer groups) à la Mazur–Tate [27] and Darmon [12] in the anti-cyclotomic setting.

Let E be an elliptic curve over $\mathbb{Q}$ with conductor N. For any number field $F \subset \overline{\mathbb{Q}}$, we denote by $\mathrm{Gal}_F := \mathrm{Gal}(\overline{\mathbb{Q}}/F)$ the absolute Galois group of F. One important arithmetic invariant of E/F is the Mordell–Weil group $E(F)$, a finitely-generated abelian group:

$$E(F) \simeq \mathbb{Z}^{r_{MW}} \oplus \text{ finite group},$$

where the integer $r_{MW} = r_{MW}(E/F)$ is called the Mordell–Weil rank. Another important arithmetic invariant of E/F is the Tate–Shafarevich group of E/F, denoted by $\text{Ш}(E/F)$:

$$\text{Ш}(E/F) := \mathrm{Ker}(H^1(F, E) \to \prod_v H^1(F_v, E)),$$

where the map is the product of the localization at all places v of F, and, as usual, $H^i(k, E) := H^i(\mathrm{Gal}(\overline{k}/k), E)$ for $k = F, F_v$ and $i \in \mathbb{Z}_{\geq 0}$. The group $\text{Ш}(E/F)$ is torsion abelian, and conjectured to be *finite* by Tate and Shafarevich. As a set, it is closely related to the set of isomorphism classes of smooth projective curves C/F such that

$$\mathrm{Jac}(C) \simeq E, \quad C(F_v) \neq \emptyset, \text{ for all } v.$$

Let p be a prime and $\text{Ш}(E/F)[p^\infty]$ the p-primary part of $\text{Ш}(E/F)$. Incorporating the information of both $E(F)$ and $\text{Ш}(E/F)$, there is the p^∞-Selmer group denoted by $\mathrm{Sel}_{p^\infty}(E/F)$ defined as follows (cf. [13, §2]). Let $E[p^\infty]$ be the group of p-primary torsion points of $E(\overline{\mathbb{Q}})$. The Galois group $\mathrm{Gal}_{\mathbb{Q}}$ acts on $E[p^\infty]$. Consider the local Kummer map

$$\delta_v : E(F_v) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to H^1(F_v, E[p^\infty]).$$

Then $\mathrm{Sel}_{p^\infty}(E/F)$ is defined as

$$\mathrm{Sel}_{p^\infty}(E/F) := \mathrm{Ker}(H^1(F, E[p^\infty]) \to \prod_v H^1(F_v, E[p^\infty])/\mathrm{Im}(\delta_v)),$$

where the map is the product of the localization at all places v of F. The $\mathbb{Z}_p$-corank of $\mathrm{Sel}_{p^\infty}(E/F)$ is denoted by $r_p(E/F)$.

The Mordell–Weil group $E(F)$, the p^∞-Selmer group $\mathrm{Sel}_{p^\infty}(E/F)$ and the p-primary part of Tate–Shafarevich group $Ш(E/F)[p^\infty]$ are related by the following exact sequence:

$$0 \to E(F) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to \mathrm{Sel}_{p^\infty}(E/F) \to Ш(E/F)[p^\infty] \to 0.$$

This sequence may be called the *p^∞-descent of E/F*. Then we have an inequality

$$0 \le r_{MW}(E/F) \le r_p(E/F),$$

where the equality $r_{MW}(E/F) = r_p(E/F)$ holds if and only if $Ш(E/F)[p^\infty]$ is finite. Therefore, assuming $\#Ш(E/F) < \infty$, the Selmer rank $r_p(E/F)$ is independent of p.

We may also consider the p-Selmer group $\mathrm{Sel}_p(E/F)$ and the p-torsion $Ш(E/F)[p]$ of $Ш(E/F)$. We have the exact sequence of vector spaces over $\mathbb{F}_p$ (the finite field of p elements):

$$0 \to E(F) \otimes \mathbb{Z}/p\mathbb{Z} \to \mathrm{Sel}_p(E/F) \to Ш(E/F)[p] \to 0.$$

This sequence may be called the *p-descent (or the first descent) of E/F*. Then we have a natural surjective homomorphism

$$\mathrm{Sel}_p(E/F) \to \mathrm{Sel}_{p^\infty}(E/F)[p],$$

where $[p]$ denotes the subgroup of p-torsion elements.

We will denote the action of $\mathrm{Gal}_\mathbb{Q} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the p-torsion points $E[p]$ by

$$\overline{\rho}_{E,p} : \mathrm{Gal}_\mathbb{Q} \to \mathrm{Aut}(E[p]) \simeq \mathrm{GL}_2(\mathbb{F}_p).$$

Throughout this paper we assume that $\overline{\rho}_{E,p}$ is surjective, $p \nmid N$, and $p \ge 5$.

Let $L(E/\mathbb{Q}, s)$ be the L-function associated to $E/\mathbb{Q}$[1]. We take the normalization such that the center of the functional equation is at $s = 1$. The vanishing order of $L(E/\mathbb{Q}, s)$ at $s = 1$ is called the analytic rank of $E/\mathbb{Q}$.

[1]Note that this L-function does not include the archimedean local L-factor.

The theorem of Gross–Zagier and Kolyvagin asserts that if the analytic rank of $E/\mathbb{Q}$ is at most one, then the Mordell–Weil rank is equal to the analytic rank and $Ш(E/\mathbb{Q})$ is finite. The proof of their theorem is through the study of the Heegner points. To define these points, we let $K = \mathbb{Q}[\sqrt{-D}]$ be an imaginary quadratic field of discriminant $D_K = -D < 0$ with $(D, N) = 1$. Write $N = N^+N^-$ where the prime factors of N^+ (N^-, resp.) are all split (inert, resp.) in K. Assume that N^- is square-free and denote by $\nu(N^-)$ by the number of prime factors of N^-. Then the root number for E/K is $(-1)^{1+\nu(N^-)}$. We say that the pair (E, K) satisfies the generalized Heegner hypothesis if $\nu(N^-)$ is even. Then there exist a collection of points $y(n)$ on E defined over the ring class field $K[n]$ of conductor n (cf. §3). The trace of $y(1)$ from $K[1]$ to K will be denoted by y_K. The work of Gross–Zagier [17] and S. Zhang [46] asserts that y_K is non-torsion if and only if the analytic rank of E/K is one. The method of Kolyvagin is to construct cohomology classes from the Heegner points $y(n)$ to bound the p^∞-Selmer group, in particular, to show that the Mordell–Weil rank of E/K is one and $Ш(E/K)$ is finite, if y_K is non torsion. We fix a prime p with surjective $\overline{\rho}_{E,p}$. We call a prime ℓ a Kolyvagin prime if ℓ is prime to NDp, inert in K and the Kolyvagin index $M(\ell) := \min\{v_p(\ell+1), v_p(a_\ell)\}$ is strictly positive. Let Λ be the set of square-free product of distinct Kolyvagin primes. Define $M(n) = \min\{M(\ell) : \ell | n\}$ if $n > 1$, and $M(1) = \infty$. To each $y(n)$ and $M \leq M(n)$, Kolyvagin associated a cohomology class $c_M(n) \in H^1(K, E[p^M])$ (cf. §3 (3.21) for the precise definition). Denote

$$\kappa^\infty = \{c_M(n) \in H^1(K, E[p^M]) : n \in \Lambda, M \leq M(n)\}.$$

In particular, the term $c_M(1)$ of κ^∞ is the image under the Kummer map of the Heegner point $y_K \in E(K)$. Therefore, when the analytic rank of E/K is equal to one, the Gross–Zagier formula implies that $y_K \in E(K)$ is non torsion and hence $c_M(1) \neq 0$ for all $M \gg 0$. Kolyvagin then used the non-zero system κ^∞ to bound the Selmer group of E/K. In [24], Kolyvagin conjectured that κ^∞ is always nonzero even if the analytic rank of E/K is strictly larger than one. Assuming this conjecture, he proved various results about the Selmer group of E/K (in particular, see Theorem 11.2 and Remark 18 in §10). In this paper we will prove his conjecture under some conditions we now describe.

Let $\mathrm{Ram}(\overline{\rho}_{E,p})$ be the set of primes $\ell || N$ such that $\overline{\rho}_{E,p}$ is ramified at ℓ. We further impose the following ramification assumption on $\overline{\rho}_{E,p}$ (depending on the decomposition $N = N^+N^-$, hence on K), called *Hypothesis* ♠ for (E, p, K):

(1) $\mathrm{Ram}(\overline{\rho}_{E,p})$ contains all primes ℓ such that $\ell || N^+$ and all primes $\ell | N^-$ such that $\ell \equiv \pm 1 \mod p$.
(2) If N is not square-free, then $\#\mathrm{Ram}(\overline{\rho}_{E,p}) \geq 1$, and either $\mathrm{Ram}(\overline{\rho}_{E,p})$ contains a prime $\ell || N^-$ or there are at least two primes factors $\ell || N^+$.

Note that there is no requirement on the ramification of $E[p]$ at those primes ℓ for which $\ell^2 | N$; that is, at the primes where E has additive reduction.

Then we prove (cf. see Theorem 9.3)

Theorem 1.1. *Let $E/\mathbb{Q}$ be an elliptic curve of conductor N, p a prime and K an imaginary quadratic field, such that*

- *N^- is square-free with even number of prime factors.*
- *The residue representation $\overline{\rho}_{E,p}$ is surjective.*
- *Hypothesis ♠ holds for (E, p, K).*
- *The prime $p \geq 5$ is ordinary, $p \nmid D_K N$ and $(D_K, N) = 1$.*

Then we have $c_1(n) \neq 0$ for some $n \in \Lambda$, and hence $\kappa^\infty \neq \{0\}$.

Following the terminology of [26], suitably modified for the Heegner point setting [19], we call the collection κ^∞ a *Kolyvagin system*. The *vanishing order* $\mathrm{ord}\,\kappa^\infty$ of the Kolyvagin system κ^∞ is, by definition, the minimal number of prime factors of $n \in \Lambda$ such that $c_M(n) \neq 0$ for some $M \leq M(n)$. Let $\mathrm{Sel}^{\pm}_{p^\infty}(E/K)$ denote the eigenspace with eigenvalue ± 1 of $\mathrm{Sel}_{p^\infty}(E/K)$ under the complex conjugation. Let $r_p^{\pm}(E/K)$ be the $\mathbb{Z}_p$-corank of $\mathrm{Sel}^{\pm}_{p^\infty}(E/K)$. Combining Theorem 1.1 with Kolyvagin's theorem [24, Theorem 4], we have the following relation between the $\mathbb{Z}_p$-coranks $r_p^{\pm}(E/K)$ and the vanishing order $\mathrm{ord}\,\kappa^\infty$.

Theorem 1.2. *Let (E, p, K) be as in Theorem 1.1. Then we have*

$$\mathrm{ord}\,\kappa^\infty = \max\{r_p^+(E/K), r_p^-(E/K)\} - 1. \tag{1.1}$$

Furthermore, we denote $\nu^\infty = \mathrm{ord}\,\kappa^\infty$ and

$$\epsilon_{\nu^\infty} := \epsilon \cdot (-1)^{\nu^\infty + 1} \in \{\pm 1\},$$

where $\epsilon = \epsilon(E/\mathbb{Q})$ is the global root number of $E/\mathbb{Q}$. Then we have

$$r_p^{\epsilon_{\nu^\infty}}(E/K) = \nu^\infty + 1,$$

and

$$0 \leq \nu^\infty - r_p^{-\epsilon_{\nu^\infty}}(E/K) \equiv 0 \mod 2.$$

Remark 1. In particular, under the assumption of Theorem 1.2, the parity conjecture for p^∞-Selmer group holds:

$$(-1)^{r_p(E/\mathbb{Q})} = \epsilon(E/\mathbb{Q}).$$

The parity conjecture is known in a more general setting [32] but our proof does not use it and in fact implies it for our (E, p, K).

This is proved in Theorem 11.2. We may further construct all elements in the p-Selmer group $\mathrm{Sel}_p(E/K)$, cf. Theorem 11.1. Our Theorem 1.1 and Kolyvagin's result [24] shows that the eigenspace $\mathrm{Sel}_{p^\infty}^{\epsilon_{\nu^\infty}}(E/K)$ of Selmer groups under the complex conjugation is contained in the subgroup generated by the cohomology classes $c(n)$ (Theorem 11.2). By choosing a suitable K, this also allows us to construct all $\mathrm{Sel}_{p^\infty}(E/\mathbb{Q})$ for certain primes p and elliptic curves $E/\mathbb{Q}$ (cf. Corollary 11.3). Moreover, one obtains the structure of the indivisible quotient of $Ш(E/K)[p^\infty]$ in terms of the divisibility of Heegner points ([23], see Remark 18 in §10).

We now state some applications to elliptic curves $E/\mathbb{Q}$ whose Selmer groups have $\mathbb{Z}_p$-corank one. From Theorem 1.2, one may deduce a result for E/K:

Theorem 1.3. *Let (E, p, K) be as in Theorem 1.1. If $\mathrm{Sel}_{p^\infty}(E/K)$ has $\mathbb{Z}_p$-corank one, then the Heegner point $y_K \in E(K)$ is non-torsion. In particular, the analytic rank (i.e., $\mathrm{ord}_{s=1}L(E/K, s)$) and the Mordell–Weil rank of E/K are equal to one, and $Ш(E/K)$ is finite.*

Proof. Since $r_p(E/K) = 1$ and $r_p(E/K) = r_p^+(E/K) + r_p^-(E/K)$, we must have

$$\max\{r_p^+(E/K), r_p^-(E/K)\} = 1.$$

By Theorem 1.2, we must have $\nu^\infty = 0$, i.e., $c_M(1) \neq 0$, for some M. The cohomology class $c_M(1)$ is the image of the Heegner point $y_K \in E(K)$ under the injective Kummer map $E(K)/p^M E(K) \to H^1(K, E[p^M])$, and so $y_K \notin p^M E(K)$. The hypothesis on the subjectivity of $\overline{\rho}_{E,p}$ implies that $E(K)$ has no p-torsion, and it follows that $y_K \in E(K)$ is non-torsion. The "in particular" part is then due to the Gross–Zagier formula ([17] in the case of modular curves), Kolyvagin's theory of Euler system, and their extension to the setting of Shimura curves [42, 45]. □

When $p = 2$, the same kind of result was earlier obtained by Y. Tian for the congruent number elliptic curves [39, 40].

Now we state some results for $E/\mathbb{Q}$.

Theorem 1.4. *Let $E/\mathbb{Q}$ be an elliptic curve of conductor N, and $p \geq 5$ a prime such that:*

(1) $\overline{\rho}_{E,p}$ is surjective.
(2) If $\ell \equiv \pm 1 \mod p$ and $\ell || N$, then $\overline{\rho}_{E,p}$ is ramified at ℓ.
(3) If N is not square-free, then $\#\mathrm{Ram}(\overline{\rho}_{E,p}) \geq 1$ and when $\#\mathrm{Ram}(\overline{\rho}_{E,p}) = 1$, there are even number of prime factors $\ell || N$.
(4) The prime p is good ordinary.

Then we have:

(i) If $\mathrm{Sel}_{p^\infty}(E/\mathbb{Q})$ has $\mathbb{Z}_p$-corank one, then the analytic rank and the Mordell-Weil rank of $E/\mathbb{Q}$ are both equal to one, and $\text{Ш}(E/\mathbb{Q})$ is finite.
(ii) If the analytic rank of $E/\mathbb{Q}$ is larger than one

$$\mathrm{ord}_{s=1} L(E/\mathbb{Q}, s) > 1,$$

then the $\mathbb{Z}_p$-corank of $\mathrm{Sel}_{p^\infty}(E/\mathbb{Q})$ is at least two (three, resp.) if the root number $\epsilon(E/\mathbb{Q})$ is $+1$ (-1, resp.).

Proof. To prove (i), by [6, 31], we may choose an imaginary quadratic field K such that

(a) (E, K) satisfies the generalized Heegner hypothesis (i.e., N^- has even number of factors) and (E, p, K) satisfies Hypothesis ♠. To see why such a K exists, first suppose that N is square-free. If N has an even number of prime factors, then choose K such that $N^+ = 1$ and $N^- = N$. If N has an odd number of prime factors, then choose an $\ell | N$ where $\overline{\rho}_{E,p}$ is ramified, and then choose K such that $N^+ = \ell$ and $N^- = N/\ell$. Note that such ℓ exists by Ribet's level-lowering theorem [34]; otherwise, since p does not divide N, $\overline{\rho}_{E,p}$ is modular of level 1 by [34, Theorem 1.1], a contradiction! If N is not square-free, we have two cases under the condition (3): when $\#\mathrm{Ram}(\overline{\rho}_{E,p}) = 1$ or there are even number of primes $\ell || N$, we may choose N^- as the product of all $\ell || N$; when $\#\mathrm{Ram}(\overline{\rho}_{E,p}) \geq 2$ and there are odd number of primes $\ell || N$, we may choose N^- as the product of all $\ell || N$ but one $\ell \in \mathrm{Ram}(\overline{\rho}_{E,p})$.
(b) The L-function attached to the quadratic twist, denoted by E^K, of E by K has non-zero central value:

$$L(E^K, 1) \neq 0.$$

The non-vanishing requirement can be achieved since we may first prove that the root number of $\epsilon(E/\mathbb{Q})$ is -1 by Theorem 1.2. Indeed, we may first choose a K to satisfy (a) only. Then by Theorem 1.2, we know that the root number $\epsilon(E/\mathbb{Q})$ is -1 since the $\mathbb{Z}_p$-corank of $\mathrm{Sel}_{p^\infty}(E/\mathbb{Q})$ is odd.

Once we have chosen such K, we see that $E^K(\mathbb{Q})$ and $\text{Ш}(E^K/\mathbb{Q})$ are both finite (by Gross–Zagier and Kolyvagin, or Kato, or Bertolini–Darmon). In particular, $\mathrm{Sel}_{p^\infty}(E^K/\mathbb{Q})$ is finite. It follows that $\mathrm{Sel}_{p^\infty}(E/K)$ has $\mathbb{Z}_p$-corank one. Since now our (E, p, K) satisfies the assumption of Theorem 1.3, the desired result follows.

To show part (ii), we again choose K as in the proof of part (i) with only one modification: if $\epsilon(E/\mathbb{Q}) = 1$, we require that $L'(E^K, 1) \neq 0$. Then by Gross–Zagier formula [45], the Heegner point y_K is a torsion point. Hence the class $c_M(1) = 0$ for all $M \in \mathbb{Z}_{>0}$ and the vanishing order ν^∞ of the Kolyvagin system κ^∞ is at least 1. Then part (ii) follows from Theorem 1.2. □

Remark 2. A version of Theorem 1.3 is also proved by Skinner [36] under some further assumption that $p = \mathfrak{P}\overline{\mathfrak{P}}$ is split in $K/\mathbb{Q}$, and the localization homomorphism at $\mathfrak{P}$,

$$\mathrm{loc}_{\mathfrak{P}} : \mathrm{Sel}_{p^\infty}(E/K) \to H^1_{fin}(K_{\mathfrak{P}}, E[p^\infty]),$$

is surjective, where $H^1_{fin}(K_{\mathfrak{P}}, E[p^\infty])$ is the image of the local Kummer map at $\mathfrak{P}$. He also announced a version of Theorem 1.4 under similar surjectivity assumption on loc_p. It is worthing noting that Skinner considers the localization at p of the cohomology class of the Heegner point y_K, while the current paper considers the localization at many primes away from p (so we do not need the local surjectivity assumption at p) of the cohomology classes of Heegner points over ring class fields (so one may take advantage of Kolyvagin system). Skinner then uses a p-adic formula due to Bertolini–Darmon–Prasanna [5] and (one divisibility of) the main conjecture proved by X. Wan [44], while the current paper uses the Gross formula modulo p ([14], an explicit version of Waldspurger formula, cf. §6), the congruence of Bertolini–Darmon [4], and the main conjecture proved by Kato [21] and Skinner–Urban [37].

Remark 3. For an elliptic curve $E/\mathbb{Q}$, the set of primes p satisfying (1)-(4) in Theorem 1.4 has density one, and depends only on the residue representation $\overline{\rho}_{E,p}$. The theorem also implies that: r_p is independent of p in this set if we have $r_p(E/\mathbb{Q}) = 1$ for one p in this set.

Theorem 1.5. *Let $E/\mathbb{Q}$ be an elliptic curve of conductor N. If N is not square-free, then we assume that there are at least two prime factors $\ell||N$. Then the following are equivalent:*

(i) $r_{MW}(E/\mathbb{Q}) = 1$ *and* $\#\text{Ш}(E/\mathbb{Q}) < \infty$.
(ii) $\mathrm{ord}_{s=1}L(E/\mathbb{Q}, s) = 1$.

The direction $(i) \implies (ii)$ is a converse to the theorem of Gross–Zagier and Kolyvagin. Such a converse was first proved by Skinner [36] for square-free N with some mild restriction.

Together with the theorem of Yuan–Zhang–Zhang on Gross–Zagier formula for Shimura curves [45] and Kolyvagin theorem [23], we may prove the p-part of the refined Birch–Swinnerton-Dyer formula (shortened as "B-SD formula" in the rest of the paper) for E/K in the rank one case under the same assumption as in Theorem 1.1 (see Theorem 10.2). By a careful choice of auxiliary quadratic field K, we may deduce the p-part of the B-SD formula for $E/\mathbb{Q}$ in the rank one case (cf. Theorem 10.3).

Theorem 1.6. *Let* (E, p) *be as in Theorem 1.4. If* $\mathrm{ord}_{s=1}L(E/\mathbb{Q}, s) = 1$*, then the p-part of the B-SD formula for* $E/\mathbb{Q}$ *holds:*

$$\left|\frac{L'(E/\mathbb{Q},1)}{\Omega_E \cdot \mathrm{Reg}(E/\mathbb{Q})}\right|_p = \left|\#\text{Ш}(E/\mathbb{Q}) \cdot \prod_{\ell | N} c_\ell\right|_p,$$

where the regulator is defined by $\mathrm{Reg}(E/\mathbb{Q}) := \frac{\langle y,y\rangle_{NT}}{[E(\mathbb{Q}):\mathbb{Z}y]^2}$ *for any non-torsion* $y \in E(\mathbb{Q})$*,* $\langle y, y\rangle_{NT}$ *is the Néron-Tate height pairing, and* c_ℓ *is the local Tamagawa number of* $E/\mathbb{Q}_\ell$*.*

Remark 4. Skinner–Urban and Kato [37, Theorem 2] have proved the p-part of the B-SD formula in the rank zero case for any good ordinary p with certain conditions (less restrictive than ours).

Remark 5. With the Gross–Zagier formula, the previous result of Kolyvagin [23] shows that, in the analytic rank one case, the p-part of the B-SD formula for E/K is equivalent to a certain p-indivisibility property of κ^∞. Under the condition of the Theorem 10.2 we prove such property (i.e., $\mathscr{M}_\infty = 0$). One then obtains the p-part of the B-SD formula for $E/\mathbb{Q}$ with the help of the theorem of Kato and Skinner–Urban on the B-SD formula in the rank zero case.

We now give an overview of the proof of Theorem 1.1. We start with the simpler case where the p-Selmer group of E/K has rank one. Let g be the modular form associated with E, choose a level-raising prime ℓ which is inert in K, and a modular form g_ℓ (of level $N\ell$) congruent to g modulo p. Using a Čebotarev argument, this ℓ may be chosen so that the relevant p-Selmer group for g_ℓ has lower rank, hence trivial. By the deep result of Kato and

Skinner–Urban on the rank zero B-SD formula, the central value of the L-function attached to g_ℓ must be a p-adic unit. A Jochnowitz-type congruence of Bertolini–Darmon allows us to conclude that the Heegner point y_K has nontrivial Kummer image in $H^1(K_\ell, E[p])$, and hence is nonzero. To treat the general case, we use induction on the dimension of the p-Selmer group of E/K. The induction proceeds by applying level-raising at two suitable primes to reduce the rank of the p-Selmer group. We refer to §9 for more details.

Notations

(i) $p \geq 5$: a prime such that $(p, N) = 1$.

(ii) $\mathbb{A}$: the adeles of $\mathbb{Q}$. $\mathbb{A}_f$: the finite adeles of $\mathbb{Q}$. $\mathbb{A}_f^m$: the finite adeles of $\mathbb{Q}$ away from the primes dividing m.

(iii) For an integer n, we denote by $\nu(n)$ the number of distinct prime factors of n.

(iv) g: a newform of weight two on $\Gamma_0(N)$ (hence with trivial nebentypus), with Fourier expansion

$$\sum_{n\geq 1} a_n(g) q^n, \quad a_1 = 1.$$

The field of coefficient is denoted by $F = F_g$ and its ring of integer by $\mathscr{O} = \mathscr{O}_g$.

(v) $\mathfrak{p} : F \hookrightarrow \overline{\mathbb{Q}}_p$ a place above p, $F_\mathfrak{p}$ the corresponding completion of F. We also denote by $\mathfrak{p}$ the prime ideal $\mathscr{O} \cap \mathfrak{m}_{\overline{\mathbb{Z}}_p}$ of $\mathscr{O}$, $\mathscr{O}_\mathfrak{p}$ the completion of $\mathscr{O}$ at $\mathfrak{p}$. The modular form g is assumed to be good ordinary at p, i,e,:

$$a_p \notin \mathfrak{p}.$$

Equivalently, $v_\mathfrak{p}(a_p) = 0$ where $v_\mathfrak{p} : \mathscr{O}_\mathfrak{p} \to \mathbb{Z}$ is the $\mathfrak{p}$-adic valuation.

(vi) We denote by $\mathscr{O}_0 \subset \mathscr{O}$ the order generated over $\mathbb{Z}$ by the Fourier coefficients $a_n(g)$'s of g. Let $\mathfrak{p}_0 = \mathfrak{p} \cap \mathscr{O}_0$, and

$$k_0 := \mathscr{O}_0/\mathfrak{p}_0 \subset k := \mathscr{O}/\mathfrak{p}.$$

Both are finite fields of characteristic p. Let $\mathscr{O}_\mathfrak{p}$ ($\mathscr{O}_{0,\mathfrak{p}_0}$, resp.) be the $\mathfrak{p}$-adic ($\mathfrak{p}_0$-adic, resp.) completion of $\mathscr{O}$ ($\mathscr{O}_0$, resp.).

(vii) $A = A_g$: a GL_2-type abelian-variety over $\mathbb{Q}$ attached to g, unique up to isogeny. We always choose an isomorphism class A with an embedding $\mathscr{O} \hookrightarrow \mathrm{End}_{\mathbb{Q}}(A)$. Then the $\mathfrak{p}$-adic Tate module $T_{\mathfrak{p}}(A) = \operatorname{proj\,lim} A[\mathfrak{p}^i]$ is a free $\mathscr{O}_{\mathfrak{p}}$-module of rank two with a Galois representation

$$\rho_{A,\mathfrak{p}} : \mathrm{Gal}_{\mathbb{Q}} \to \mathrm{GL}_{\mathscr{O}_{\mathfrak{p}}}(T_{\mathfrak{p}}(A)), \quad \mathrm{Gal}_{\mathbb{Q}} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}).$$

Denote by $\overline{\rho}_{A,\mathfrak{p},M}$ the reduction modulo $\mathfrak{p}^M$ of $\rho_{A,\mathfrak{p}}$:

$$\overline{\rho}_{A,\mathfrak{p},M} : \mathrm{Gal}_{\mathbb{Q}} \to \mathrm{Aut}_{\mathscr{O}_{\mathfrak{p}}}(A[\mathfrak{p}^M]) \simeq \mathrm{GL}_2(\mathscr{O}/\mathfrak{p}^M).$$

By [7], the Galois representation $\rho_{A,\mathfrak{p}}$ is actually defined over the smaller subring $\mathscr{O}_{0,\mathfrak{p}_0} \subset \mathscr{O}_{\mathfrak{p}}$:

$$\rho_{A,\mathfrak{p}_0} : \mathrm{Gal}_{\mathbb{Q}} \to \mathrm{GL}_2(\mathscr{O}_{0,\mathfrak{p}_0}) \subset \mathrm{GL}_2(\mathscr{O}_{\mathfrak{p}}),$$

such that

$$\rho_{A,\mathfrak{p}} = \rho_{A,\mathfrak{p}_0} \otimes_{\mathscr{O}_{0,\mathfrak{p}_0}} \mathscr{O}_{\mathfrak{p}}. \tag{1.2}$$

(viii) We consider the reduction of $\rho_{A,\mathfrak{p}}$ and $\rho_{A,\mathfrak{p}_0}$. We will write the underlying representation space of $\overline{\rho}_{A,\mathfrak{p}}$:

$$V_k = A[\mathfrak{p}]$$

as a $k = \mathscr{O}/\mathfrak{p}$-vector space of dimension two, endowed with the action of $\mathrm{Gal}_{\mathbb{Q}}$. By (1.2) it can be obtained from by extending scalars from k_0 to k, i.e., there is a two-dimensional k_0-vector subspace V with $\mathrm{Gal}_{\mathbb{Q}}$-action such that

$$V_k = V \otimes_{k_0} k. \tag{1.3}$$

(ix) We will *always* assume that the residual Galois representation

$$\overline{\rho}_{A,\mathfrak{p}_0} : \mathrm{Gal}_{\mathbb{Q}} \to \mathrm{GL}(V) \simeq \mathrm{GL}_2(k_0)$$

is surjective[2]. In particular, $\overline{\rho}_{A,\mathfrak{p}_0}$ (and hence $\overline{\rho}_{A,\mathfrak{p}}$) is absolutely irreducible since p is odd. Then A is unique up to prime-to-$\mathfrak{p}$ isogeny. In this case, we may also write $\overline{\rho}_{g,\mathfrak{p},M}$ for $\overline{\rho}_{A,\mathfrak{p},M}$ since it depends only on g, but not on A.

[2]This impose strong conditions on k_0 and indeed implies that $k_0 = \mathbb{F}_p$. But this suffices for our purpose.

(x) $K = \mathbb{Q}[\sqrt{-D}]$: an imaginary quadratic of discriminant $-D = D_K < 0$ with $(D, N) = 1$. The field K determines a factorization $N = N^+N^-$ where the factors of N^+ (N^-, resp.) are all split (inert, resp.). Let g^K (A^K, resp.) be the quadratic twist of g (A, resp.). *Throughout this paper, N^- is square-free.*

(xi) We will consider the base change L-function (without the archimedean local factors) $L(g/K, s) = L(g/\mathbb{Q}, s)L(g^K/\mathbb{Q}, s)$. We use the classical normalization so that the functional equation is centered at $s = 1$. Then the root number (i.e., the sign of the functional equation of the L-function $L(g/K, s)$) is given by

$$\epsilon(g/K) = (-1)^{\#\{\nu(N^-)+1} \in \{\pm 1\}. \tag{1.4}$$

(xii) Λ: the set of square free products n of Kolyvagin primes ℓ's. We also include 1 into Λ. Recall that a prime ℓ is called a Kolyvagin prime if ℓ is prime to NDp, inert in K and the Kolyvagin index

$$M(\ell) := \min\{v_{\mathfrak{p}}(\ell + 1), v_{\mathfrak{p}}(a_\ell)\}$$

is strictly positive. Define for $n \in \Lambda$:

$$M(n) = \min\{M(\ell) : \ell | n\},$$

if $n > 1$ and $M(1) = \infty$. Write Λ_r as the set of $n \in \Lambda$ with exactly r factors. Define

$$M_r = \min\{M(n) : n \in \Lambda_r\}.$$

Note that the set Λ depends only on the residue Galois module $\overline{\rho}_{g,\mathfrak{p}}$. Denote by $\Lambda^\pm$ the set of $n \in \Lambda$ such that $(-1)^{\nu(n)} = \pm 1$.

(xiii) For n coprime to D_K, we denote by $\mathcal{O}_{K,n} = \mathbb{Z} + n\mathcal{O}_K$ the order of conductor n, and by $K[n]$ the ring class field of conductor n.

(xiv) Λ': the set of square free products m of admissible primes (after Bertolini–Darmon) q. Recall that a prime q is called admissible if q is prime to NDp, inert in K, p does not divide $q^2 - 1$, and the index

$$v_{\mathfrak{p}}((q + 1)^2 - a_q^2) \geq 1.$$

Similarly define Λ'_r, $\Lambda'^{\pm}$ etc.. Note that the two sets Λ and Λ' are disjoint.

(xv) Let $\mathrm{Ram}(\overline{\rho}_{g,\mathfrak{p}})$ denote the set of $\ell || N$ such that $\overline{\rho}_{g,\mathfrak{p}}$ is ramified at ℓ. We will consider the following hypothesis, called Hypothesis $\heartsuit$, for $(g, \mathfrak{p}, K)$:

(1)$\mathrm{Ram}(\overline{\rho}_{g,\mathfrak{p}})$ contains all prime factors $\ell || N^+$ and all $q|N^-$ such that $q \equiv \pm 1 \mod p$.

(2)If N is not square-free, then $\#\mathrm{Ram}(\overline{\rho}_{g,\mathfrak{p}}) \geq 1$, and either $\mathrm{Ram}(\overline{\rho}_{g,\mathfrak{p}})$ contains a prime $\ell || N^-$ or there are at least two primes factors $\ell || N^+$.

(3)For all prime ℓ with $\ell^2 | N^+$, we have $H^1(\mathbb{Q}_\ell, \overline{\rho}_{g,\mathfrak{p}}) = \overline{\rho}_{g,\mathfrak{p}}^{\mathrm{Gal}_\ell} = 0$. Here $\mathrm{Gal}_\ell \subset \mathrm{Gal}_{\mathbb{Q}}$ denotes a decomposition group at ℓ.

2. Level-raising of modular forms

We first recall the level-raising of Ribet, following Diamond–Taylor's generalization [10, 11].

Theorem 2.1 (Ribet, Diamond–Taylor)**.** *Let g be a newform of weight two of level N (and trivial nebentypus). Let $\mathfrak{p}$ be a prime of $\mathscr{O}_g$ such that $\overline{\rho}_{g,\mathfrak{p}}$ is irreducible with residue characteristic $p \geq 5$. Then for each admissible prime q, there exists a newform g' of level Nq (and trivial nebentypus), with a prime $\mathfrak{p}'$ of $\mathscr{O}_{g'}$ and $\mathscr{O}_{g',0}/\mathfrak{p}'_0 \simeq \mathscr{O}_{g,0}/\mathfrak{p}_0 = k_0$ such that*

$$\overline{\rho}_{g,\mathfrak{p}_0} \simeq \overline{\rho}_{g',\mathfrak{p}'_0}.$$

Equivalently, for all primes $\ell \neq q$, we have

$$a_\ell(g) \mod \mathfrak{p} \equiv a_\ell(g') \mod \mathfrak{p}',$$

where both sides lie in k_0.

Proof. Fix a place of $\overline{\mathbb{Q}}$ above a prime ℓ, and let $\mathrm{Gal}_\ell \hookrightarrow \mathrm{Gal}_{\mathbb{Q}}$ be the corresponding decomposition group. For $\ell \neq q$, we denote by τ_ℓ the restriction of $\rho_{g,\mathfrak{p}}$ to Gal_ℓ. At $\ell = q$, let τ_ℓ be the p-adic representation of Gal_q corresponding to an unramified twist of the Steinberg representation under the local Langlands correspondence, such that $\overline{\tau}_q$ is isomorphic to the restriction of $\overline{\rho}_{g,\mathfrak{p}_0}$ to Gal_q. Such τ_q exists because $a_q(g) \equiv \pm(q+1) \mod \mathfrak{p}$ by the admissibility of q. Then we apply [11, Theorem 1] (cf. [10, Theorem B]) to obtain a weight two modular form g' of level dividing Nq, and a prime $\mathfrak{p}'$ such that the representation $\rho_{g',\mathfrak{p}'}$ has the prescribed restriction to the inertial subgroups I_ℓ: $\rho_{g',\mathfrak{p}'}|_{I_\ell} \simeq \tau_\ell|_{I_\ell}$ for all $\ell \neq p$. Since the level of g' depends only on the restriction of $\rho_{g',\mathfrak{p}'}$ to the inertia I_ℓ for all ℓ, we see that its level is divisible by Nq and hence equal to Nq. To see that g' has trivial nebentypus, we note that the character $\det(\rho_{g',\mathfrak{p}'})$ is the p-adic cyclotomic character ϵ_p twisted by a character χ of $\mathrm{Gal}_{\mathbb{Q}}$. Since the level of g' is prime to p, χ is unramified at p. Since g has trivial nebentyputs, by $\det(\rho_{g,\mathfrak{p}})|_{I_\ell} \simeq \det(\rho_{g',\mathfrak{p}'})|_{I_\ell}$ for all

$\ell \neq p$, the character χ is unramified at all primes $\ell \neq p$. It follows that χ is unramified at all primes ℓ and hence $\chi = 1$ and g' has trivial nebentypus. This completes the proof. $\square$

Let $m \in \Lambda'$ be a product of distinct admissible primes. By Theorem 2.1, we obtain a weight-two newform g_m of level Nm together with a prime $\mathfrak{p}_m$ of $\mathscr{O}_{g_m}$. Here all notations for g will have their counterparts for g_m and we will simply add an index m in a self-evident way. We have the residue field $k_m = \mathscr{O}_{g_m}/\mathfrak{p}_m$ and *isomorphic* subfields $k_0 = \mathscr{O}_{g,0}/\mathfrak{p}_0 \simeq \mathscr{O}_{g_m,0}/\mathfrak{p}_{m,0}$. The isomorphism will be fixed in the rest of the paper. The modular form g_m and g carry isomorphic $\mathrm{Gal}_{\mathbb{Q}}$-actions on the two-dimensional k_0-vector space

$$\overline{\rho}_{g_m,\mathfrak{p}_{m,0}} \simeq \overline{\rho}_{g,\mathfrak{p}_0}.$$

We will fix an isomorphism and denote the underlying two-dimensional k_0-vector space by V.

3. Shimura curves and Heegner points

3.1. Shimura curves and Shimura sets.

Let $N = N^+N^-$, $(N^+, N^-) = 1$ and N^- square-free. In this section we assume that the number of prime factors of N^- is *even*.

For $m \in \Lambda'^+$ (i.e., m has an even number of prime factors), let $B(N^-m)$ be the quaternion algebra over $\mathbb{Q}$ ramified precisely at N^-m (in particular, indefinite at the archimedean place). We let X_{N^+,N^-m} be the (compactified) Shimura curve defined by the indefinite quaternion algebra $B(N^-m)$ with the $\Gamma_0(N^+)$-level structure.

For $m \in \Lambda'^-$, let $B(N^-m\infty)$ be the quaternion algebra over $\mathbb{Q}$ ramified precisely at $N^-m\infty$ (in particular, definite at the archimedean place). We let $X_m := X_{N^+,N^-m}$ be the double coset space defined by the definite quaternion algebra $B(N^-m\infty)$ with the $\Gamma_0(N^+)$-level (sometimes called *"Gross curve"* in the literature, [43, §2]):

$$X_{N^+,N^-m} = B^\times \backslash B(\mathbb{A}_f)^\times / \widehat{R}^\times,$$

where $B = B(N^-m\infty)$, and R is an Eichler order of level N^+. We will call it a *Shimura set*.

For short we will write (noting that $N = N^+N^-$ is fixed) B_m for $B(N^-m)$ when $m \in \Lambda'^+$, or $B(N^-m\infty)$ when $m \in \Lambda'^-$. We write the Eichler order in B_m by R_m. We also write

$$X_m = X_{N^+,N^-m}. \tag{3.1}$$

For example, if $N^- = 1$, we have $X_1 = X_0(N)$.

From now on, we will fix an isomorphism between $B\otimes_{\mathbb{Q}}\mathbb{Q}_\ell$ and the matrix algebra $M_{2,\mathbb{Q}_\ell}$ (a fixed division algebra over $\mathbb{Q}_\ell$, resp.) if a quaternion algebra B over $\mathbb{Q}$ is unramified (ramified, resp.) at a (possibly archimedean) prime ℓ. This will allow us, for example, to identify $B_m(\mathbb{A}_f^{(\ell)})$ with $B_{m\ell}(\mathbb{A}_f^{(\ell)})$ for $\ell, m \in \Lambda'$ and $\ell \nmid m$.

3.2. Heegner points on Shimura curves

Let $m \in {\Lambda'}^+$ and $A_m = A_{g_m}$ a quotient of the Jacobian $J(X_m)$:

$$\pi : J(X_m) \to A_m.$$

Let $n \in \Lambda$ be a product of Kolyvagin primes. We now define a system of points defined over the ring class field $K[n]$:

$$x_m(n) \in X_m(K[n]), \quad y_m(n) \in A_m(K[n]).$$

Remark 6. We need to be careful when defining $y_m(n)$. We may define an embedding $X_m \to J$ by $x \mapsto (x) - (\infty)$ if X_m is the modular curve $X_0(N^+)$, i.e., $N^-m = 1$. In general, there is no natural base point to embed X_m into its Jacobian. We may take a certain Atkin-Lehner involution w and take $y_m(n) \in A_m(K[n])$ to be the image of the degree-zero divisor $(x) - (w(x))$ where $x = x_m(n)$. This works if the Atkin-Lehner involution acts on A_m by -1. Otherwise, we may take a fixed auxiliary prime ℓ_0 and define $y_m(n)$ to be the image of the degree-zero divisor $(\ell_0 + 1 - T_{\ell_0})x_m(n)$. This does not lose generality if $(\ell_0 + 1 - a_{\ell_0}(g_m))$ is a $\mathfrak{p}_m$-adic unit. Such ℓ_0 exists, for example, if $\overline{\rho}_{g_m,\mathfrak{p}_{m,0}}$ is surjective. Furthermore, since we wish to eliminate the dependence on the choice of ℓ_0 (up to torsion points), we will define $y_m(n)$ to be the image of the divisor with $\mathbb{Q}$-coefficients

$$\widetilde{x}_m(n) := \frac{1}{\ell_0 + 1 - a_{\ell_0}(g_m)}(\ell_0 + 1 - T_{\ell_0})x_m(n) \tag{3.2}$$

viewed as an element in $A_m(K[n]) \otimes_{\mathbb{Z}} \mathbb{Q}$.

Remark 7. The definition of $y_m(n)$ also involves a parametrization π of A_m by $J(X_m)$, as well as a choice A_m in the isogeny class determined by g. We will take either the optimal quotient (which has only $\mathscr{O}_{g_m,0}$-multiplication in general) or one with $\mathscr{O}_{g_m}$-multiplication. But for the moment we do not want to specify the choice yet.

We describe the points $x_m(n)$ in terms of the complex uniformization of X_m. The complex uniformization of X_m is given by

$$X_m(\mathbb{C}) = B_m^\times \backslash \mathcal{H}^\pm \times B_m(\mathbb{A}_f)^\times / \widehat{R_m}^\times, \quad \mathcal{H}^\pm := \mathbb{C} \setminus \mathbb{R}.$$

Fix an (optimal) embedding

$$K \hookrightarrow B_m \tag{3.3}$$

such that $R \cap K = \mathcal{O}_K$. Such an embedding exists since all primes dividing N^+ are assumed to be split in K. Then we have a unique fixed point h_0 of $K^\times$ on $\mathcal{H}^+$. Then the total set of Heegner points is given by (cf. [42]):

(3.4)
$$\mathscr{C}_m = \mathscr{C}_{K,m} = B_m^\times \backslash (B_m(\mathbb{Q})^\times h_0) \times B_m(\mathbb{A}_f)^\times / \widehat{R_m}^\times \simeq K^\times \backslash B_m(\mathbb{A}_f)^\times / \widehat{R_m}^\times.$$

In this paper, we only need to use a subset of $\mathscr{C}_K$. Let

$$B_m(\mathbb{A}_f)^{\times,+} = K^\times \left(\prod_\ell{}' B_m(\mathbb{Q}_\ell)^\times \right) \widehat{R_m}^\times,$$

where the restricted direct product for ℓ runs over all inert primes such that $(\ell, Nm) = 1$ and $\ell \equiv -1 \mod p$ (hence $B_m(\mathbb{A}_f)^{\times,+}$ implicitly depends on the prime p). Define

$$\mathscr{C}_m^+ = K^\times \backslash B_m(\mathbb{A}_f)^{\times,+} / \widehat{R_m}^\times. \tag{3.5}$$

There is a Galois action of $\mathrm{Gal}(K^{\mathrm{ab}}/K)$ on $\mathscr{C}_{K,m}$ given by

$$\sigma([h]) = [\mathrm{rec}(\sigma) h], \tag{3.6}$$

where $[h] \in \mathscr{C}_{K,m}$ is a double coset of $h \in B_m(\mathbb{A}_f)^\times$, and we have the reciprocity map given by class field theory

$$\mathrm{rec} : \mathrm{Gal}(K^{\mathrm{ab}}/K) \simeq K^\times \backslash \widehat{K}^\times.$$

We now may define more explicitly the point $x_m(n)$ already mentioned earlier: in the set $\mathscr{C}_K^+$, the point $x_m(n)$ for $n \in \Lambda$ corresponds to the coset of $h = (h_\ell) \in B_m(\mathbb{A}_f)^{\times,+}$ where

$$h_\ell = \begin{cases} \begin{pmatrix} \ell & 0 \\ 0 & 1 \end{pmatrix}, & \ell | n, \\ 1, & (\ell, n) = 1. \end{cases} \tag{3.7}$$

When $m = 1$ or there is no confusion, we simply write

$$x(n) = x_m(n), \quad y(n) = y_m(n). \tag{3.8}$$

3.3. Heegner points on Shimura sets

When $m \in \Lambda'$ has *odd* number of prime factors, we have the Shimura set:

$$X_m = B_m^\times \backslash B_m(\mathbb{A}_f)^\times / \widehat{R_m}^\times. \tag{3.9}$$

The Shimura set is a finite set. Again fix an optimal embedding $K \hookrightarrow B_m$. We then define the set $\mathscr{C}_{K,m}$ of *Heegner points* on the Shimura set X_m by

$$\mathscr{C}_m = \mathscr{C}_{K,m} = K^\times \backslash B_m(\mathbb{A}_f)^\times / \widehat{R_m}^\times. \tag{3.10}$$

Similarly we may define the set $\mathscr{C}_{K,m}^+$, and an action of the Galois group $\mathrm{Gal}(K^{\mathrm{ab}}/K)$ on the set $\mathscr{C}_{K,m}$ by the formula (3.6). We again consider the Heegner points given by the same formula as (3.7)

$$x_m(n) \in \mathscr{C}_{K,m}, \quad n \in \Lambda.$$

We have a natural map (usually not injective)

$$\mathscr{C}_{K,m} \to X_m. \tag{3.11}$$

When there is no ambiguity, we will consider $x_m(n)$ as an element in the Shimura set X_m.

3.4. Reduction of Shimura curves

We consider the reduction of the canonical integral model of $X_m = X_{N^+,N^-m}$ at a prime q, where $m \in \Lambda'^+$.

First let q be an admissible prime not dividing the level Nm. Then X_m has an integral model over $\mathbb{Z}_q$ parametrizing abelian surfaces with auxiliary structure (cf. [1] for the detail). The integral model has good reduction at q and the set of supersingular points $X_m(\mathbb{F}_{q^2})^{\mathrm{ss}}$ are naturally parameterized by the Shimura set X_{mq}:

$$X_m(\mathbb{F}_{q^2})^{\mathrm{ss}} \simeq X_{mq}, \tag{3.12}$$

where $mq \in \Lambda^{'-}$. This identification needs to choose a base point, which we will choose to be the reduction of the Heegner point corresponding to the identity coset in (3.4) (cf. the convention before (3.18)). Via the moduli interpretation of the integral model of X_m, this choice of base point also gives an embedding of K (as the endomorphism algebra of the abelian surface $\mathcal{A}$ preserving the auxiliary structure, corresponding to the base point) into the quaternion algebra B_{mq} (as the endomorphism algebra of the special fiber of the $\mathcal{A}$):

$$K \hookrightarrow B_{mq}. \tag{3.13}$$

Now let $q|m$ be a prime. Then the curve X_m has a semistable integral model, denoted by $X_{m,\mathbb{Z}_p}$, over $\mathbb{Z}_q$ by a moduli interpretation via Drinfeld's special action by a maximal order in a quaternion algebra [1]. We will consider the base change to $\mathbb{Z}_{q^2}$, the unramified quadratic extension of $\mathbb{Z}_q$. Let $(\mathscr{E}(X_m), \mathscr{V}(X_m))$ be the *dual reduction graph* of the special fiber $X_{m,\mathbb{F}_{q^2}}$ of $X_{m,\mathbb{Z}_{q^2}}$, where $\mathscr{E}(X_m)$ ($\mathscr{V}(X_m)$, resp.) denotes the set of edges (vertices, resp.). The graph is constructed such that each vertex corresponds to an irreducible component and two vertices are adjacent if and only if their corresponding components have an intersecting point. By [34, Prop. 4.4], it follows from the Cerednik–Drinfeld uniformization [1, Theorem 5.2] that the special fiber $X_{m,\mathbb{F}_{q^2}}$ is a union of projective lines crossing transversely. Moreover, the set of irreducible components of $X_{\mathbb{F}_{q^2}}$ can be identified with two copies of the Shimura set $X_{m/q}$:

$$\mathscr{V}(X_m) \simeq X_{m/q} \times \mathbb{Z}/2\mathbb{Z}, \tag{3.14}$$

where $m/q \in \Lambda^{'-}$. We choose the base point to be the irreducible component corresponding to the *unique* irreducible component containing the reduction of the base point of Heegner points in (3.4). The uniqueness follows from the fact that Heegner points in (3.4) are reduced to a non-singular point on the special fiber (cf. [4, §8, p.55]). This also induces an embedding (*loc. cit.*)

$$K \hookrightarrow B_{m/q}. \tag{3.15}$$

Under this identification, the Atkin-Lehner involution at q acts by changing the second factor of the above product. So does the Frobenius for the quadratic extension $\mathbb{F}_{q^2}/\mathbb{F}_q$. For our later purpose, we also give the adelic description (cf. [34, §4], [47, Lemma 5.4.4]):

$$\mathscr{V}(X_m) = B_0^\times \backslash \mathrm{GL}_2(\mathbb{Q}_q)/\mathbb{Q}_q^\times \mathrm{GL}_2(\mathbb{Z}_q) \times B(\mathbb{A}_f^q)^\times / \widehat{R}^{q,\times}, \tag{3.16}$$

where $B = B_{m/q}$ and $B_0^\times \subset B^\times$ is the kernel of $\gamma \mapsto \mathrm{ord}_q(\det(\gamma))$ (here det denotes the reduced norm on B). The group $B_0^\times$ acts diagonally by left multiplication on the product. Then the isomorphism (3.14) is defined as follows: for a given $B_0^\times$-coset $[h_q, h^q]$, we send it to the $B^\times$-coset $[h_q, h^q]$ in the Shimura set $X_{m/q}$, to $\mathrm{ord}_q(\det(h_q)) \mod 2$ in $\mathbb{Z}/2\mathbb{Z}$. This defines the isomorphism in (3.16). We thus write

$$\mathscr{V}(X_m) = \mathscr{V}_0(X_m) \sqcup \mathscr{V}_1(X_m) \tag{3.17}$$

as a disjoint union according to $\mathrm{ord}_q(\det(h_q)) \mod 2$. Noting that $\mathbb{Q}$ has class number one and $\det(\widehat{R}^\times) = \widehat{\mathbb{Z}}^\times$, we have an equivalent description to (3.9):

$$X_{m/q} = B_{m/q}^\times \backslash B_{m/q}(\mathbb{A}_f)^\times / \mathbb{Q}_q^\times \cdot \widehat{R_{m/q}}^\times.$$

From this description and the isomorphism (3.14), we will identify $X_{m/q}$ with the subset $\mathscr{V}_0(X_m) \simeq X_{m/q} \times \{0\}$ of $\mathscr{V}(X_m)$.

3.5. Reduction of Heegner points

We consider Heegner points (CM points in [42, 45]) on the Shimura curves X_m, for $m \in \Lambda'^+$.

Let $q \in \Lambda'$ be a prime not dividing m. Then X_m has good reduction at q. The Heegner points in $\mathscr{C}_{K,m}^+$ are defined over abelian extensions of K over which the prime $(q) \subset \mathcal{O}_K$ splits completely. Let $K(q)$ be an abelian extension of K containing all these fields and we fix a choice of a prime $\mathfrak{q}$ above $(q) \subset \mathcal{O}_K$. This allows us to reduce these points modulo $\mathfrak{q}$. Identifying $\mathcal{O}_{K(q)}/\mathfrak{q} \simeq \mathbb{F}_{q^2}$, they all reduce to supersingular points on $X_{m,\mathbb{F}_{q^2}}$. We write the composition of the isomorphism (3.12) with the reduction map as:

$$\mathrm{Red}_q : \mathscr{C}_{K,m}^+ \to X_{mq}. \tag{3.18}$$

This is given by (3.5) and the following map:

$$\begin{aligned} K^\times\backslash B_m(\mathbb{A}_f)^{\times,+}/\widehat{R_m}^\times &\to B_{mq}^\times\backslash\mathbb{Q}_q^\times \times B_{mq}(\mathbb{A}_f^q)^\times/(\mathbb{Z}_q^\times)\cdot(R_{mq}\otimes\widehat{\mathbb{Z}}^q)^\times \\ &\to B_{mq}^\times\backslash B_{mq}(\mathbb{A}_f)^\times/\widehat{R_{mq}}^\times \end{aligned}$$

where the first arrow at the q-th component is induced by $b\in \mathrm{GL}_2(\mathbb{Q}_q)\mapsto \det(b)\in\mathbb{Q}_q$, the second one is an isomorphism induced by the reduced norm on the division algebra $\det: B_{mq}(\mathbb{Q}_q)^\times/\mathcal{O}_{B_{mq}(\mathbb{Q}_q)}^\times\to\mathbb{Q}_q^\times/\mathbb{Z}_q^\times$ (cf. [47, Lemma 5.4.3]). We are implicitly using the embedding $K\hookrightarrow B_{mq}$ given by (3.13).

Now let $q\in\Lambda'$ be a prime dividing m. Similarly as in the last paragraph, we choose a prime $\mathfrak{q}$ of $K(q)$ above q and identify $\mathcal{O}_{K(q)}/\mathfrak{q}\simeq\mathbb{F}_{q^2}$ to reduce the Heegner points to the special fiber $X_{m,\mathbb{F}_{q^2}}$. Any point in the set $\mathscr{C}^+_{K,Nm}$ reduces to a non-singular point of the special fiber $X_{m,\mathbb{F}_{q^2}}$ (cf. [4, §8, p.55]). Hence we have a specialization map from $\mathscr{C}^+_{K,Nm}$ to the set of irreducible components $\mathscr{V}$. Since the q-component of an element in $\mathscr{C}^+_{K,Nm}$ has reduced norm of even valuation, the specialization of $\mathscr{C}^+_{K,Nm}$ lies in the subset $X_{m/q}\times\{0\}$ of $\mathscr{V}$. We thus write the specialization map as

$$\mathrm{Sp}_q:\mathscr{C}^+_{K,m}\to X_{m/q}. \tag{3.19}$$

The specialization is given by (3.5) and the following map:

$$\begin{aligned} K^\times\backslash B_m(\mathbb{A}_f)^{\times,+}/\widehat{R_m}^\times &\to K^\times\backslash B_m(\mathbb{A}_f^q)^{\times,+}/(R_m\otimes\widehat{\mathbb{Z}}^q)^\times \\ &\to B_{m/q}^\times\backslash B_{m/q}(\mathbb{A}_f)^\times/\widehat{R_{m/q}}^\times, \end{aligned}$$

where the first arrow is given by forgetting the q-th opponent, and the second one maps $[h^q]$ to $[1,h^q]$ for $h^q\in B_m(\mathbb{A}_f^q)\simeq B_{m/q}(\mathbb{A}_f^q)$ (cf. [47, Lemma 5.4.6]). We are implicitly using the embedding $K\hookrightarrow B_{mq}$ given by (3.15).

3.6. Geometric congruence between Heegner points

The main geometric observation is the following congruence between coherent and incoherent Heegner points.

Theorem 3.1. *Let m be in Λ'^+, X_m the Shimura curve X_{N^+,N^-m}. Then we have the following relation:*

- *When a prime $q\in\Lambda'$ does not divide $m\in\Lambda'^+$,*

$$\mathrm{Red}_q(x_m(n)) = x_{mq}(n)\in\mathscr{C}_{mq,K}.$$

In particular, we have $\mathrm{Red}_q(x_m(n)) = x_{mq}(n) \in X_{mq}$*, under (3.11).*

- *When a prime* $q \in \Lambda'$ *divides* $m \in \Lambda'^{+}$,

$$\mathrm{Sp}_q(x_m(n)) = x_{m/q}(n) \in X_{m/q}.$$

Proof. This follows from the description of the reduction of Heegner points (3.18), (3.19). □

3.7. Kolyvagin cohomology classes

We now prepare to formulate the Kolyvagin conjecture for GL_2-type abelian variety analogous to [24] for elliptic curves. We first define Kolyvagin cohomology classes.

We consider a newform g of level N with a prime $\mathfrak{p}$ of $\mathscr{O}$ satisfying the hypothesis in "Notations". Let $A = A_g$ be an associated GL_2-type abelian variety over $\mathbb{Q}$ with real multiplication by $\mathscr{O}$. Let X be $X_1 = X_{N^+,N^-}$. The abelian variety A_g may not be an optimal quotient of $J(X)$. Possibly changing A in its isogeny class (still with $\mathscr{O}$-multiplication), we will choose a parameterization

$$J(X) \to A \tag{3.20}$$

such that the image of the induced homomorphism on the p-adic Tate module

$$\mathbf{T}_p(J(X)) \to \mathbf{T}_p(A)$$

is not contained in $\mathfrak{p}\mathbf{T}_p(A)$. We say that such a parameterization is $(\mathscr{O},\mathfrak{p})$-*optimal* and that the abelian variety A is $(\mathscr{O},\mathfrak{p})$-*optimal*. To see that an $(\mathscr{O},\mathfrak{p})$-optimal parameterization exists, we note that there exists another A' with $\mathscr{O}$-multiplication and an $\mathscr{O}$-isogeny $A' \to A$ such that the image of the induced homomorphism on the p-adic Tate module $\mathbf{T}_p(A') \to \mathbf{T}_p(A)$ is $\mathfrak{p}\mathbf{T}_p(A)$. If the image of $\mathbf{T}_p(J(X)) \to \mathbf{T}_p(A)$ is contained in $\mathfrak{p}\mathbf{T}_p(A)$, the morphism $J(X) \to A$ must factor through A'. We may then replace A by A'.

We now define the Kolyvagin cohomology classes (cf. [15, 23] for elliptic curves). Let T_pA_g be the p-adic Tate module of A_g and consider the $\mathfrak{p}$-adic Tate module:

$$T_\mathfrak{p}A_g := T_pA \otimes_{\mathscr{O}\otimes\mathbb{Z}_p} \mathscr{O}_\mathfrak{p}.$$

It is a free $\mathscr{O}_\mathfrak{p}$-module of rank two. Set

$$A_{g,M} = T_\mathfrak{p}A_g \otimes_{\mathscr{O}_\mathfrak{p}} \mathscr{O}_\mathfrak{p}/\mathfrak{p}^M,$$

and

$$A_{g,\infty} = T_{\mathfrak{p}} A_g \otimes_{\mathscr{O}_{\mathfrak{p}}} F_{\mathfrak{p}}/\mathscr{O}_{\mathfrak{p}},$$

where $F_{\mathfrak{p}}$ is the fraction field of $\mathscr{O}_{\mathfrak{p}}$. We now define

$$c_M(n) \in H^1(K, A_{g,M}), \quad M \le M(n),$$

by applying Kolyvagin's derivative operators to the points $y(n) \in A(K[n]) \otimes \mathbb{Q}$ defined in (3.2). Note that the denominator of $y(n)$ is a $\mathfrak{p}$-adic unit and hence we may interpret $y(n)$ as an element of $A(K[n])_{\mathbb{Z}_p} \otimes_{\mathscr{O}\otimes\mathbb{Z}_p} \mathscr{O}_{\mathfrak{p}}$. Denote $G_n = \mathrm{Gal}(K[n]/K[1])$ and $\mathcal{G}_n = \mathrm{Gal}(K[n]/K)$ for $n \in \Lambda$. Then we have a canonical isomorphism:

$$G_n = \prod_{\ell | n} G_\ell,$$

where the group $G_\ell = \mathrm{Gal}(K[\ell]/K[1])$ is cyclic of order $\ell+1$. Choose a generator σ_ℓ of G_ℓ, and define the Kolyvagin derivative operator

$$\mathbb{D}_\ell := \sum_{i=1}^{\ell+1} i\sigma_\ell^i \in \mathbb{Z}[G_\ell],$$

and

$$\mathbb{D}_n := \prod_{\ell|n} \mathbb{D}_\ell \in \mathbb{Z}[G_n].$$

Fix a set $\mathcal{G}$ of representatives of $\mathcal{G}_n/G_n$. Then we define the derived Heegner point

$$P(n) := \sum_{\sigma\in\mathcal{G}} \sigma(\mathbb{D}_n y(n)) \in A_g(K[n]).$$

We have a commutative diagram of Kummer maps:

$$\begin{array}{ccc} A(K)_{\mathbb{Z}_p} \otimes_{\mathscr{O}\otimes\mathbb{Z}_p} \mathscr{O}_{\mathfrak{p}}/\mathfrak{p}^M & \longrightarrow & H^1(K, A_{g,M}) \\ \downarrow & & \downarrow \mathrm{Res} \\ A(K[n])_{\mathbb{Z}_p} \otimes_{\mathscr{O}\otimes\mathbb{Z}_p} \mathscr{O}_{\mathfrak{p}}/\mathfrak{p}^M & \longrightarrow & H^1(K[n], A_{g,M}) \end{array}$$

where $A(K)_{\mathbb{Z}_p}$ denotes $A(K)\otimes_{\mathbb{Z}} \mathbb{Z}_p$. When $M \le M(n)$, the Kummer image of $P(n)$ in $H^1(K[n], A_{g,M})$ is actually $\mathrm{Gal}(K[n]/K)$-invariant. Since $\overline{\rho}_{g,\mathfrak{p}}$ is essentially surjective and $n \in \Lambda$, we have (cf. [15, Lemma 4.3])

$$A_{g,M}^{\mathrm{Gal}_{K[n]}} = 0.$$

Hence the restriction map

$$H^1(K, A_{g,M}) \to H^1(K[n], A_{g,M})^{\mathrm{Gal}(K[n]/K)}$$

is an isomorphism. The derived point $P(n)$ defines a $\mathrm{Gal}(K[n]/K)$-invariant element in $A(K[n])_{\mathbb{Z}_p} \otimes_{\mathscr{O}\otimes\mathbb{Z}_p} \mathscr{O}_{\mathfrak{p}}/\mathfrak{p}^M$. Hence the Kummer image of $P(n)$ descends to a cohomology class denoted by

$$c_M(n) \in H^1(K, A_{g,M}). \tag{3.21}$$

When $n = 1$, we also denote

$$y_K := P(1) = \mathrm{tr}_{K[1]/K} y(1) \in A(K), \tag{3.22}$$

and the point $y_K \in A(K)$ is usually called the Heegner point. This is the only case where the derivative operator is trivial and hence can be related to suitable L-values via the Waldspurger or Gross–Zagier formula, as we will see.

One could also describe the action of the complex conjugation on the classes $c_M(n)$. Let $\epsilon \in \{\pm 1\}$ be the root number of A_g. Define

$$\nu(n) = \#\{\ell : \ell | n\}, \tag{3.23}$$

and

$$\epsilon_\nu = \epsilon \cdot (-1)^{\nu+1} \in \{\pm 1\}. \tag{3.24}$$

Then the class $c_M(n)$ lies in the $\epsilon_{\nu(n)}$-eigenspace under complex conjugation ([15, Prop. 5.4], [2, Prop. 2.6]):

$$c_M(n) \in H^1(K, A_{g,M})^{\epsilon_{\nu(n)}}.$$

3.8. Kolyvagin's conjecture.

Let $\mathscr{M}(n) \in \mathbb{Z}_{\geq 0} \cup \{\infty\}$ be the divisibility index of the class $c(n)$, i.e., the maximal $\mathscr{M} \in \mathbb{Z}_{\geq 0} \cup \{\infty\}$ such that $c_M(n) \in \mathfrak{p}^{\mathscr{M}} H^1(K, A_{g,M})$ for all $M \leq M(n)$. Define $\mathscr{M}_r$ to be the minimal $\mathscr{M}(n)$ for all $n \in \Lambda_r$. Then in [24] Kolyvagin shows that for all $r \geq 0$:

$$\mathscr{M}_r \geq \mathscr{M}_{r+1} \geq 0. \tag{3.25}$$

We define

$$\mathscr{M}_\infty(g) = \lim_{r\to\infty} \mathscr{M}_r \tag{3.26}$$

as the minimum of $\mathscr{M}_r$ for varying $r \geq 0$.

Then the conjecture of Kolyvagin [24, Conj. A] (generalized to Shimura curves) asserts that

Conjecture 3.2. *Let g be a weight two newform of level N with trivial nebentypus. Assume that the residue representation $\overline{\rho}_{g,\mathfrak{p}_0}$ is surjective. Then the collection of cohomology classes*

$$\kappa^\infty := \{c_M(n) \in H^1(K, A_{g,M}) : n \in \Lambda, M \leq M(n)\} \tag{3.27}$$

is nonzero. Equivalently, we have

$$\mathscr{M}_\infty(g) < \infty.$$

The rest of the paper is to confirm this conjecture under a certain restriction on g.

3.9. Kolyvagin classes $c(n, m) \in H^1(K, V)$.

We will apply Theorem 2.1 to define Kolyvagin classes $c(n, m) \in H^1(K, V)$ parameterized by both $n \in \Lambda$ and $m \in \Lambda^{'+}$. Fixing $m = 1$, the collection of classes $c(n, 1)$ as $n \in \Lambda$ varies is precisely the collection $c_1(n) \in H^1(K, A_{g,1})$ defined in §3.7.

Let $\mathbb{T}_{N^+,N^-m}$ be the Hecke algebra over $\mathbb{Z}$ generated by T_ℓ for $(\ell, Nm) = 1$ and U_ℓ for $\ell|Nm$ acting on the Jacobian $J(X_m)$, equivalently acting on the space of weight two modular forms which are new at all factors of N^-m. Recall that $X_m = X_{N^+,N^-m}$ is the Shimura curve defined in §3.1, and when $\ell|N^-m$, the operator U_ℓ is an involution induced by a uniformizer of the division algebra $B_m(\mathbb{Q}_\ell)^\times$ (cf. [34, §4]). The Hecke action on the modular form g_m gives rise to a surjective homomorphism

$$\phi : \mathbb{T}_{N^+,N^-m} \to \mathscr{O}_{g_m,0},$$

whose kernel is denoted by $\mathscr{I}$. Then the optimal quotient by $J(X_m)$ attached to g_m is the abelian variety

$$A^0_{g_m} := J(X_m)/\mathscr{I} J(X_m), \tag{3.28}$$

on which $\mathbb{T}_{N^+,N^-m}$ acts via the homomorphism ϕ. In particular, we obtain an $\mathscr{O}_0$-action on $A^0_{g_m}$.

Let $\phi \mod \mathfrak{p}_{m,0}$ be the composition of $\mod \mathfrak{p}_{m,0}$ with ϕ:

$$\phi \mod \mathfrak{p}_{m,0} : \mathbb{T}_{N^+,N^-m} \to \mathscr{O}_{g_m,0}/\mathfrak{p}_{m,0} \simeq k_0.$$

Denote by $\mathfrak{m}$ the kernel of $\phi \mod \mathfrak{p}_{m,0}$.

Lemma 3.3. *Assume that $(g, \mathfrak{p}, K)$ satisfies Hypothesis ♡. Then for all $m \in \Lambda'^+$ we have an isomorphism of* $\mathrm{Gal}_{\mathbb{Q}}$*-modules*

$$J(X_m)[\mathfrak{m}] \simeq V \simeq A^0_{g_m}[\mathfrak{p}_{m,0}], \tag{3.29}$$

where all vector spaces are 2-dimensional over k_0.

Proof. The case of modular curve (i.e., $N^-m = 1$) is well-known due to the work of Mazur, Ribet, Wiles (cf. [4]). The case for Shimura curve under our Hypothesis ♡ is proved by Helm [18, Corollary 8.11]. □

For each $n \in \Lambda$, and $m \in \Lambda'^+$ [3] (i.e., with *even* number of factors), we now define the Kolyvagin cohomology class

$$c(n, m) \in H^1(K, J(X_m)[\mathfrak{m}]) \simeq H^1(K, V), \tag{3.30}$$

as the derived cohomological class from the Heegner point $x_m(n) \in X_m(K[n])$ and $y_m(n) \in A^0_{g_m}(K[n])$ (cf. §3.2). When $m = 1$ we simply write

$$c(n) = c(n, 1) \in H^1(K, V).$$

Note that these classes only take values in V (unlike in §3.7, where the classes $c_M(n)$ lie in the cohomology of some $A_{g,M}$). We will denote for each $m \in \Lambda'^+$

$$\kappa_m := \{c(n, m) \in H^1(K, V) : n \in \Lambda\},$$

and we will again call κ_m a *Kolyvagin system.*

Remark 8. The classes $c(n, m)$ depend on the choice of the level-raising newform g_m of level Nm, and the choice of the generators σ_ℓ's made in §3.7. For our purpose, it will suffice to fix a choice for each $m \in \Lambda'^+$. They also depend on the parameterization of the set of Heegner points (3.4) for each

[3] It is easy to see that the set Λ'_1 of admissible primes for g_m almost depends only on the $\mathrm{Gal}_{\mathbb{Q}}$-module V, with only exception that the set Λ'_1 for g_m does not contain prime factors of m.

$m \in \Lambda'^{+}$. To compare the localization of the classes $c(n,m)$ in §4, for each $m \in \Lambda'^{+}$, we require that the following induced embeddings $K \hookrightarrow B_{mq}$ into the definite quaternion algebra are the same

- the one given by (3.13) applied to the curve X_m and an admissible prime q,
- the one given by (3.15) applied to the curve $X_{mqq'}$ and an admissible prime q',

Remark 9. We will also consider a GL_2-type abelian variety A_g with multiplication by $\mathscr{O}_g$ attached to g. Then we will also view $c(n,m) \in H^1(K,V)$ as a class in $H^1(K, V \otimes_{k_0} k)$ by identifying $A[\mathfrak{p}] \simeq V \otimes_{k_0} k$ as $k[\mathrm{Gal}_{\mathbb{Q}}]$-module.

We will again call these global cohomology classes $c(n,m)$ *Kolyvagin classes*. They are the main objects in the rest of the papers. We will analyze their local property in the next section and we will see that the m-aspect of $c(n,m)$ behaves very similar to the n-aspect.

4. Cohomological congruence of Heegner points

Let g be a newform of level N with a prime $\mathfrak{p}$ of $\mathscr{O}_g$ as in "Notations". Recall that V is the 2-dimensional $\mathrm{Gal}_{\mathbb{Q}}$-module over k_0.

4.1. Local cohomology

We recall the definition of some local cohomology groups (cf. [4, §2]).

Definition 4.1. *Let q be a prime not dividing N. The finite or unramified part of $H^1(K_q,V)$ is the k_0-subspace:*

$$H^1_{fin}(K_q,V) = H^1_{ur}(K_q,V)$$

defined as the inflation of $H^1(K_q^{ur}/K_q,V)$, where K_q^{ur} is the maximal unramified extension of K_q. The singular part is defined as

$$H^1_{sing}(K_q,V) = H^1(I_q,V)^{\mathrm{Gal}(K_q^{ur}/K_q)}.$$

We have the inflation-restriction exact sequence

$$0 \to H^1_{fin}(K_q,V) \to H^1(K_q,V) \to H^1_{sing}(K_q,V).$$

Now assume that $q \in \Lambda'$ is an admissible prime. Then the $\mathrm{Gal}_{\mathbb{Q}}$-module V is unramified at q. Then as Gal_{K_q}-modules, the vector space V splits as a direct sum of two k_0-lines:

$$V \simeq k_0 \oplus k_0(1), \quad k_0(1) := \mu_p \otimes_{\mathbb{F}_p} k_0.$$

Note that in our case we have $q \not\equiv \pm 1 \mod p$. Hence the Gal_{K_q}-action is nontrivial on $k_0(1)$. In particular, the direct sum decomposition is unique. This induces a unique direct sum decomposition:

$$H^1(K_q, V) = H^1(K_q, k_0) \oplus H^1(K_q, k_0(1)). \tag{4.1}$$

Lemma 4.2. *Assume that $q \in \Lambda'$ is an admissible prime.*

(1) $\dim H^1(K_q, k_0) = \dim H^1(K_q, k_0(1)) = 1.$
(2) Inside $H^1(K_q, V)$, we have

$$H^1_{fin}(K_q, V) = H^1(K_q, k_0),$$

and, the restriction map induces an isomorphism

$$H^1_{sing}(K_q, V) \simeq H^1(K_q, k_0(1)).$$

Proof. This is proved in [4, Lemma 2.6] or [16, Lemma 8]. □

From this lemma, we will write a direct sum decomposition

$$H^1(K_q, V) = H^1_{fin}(K_q, V) \oplus H^1_{sing}(K_q, V), \tag{4.2}$$

where H^1_{sing} is identified with the subspace $H^1(K_q, k_0(1))$ of $H^1(K_q, V)$.

4.2. Cohomological congruence between Heegner points

Recall that in §3, for a fixed newform g of level $N = N^+N^-$ for a square-free N^- (with $\nu(N^-)$ even), we have defined a family of cohomology classes $c(n, m) \in H^1(K, V)$ indexed by $n \in \Lambda, m \in \Lambda'^{+}$.

Now let

$$\mathrm{loc}_v : H^1(K, V) \to H^1(K_v, V)$$

be the localization map at a place v of K. We then have the following cohomological congruence between Heegner points when varying $m \in \Lambda'^{+}$, which can be essentially deduced from the work of Vatsal [43] and Bertolini–Darmon [4]. This will be the key ingredient to show the non-vanishing of the Kolyvagin system

$$\kappa_m := \{c(n,m) \in H^1(K,V) : n \in \Lambda\}, \quad m \in \Lambda'^{+}.$$

Theorem 4.3. *Assume that $(g, \mathfrak{p}, K)$ is as in "Notations" and satisfies* Hypothesis ♡. *Let $m \in \Lambda'^{+}$ and $q_1, q_2 \in \Lambda'_1$ not dividing m. Then we have*

$$\mathrm{loc}_{q_1}(c(n,m)) \in H^1(K_{q_1}, k_0), \quad \mathrm{loc}_{q_2}(c(n,mq_1q_2)) \in H^1(K_{q_2}, k_0(1)). \tag{4.3}$$

Fixing isomorphisms

$$H^1(K_{q_1}, k_0) \simeq k_0 \simeq H^1(K_{q_2}, k_0(1)), \tag{4.4}$$

we have an equality for all $n \in \Lambda$:

$$\mathrm{loc}_{q_1}(c(n,m)) = \mathrm{loc}_{q_2}(c(n,mq_1q_2)), \tag{4.5}$$

up to a unit in k_0 (dependent only on the choice of isomorphisms (4.4)).

Remark 10. The item (3) in Hypothesis ♡ is not used in the proof of this result.

Proof. Let A^0, A^0_1, A^0_2 be the optimal quotients attached to g_m, g_{mq_1}, $g_{mq_1q_2}$. They all carry the common $\mathrm{Gal}_{\mathbb{Q}}$-module V.

We first calculate $\mathrm{loc}_{q_1}(c(n,m))$. We describe the local Kummer map of Heegner points $x \in \mathscr{C}^{+}_{K,Nm}$:

$$\begin{aligned}\delta_{q_1} : J(X_m)(K_{q_1}) \to A^0(K_{q_1}) &\to H^1_{fin}(K_{q_1}, A^0[\mathfrak{p}_{m,0}]) \\ &\simeq H^1_{fin}(K_{q_1}, V) = H^1(K_{q_1}, k_0).\end{aligned} \tag{4.6}$$

Here we use the remark (6) to modify x into a degree-zero divisor. By [4, §9], there exists a nontrivial k_0-valued Hecke eigenform on the Shimura set:

$$\phi : X_{mq_1} \to k_0 \tag{4.7}$$

such that

- ϕ is the reduction of the Jacquet-Langlands correspondence of g_{mq_1}, in the sense that the Hecke operator T_ℓ acts on ϕ by $a_\ell(g_{mq_1}) \mod \mathfrak{p}'$ for all ℓ (when $\ell | Nmq$, T_ℓ means U_ℓ). This determines ϕ uniquely up to a scalar. Indeed under Hypothesis ♡, by the proof of [33, Thm. 6.2] via "Mazur's principle", we have a multiplicity one property:

$$\dim_{k_0} \mathbb{Z}[X_{mq_1}] \otimes_{\mathbb{T}} \mathbb{T}/\ker(\chi) = 1, \tag{4.8}$$

where $\mathbb{T} = \mathbb{T}_{N^+,N^-mq_1}$ and $\chi : \mathbb{T} \to k_0$ is the algebra homomorphism associated to ϕ.

- It calculates the local Kummer map of Heegner points: for a suitable choice of isomorphism

$$H^1(K_{q_1}, k_0) \simeq k_0,$$

we have

$$\phi(\mathrm{Red}_{q_1}(x)) = \delta_{q_1}(x) \in k_0, \tag{4.9}$$

for all Heegner points $x \in \mathscr{C}_K^+ = \mathscr{C}_{K,Nm}^+$. Recall that the reduction map is $\mathrm{Red}_{q_1} : \mathscr{C}_K^+ \to X_{mq_1}$ defined by (3.18). This follows from [4, Theorem 9.2], essentially as a consequence of Ihara's lemma in [10] for Shimura curves over $\mathbb{Q}$ (also cf. [43, §6] for the use of the original Ihara lemma for modular curves).

The two items can be written in terms of the following commutative diagrams where $q = q_1$:

$$\begin{tikzcd}
\mathrm{Div}^0(\mathscr{C}_K^+) \arrow[r, "\mathrm{Red}_q"] \arrow[d] & \mathrm{Div}^0(X_m^{ss}) \arrow[r, "\simeq"] \arrow[d] & \mathbb{Z}[X_{mq}]^0 \arrow[d] \arrow[drr, "\phi"] & & \\
J(K_q) \arrow[r] & J(\mathbb{F}_{q^2}) \arrow[r] & H^1_{fin}(K_q, J[\mathfrak{m}]) \arrow[rr, "\simeq"] & & H^1_{fin}(K_q, V) \simeq k_0,
\end{tikzcd}$$

where $X_m^{ss} = X_m(\mathbb{F}_{q^2})^{ss}$ is the set of supersingular points, and $\mathbb{Z}[X_{mq}]^0$ is the kernel of the degree map $\deg : \mathbb{Z}[X_{mq}] \to \mathbb{Z}$.

Now we move to $\mathrm{loc}_{q_2}(c(n, mq_1q_2))$. We have a Shimura curve $X_{mq_1q_2}$ parameterizing A_2^0 and we need to calculate the local Kummer map at q_2:

$$\delta_{q_2} : J(X_{mq_1q_2})(K_{q_2}) \to A_2^0(K_{q_2}) \to H^1_{sing}(K_{q_2}, V) = H^1(K_{q_2}, k_0(1)).$$

For the last arrow, the image of $A^0(K_{q_2})$ is the singular part since $J(X_{mq_1q_2})$ has purely multiplicative reduction at q_2 by [4, Corollary 5.18] (cf. (5.6) below). Together with (4.6), this shows (4.3). Let $J = J(X_{mq_1q_2})$ and let $\mathscr{V}(X_{mq_1q_2}) = \mathscr{V}_0 \sqcup \mathscr{V}_1$ be the disjoint union (3.17). By [4, §5, §8], we have

- The Kummer map $J(K_{q_2}) \to H^1(K_q, J[\mathfrak{m}]) = H^1(K_q, V)$ factors through the group $\Phi(J/K_{q_2})$ of connected components of the Néron model of J over K_{q_2}.
- When we only consider the set $\mathscr{C}_K^+ = \mathscr{C}_{K,Nmq_1q_2}^+$, the specialization of $\mathscr{C}_K^+$ always lies in $\mathscr{V}_0 \simeq X_{mq_1}$. By [4, Prop. 5.14], there is a homomorphism $\mathbb{Z}[\mathscr{V}]^0 \to \Phi(J/K_q)$ which calculates the specialization of $\mathrm{Div}^0(\mathscr{C}_K^+)$ to the group $\Phi(J/K_q)$.
- The Hecke eigenform ϕ in (4.7) also calculates the local Kummer map of Heegner point on $X_{mq_1q_2}$: for a suitable choice of isomorphism

  $$H^1(K_{q_2}, k_0(1)) \simeq k_0,$$

  we have

  $$\phi(\mathrm{Sp}_{q_2}(x)) = \delta_{q_2}(x) \in k_0, \tag{4.10}$$

  for all Heegner points $x \in \mathscr{C}_{K,Nmq_1q_2}^+$. Recall that the specialization map is $\mathrm{Sp}_{q_2} : \mathscr{C}_{K,Nmq_1q_2}^+ \to X_{mq_1}$ defined by (3.19).

These facts can be summarized in terms of the following commutative diagrams:

$$\begin{tikzcd}
\mathrm{Div}^0(\mathscr{C}_K^+) \arrow[r, "\mathrm{Sp}_q"] \arrow[d] & \mathbb{Z}[\mathscr{V}_0]^0 \arrow[r, "\simeq"] \arrow[d] & \mathbb{Z}[X_{mq_1}]^0 \arrow[d] \arrow[dr, "\phi"] & \\
J(K_q) \arrow[r] & \Phi(J/K_q) \arrow[r] & H^1_{sing}(K_q, J[\mathfrak{m}]) \arrow[r, "\simeq"] & H^1_{sing}(K_q, V) \simeq k_0,
\end{tikzcd}$$

where $q = q_2$.

From the geometric congruence Theorem 3.1, and the description (4.9) and (4.10) of the local Kummer maps in terms of ϕ in (4.7), we have for all $n \in \Lambda$:

$$\mathrm{loc}_{q_1} \circ \delta_{q_1}(y_m(n)) = \mathrm{loc}_{q_2} \circ \delta_{q_2}(y_{mq_1q_2}(n)), \tag{4.11}$$

up to a unit in k_0 (independent of n, m), where we view $y_m(n) \in A^0(K_{q_1})$ and $y_{mq_1q_2}(n) \in A_2^0(K_{q_2})$ as local points (noting that q_1, q_2 splits completely in $K[n]$).

Note that the cohomology classes $c(n,m)$ are the Kummer images of the points $P_m(n)$ derived from $y_n(m)$. We have also chosen the derivative operators $\mathbb{D}_n$ compatibly when varying m. Then clearly (4.11) implies the desired congruence between the cohomological classes $c(n,m)$ and $c(n,mq_1q_2)$:

$$\mathrm{loc}_{q_1}(c(n,m)) = \mathrm{loc}_{q_2}(c(n,mq_1q_2)).$$

□

Remark 11. We may simply state this as the congruence between two Kolyvagin systems indexed by $m, mq_1q_2 \in \Lambda'^{+}$:

$$\mathrm{loc}_{q_1}(\kappa_m) = \mathrm{loc}_{q_2}(\kappa_{mq_1q_2}).$$

There is analogous property in the n-aspect of $c(n,m)$: for $n \in \Lambda$ and a prime $\ell \in \Lambda$ not dividing n, we have

$$\psi_\ell(\mathrm{loc}_\ell c(n,m)) = \mathrm{loc}_\ell(c(n\ell,m)),$$

where ψ_ℓ is a suitable finite/singular isomorphism at ℓ (cf. (8.1) in §8 or [26]).

Remark 12. The part on loc_{q_1} is usually called Jochnowitz congruence (cf. [43, 4, 9] and also §6). The part on loc_{q_2} already appeared in the proof of the anti-cyclotomic main conjecture by Bertolini–Darmon [4]. If we check the change of root number of $L(g/K,s)$ using (1.4), we see that the Jochnowitz congruence switch from -1 to $+1$, while the Bertolini–Darmon congruence from $+1$ to -1.

5. Rank-lowering of Selmer groups

In this section we study the effect on the Selmer group by level-raising of modular forms. Suppose that we are given:

- g: a newform of level N as in “Notations”, with a prime $\mathfrak{p}$ of $\mathscr{O}$ above p.
- $q \in \Lambda'$: an admissible prime.
- g': a level-raising form from Theorem 2.1, i.e., a newform of level Nq which is congruent to g. The congruence also requires a choice of prime $\mathfrak{p}'$ of $\mathscr{O}' = \mathscr{O}_{g'}$ above p.

Let A, A' be the GL_2-type abelian variety over $\mathbb{Q}$ associated to g, g' with multiplication by $\mathscr{O}, \mathscr{O}'$. We write $k' = \mathscr{O}'/\mathfrak{p}'$.

We want to compare the Selmer group of A and A'. This part is largely from the idea of Gross–Parson in [16] with a slight improvement.

5.1. Local conditions

Following [16], we describe the local conditions defining the Selmer group:

$$\mathrm{Sel}_{\mathfrak{p}}(A/K) = \{c \in H^1(K, A[\mathfrak{p}]) : \mathrm{loc}_\ell(c) \in \mathrm{Im}(\delta_\ell),\ \text{for all } \ell\}, \tag{5.1}$$

where

$$\delta_\ell : A(K_\ell) \to H^1(K_\ell, A[\mathfrak{p}]) \tag{5.2}$$

is the local Kummer map at ℓ. As we have identified $A[\mathfrak{p}]$ with $V \otimes_{k_0} k$, we will denote by $\mathscr{L}_{\ell,A}$ the image $\mathrm{Im}(\delta_\ell)$ as a subspace of $H^1(K_\ell, V) \otimes_{k_0} k$. A key observation in [16] is that, under suitable hypothesis, one could describe the local conditions $\{\mathscr{L}_{\ell,A}\}$ purely in terms of $\mathrm{Gal}_{\mathbb{Q}}$-structure on V together with the information on the reduction type at every prime.

Lemma 5.1. *(1) For any prime ℓ, we have*

$$H^1(\mathbb{Q}_\ell, V) = 0 \Longleftrightarrow V^{\mathrm{Gal}_\ell} = 0. \tag{5.3}$$

(2) If $V = E[p]$ for elliptic curve over $\mathbb{Q}_\ell$ with additive reduction and $p \neq \ell$, then

$$H^1(\mathbb{Q}_\ell, V) = 0.$$

Proof. We have a trivial observation:

$$\dim_k H^1(\mathbb{Q}_\ell, V) = 2 \dim V^{\mathrm{Gal}_\ell}. \tag{5.4}$$

Though this is well-known, we give a proof for the reader's convenience. Since $\ell \neq p$, by Tate theorem [30, Theorem 2.8] the Euler–Poincaré characteristic is

$$\chi(\mathrm{Gal}_\ell, V) = 0.$$

Here we recall the definition [30, Chap. I.2] of the Euler–Poincaré characteristic for any finite Gal_ℓ-module M:

$$\chi(\mathrm{Gal}_\ell, M) := \frac{\# H^0(\mathrm{Gal}_\ell, M) \# H^2(\mathrm{Gal}_\ell, M)}{\# H^1(\mathrm{Gal}_\ell, M)}.$$

Since $\det(\rho) = \epsilon_p$ (the p-adic cyclotomic character), the Galois module V is self-dual. Then the local duality asserts that $H^0(\mathbb{Q}_\ell, V)$ is dual to $H^2(\mathbb{Q}_\ell, V^*) = H^2(\mathbb{Q}_\ell, V)$. Hence $\dim H^0(\mathbb{Q}_\ell, V) = \dim H^2(\mathbb{Q}_\ell, V)$. Since

$H^0(\mathbb{Q}_\ell, V) = V^{\mathrm{Gal}_\ell}$, the desired equality (5.4) follows. Then the first part of the lemma follows.

To show the second part, it suffices to show $V^{\mathrm{Gal}_\ell} = E[p](\mathbb{Q}_\ell) = 0$, which is equivalent to $E(\mathbb{Q}_\ell)/pE(\mathbb{Q}_\ell) = 0$ since $\ell \neq p$. Since E has additive reduction, there is a filtration $E_1(\mathbb{Q}_\ell) \subset E_0(\mathbb{Q}_\ell) \subset E(\mathbb{Q}_\ell)$ where $E_1(\mathbb{Q}_\ell)$ is a pro-ℓ group, $E_0(\mathbb{Q}_\ell)/E_1(\mathbb{Q}_\ell)$ is isomorphic to $\mathbb{F}_\ell$, and $E(\mathbb{Q}_\ell)/E_0(\mathbb{Q}_\ell)$ is isomorphic to the component group of the Néron model of $E/\mathbb{Q}_\ell$. Note that the component group has order at most 4 for an elliptic curve with additive reduction. From $\ell \neq p$ and $p > 3$ it follows that $E(\mathbb{Q}_\ell)/pE(\mathbb{Q}_\ell) = 0$. This completes the proof.

□

Theorem 5.2. *Assume that Hypothesis ♡ for $(g, \mathfrak{p}, K)$ holds. For all primes ℓ (not only those in Λ), the local conditions $\mathscr{L}_{\ell,A}$ and $\mathscr{L}_{\ell,A'}$ all have k_0-rational structure, i.e.: there exist k_0-subspaces of $H^1(K_\ell, V)$ denoted by $\mathscr{L}_{\ell,A,0}$ and $\mathscr{L}_{\ell,A',0}$, such that*

$$\mathscr{L}_{\ell,A} = \mathscr{L}_{\ell,A,0} \otimes_{k_0} k, \quad \mathscr{L}_{\ell,A'} = \mathscr{L}_{\ell,A',0} \otimes_{k_0} k'.$$

Moreover, we have when $\ell \neq q$

$$\mathscr{L}_{\ell,A,0} = \mathscr{L}_{\ell,A',0},$$

and when $\ell = q$:

$$\mathscr{L}_{\ell,A,0} = H^1(K_q, k_0), \quad \mathscr{L}_{\ell,A',0} = H^1(K_q, k_0(1)).$$

Remark 13. This is only place where the item (3) in Hypothesis ♡ is used. In [16], a stronger hypothesis is imposed at a prime ℓ with $\ell^2|N$.

Proof. If $(\ell, Np) = 1$, then both A and A' have good reduction and we have

$$\mathscr{L}_{\ell,A} = H^1_{fin}(K_\ell, V) \otimes_{k_0} k, \quad \mathscr{L}_{\ell,A'} = H^1_{fin}(K_\ell, V) \otimes_{k_0} k'.$$

If $\ell^2|N$, then ℓ is split in the quadratic extension $K/\mathbb{Q}$. Under the item (3) in Hypothesis ♡, we have $H^1(K_\ell, V) = 0$ by Lemma 5.1 (1). In this case we have trivially

$$\mathscr{L}_{\ell,A} = 0, \quad \mathscr{L}_{\ell,A'} = 0.$$

Let $\ell||N$ be a prime where $\overline{\rho}_{A,\mathfrak{p}}$ is ramified at ℓ (this includes all $\ell||N^+$). Then A has purely toric reduction and the $\mathfrak{p}$-part of the component group is trivial. Let $H^1_{unr}(K_q, V)$ be the subspace of $H^1(K_\ell, \mathscr{L}_\ell)$ consisting of classes that split over an unramified extension of K_ℓ [16, §4.2]. It depends only on the $\mathrm{Gal}_{\mathbb{Q}_\ell}$-action on V. By [16, Lemma 6], we have

$$\mathscr{L}_{\ell,A} = H^1_{unr}(K_\ell, V) \otimes_{k_0} k, \quad \mathscr{L}_{\ell,A'} = H^1_{unr}(K_\ell, V) \otimes_{k_0} k'.$$

Now let $\ell | N^- q$ be a prime such that $\overline{\rho}_{A,\mathfrak{p}}$ is unramified. Recall that V splits uniquely as a direct sum of two k_0-lines as $\mathrm{Gal}_{\mathbb{Q}_\ell}$-module: $V \simeq k_0 \oplus k_0(1)$, This induces $H^1(K_\ell, V) = H^1(K_\ell, k_0) \oplus H^1(K_\ell, k_0(1))$, where each component is one-dimensional. The following is proved in [16, Lemma 8]:

- If $\ell \neq q$, both A and A' have purely toric reduction and we have

$$\mathscr{L}_{\ell,A} = H^1(K_\ell, k_0(1)) \otimes_{k_0} k, \quad \mathscr{L}_{\ell,A'} = H^1(K_\ell, k_0(1)) \otimes_{k_0} k'. \tag{5.5}$$

- If $\ell = q$, A has good reduction at q, and A' has purely toric reduction at q. Hence

$$\mathscr{L}_{q,A} = H^1(K_q, k_0) \otimes k, \quad \mathscr{L}_{q,A'} = H^1(K_q, k_0(1)) \otimes k'. \tag{5.6}$$

Finally, at $\ell = p$, both A, A' have good reduction and the local conditions can be described in terms of flat cohomology [16, Lemma 7].

From the description of $\mathscr{L}_{\ell,A}$ and $\mathscr{L}_{\ell,A'}$, the desired result follows. □

We define a k_0-vector space

$$\mathrm{Sel}_{\mathfrak{p}_0}(A/K) := \{c \in H^1(K, V) : \mathrm{loc}_\ell(c) \in \mathscr{L}_{\ell,A,0} \text{ for all } \ell\}. \tag{5.7}$$

Then we have

$$\mathrm{Sel}_{\mathfrak{p}}(A/K) = \mathrm{Sel}_{\mathfrak{p}_0}(A/K) \otimes_{k_0} k. \tag{5.8}$$

Similarly we define $\mathrm{Sel}_{\mathfrak{p}'_0}(A'/K)$. It follows that the local conditions defining $\mathrm{Sel}_{\mathfrak{p}_0}(A/K)$ and $\mathrm{Sel}_{\mathfrak{p}'_0}(A'/K)$ differ at exactly one prime, i.e., at q.

5.2. Parity lemma.

We record the parity lemma of Gross–Parson [16, Lemma 9]. This lemma was also known to Howard (cf. [20, Corollary 2.2.10]). We have four Selmer groups $\mathrm{Sel}_*(K, V), * \in \{u, t, r, s\}$, contained in $H^1(K, V)$, all defined by the same local conditions $\mathscr{L}_{\ell,A,0}$ except $\ell \neq q$. At q, we specify the local conditions

$$\mathscr{L}_{*,q} = \begin{cases} H^1(K_q, k_0), & * = u \text{ (unramified)}, \\ H^1(K_q, k_0(1)), & * = t \text{ (transverse)}, \\ H^1(K_q, V), & * = r \text{ (relaxed)}, \\ 0, & * = s \text{ (strict)}. \end{cases}$$

Lemma 5.3. *If* $\mathrm{loc}_q : \mathrm{Sel}_u(K, V) \to \mathscr{L}_{u,q}$, *then we have*

(1) $\dim_{k_0} \mathrm{Sel}_r(K, V) = \dim_{k_0} \mathrm{Sel}_s(K, V) + 1$.
(2) $\mathrm{Sel}_u(K, V) = \mathrm{Sel}_r(K, V)$ *and* $\mathrm{Sel}_t(K, V) = \mathrm{Sel}_s(K, V)$.

If $\mathrm{loc}_q : \mathrm{Sel}_t(K, V) \to \mathscr{L}_{t,q}$, *then we have*

(1) $\dim_{k_0} \mathrm{Sel}_r(K, V) = \dim_{k_0} \mathrm{Sel}_s(K, V) + 1$, *and*
(2) $\mathrm{Sel}_t(K, V) = \mathrm{Sel}_r(K, V)$ *and* $\mathrm{Sel}_u(K, V) = \mathrm{Sel}_s(K, V)$.

5.3. Rank-lowering of Selmer group

We have the following description of the Selmer group when we move from modular form g to a level-raising one g' (cf. [16, Theorem 2]).

Proposition 5.4. *Let A, A' be as in the beginning of this section. Assume that the localization* $\mathrm{loc}_q : \mathrm{Sel}_{\mathfrak{p}_0}(A/K) \subset H^1(K, V) \to H^1_{fin}(K_q, V) = H^1(K_q, k_0)$ *is surjective (equivalently, nontrivial). Then we have*

$$\dim_{\mathscr{O}'/\mathfrak{p}'} \mathrm{Sel}_{\mathfrak{p}'}(A'/K) = \dim_{\mathscr{O}/\mathfrak{p}} \mathrm{Sel}_{\mathfrak{p}}(A/K) - 1.$$

Moreover, we have

$$\mathrm{Sel}_{\mathfrak{p}'_0}(A'/K) = \mathrm{Ker}(\mathrm{loc}_q : \mathrm{Sel}_{\mathfrak{p}_0}(A/K) \to H^1_{fin}(K_q, V)).$$

Proof. This first follows immediately from the parity lemma 5.3. The second part follows since $\mathrm{Sel}_{\mathfrak{p}'_0}(A'/K) = \mathrm{Sel}_s(K, V)$ is the strict Selmer and $\mathrm{Sel}_{\mathfrak{p}_0}(A/K) = \mathrm{Sel}_r(K, V)$ is the relaxed Selmer. □

6. A special value formula mod *p*

We need a criterion for the non-vanishing of Heegner points in terms of central L-values (instead of the first derivative, as in the Gross–Zagier formula).

To do so we calculate the image of the Heegner point under the localization at an unramified prime q:

$$\mathrm{loc}_q : A(K) \to H^1_{fin}(K_q, A[\mathfrak{p}]).$$

A priori, we may choose an arbitrary q not dividing the level N. But it is easier to do so at an admissible prime q since the local unramified cohomology is of rank one by Lemma 4.2.

6.1. A special value formula

We use a formula of Gross [14]. It can be viewed as an explicit Waldspurger formula for the new vector in the relevant automorphic representation. Such explicit formulae were also obtained by other authors, cf. [47, 48, 41].

Let g be a newform of level $N = N^+N^-$, where N^- has an *odd* number of prime factors. Assume that $(g, \mathfrak{p}, K)$ satisfies the hypothesis in "Notations" (including Hypothesis ♡).

Recall that $X = X_{N^+,N^-}$ is the Shimura set attached to the definite quaternion ramified at $N^-\infty$. Let $\mathbb{T}_{N^+,N^-}$ be the Hecke algebra generated over $\mathbb{Z}$ by Hecke operators $T_\ell, (\ell, N) = 1$ and U_ℓ for $\ell | N$ acting on $\mathbb{Z}[X]$, or equivalently the N^--new quotient of the Hecke algebra generated by Hecke operators acting on the space of weight two modular forms of level N. Following [43, §2.1], we consider a normalized eigenform $\phi = \phi_g$, an $\mathscr{O}$-value function on X, via the Jacquet-Langlands correspondence. It is normalized such that the image of

$$\phi : X \to \mathscr{O} \hookrightarrow \mathscr{O}_{\mathfrak{p}}, \tag{6.1}$$

contains a unit of $\mathscr{O}_{\mathfrak{p}}$. It is then unique up to a $\mathfrak{p}$-adic unit, and we view it as an element in $\mathscr{O}_{\mathfrak{p}}[X]$. We have a bilinear pairing $\langle \cdot, \cdot \rangle$ on $\mathbb{Z}[X]$ given by the Petersson inner product with counting measure on X. We extend it linearly to $\mathscr{O}[X]$ and define (cf. also [33, §2.1, 2.2])

$$\xi_g(N^+, N^-) = \langle \phi, \phi \rangle \in \mathscr{O}. \tag{6.2}$$

We now state the Gross formula (after Vatsal [43, §2.3], also cf. [33, §2.1, 2.2]). Note that we only consider real valued function, hence we do not have the complex conjugation.

Theorem 6.1. *Let*

$$x_K = \sum_{\sigma \in \mathrm{Gal}(K[1]/K)} \sigma(x(1)) \in \mathbb{Z}[X]$$

be the Heegner divisor on the Shimura set X_m (cf. (3.6)). Then we have,

$$\frac{(\phi(x_K))^2}{\langle \phi, \phi \rangle} = u_K^2 |D|^{1/2} \frac{L(g/K, 1)}{\langle g, g \rangle},$$

where $u_K = \frac{1}{2}\#\mathcal{O}_K^\times \in \{1, 2, 3\}$, and $\langle g, g\rangle_{\mathrm{Pet}}$ is the Petersson inner product on the modular curve $X_0(Nm)$:

$$\langle g, g\rangle_{\mathrm{Pet}} = 8\pi^2 \int_{\Gamma_0(Nm)\backslash\mathcal{H}} g(z)\overline{g(z)} dx dy, \quad z = x + y\sqrt{-1}.$$

6.2. Congruence numbers and canonical periods

For a newform g of level $N = N^+N^-$, we denote by $\eta_g(N^+, N^-) \in \mathscr{O}_{\mathfrak{p}}$ a generator of the congruence ideal of the associated homomorphism $\pi_g : \mathbb{T}_{N^+,N^-} \to \mathscr{O} \hookrightarrow \mathscr{O}_{\mathfrak{p}}$. Namely as $\mathscr{O}_{\mathfrak{p}}$-ideals, we have

$$(\eta_g(N^+, N^-)) = \pi_g(\mathrm{Ann}_{\mathbb{T}_{N^+,N^-}} \ker(\pi_g)) \cdot \mathscr{O}_{\mathfrak{p}}.$$

It is only well-defined up to a $\mathfrak{p}$-adic unit. We write $\eta_g(N) = \eta_g(N, 1)$. We define the canonical period (after Hida, Vatsal [43, §2.4]):

$$\Omega_g^{can} = \frac{\langle g, g\rangle_{\mathrm{Pet}}}{\eta_g(N)}, \tag{6.3}$$

where $\eta_g(N)$, only well-defined up to units, can be taken as an element in $\mathscr{O}$. Define

$$\eta_{g,N^+,N^-} = \frac{\eta_g(N)}{\xi_g(N^+, N^-)} \in \mathscr{O}_{\mathfrak{p}}. \tag{6.4}$$

We also define the algebraic part of the special value of $L(g/K, 1)$:

$$L^{\mathrm{alg}}(g/K, 1) := \frac{L(g/K, 1)}{\Omega_g^{can}} \frac{1}{\eta_{g,N^+,N^-}} \in \mathscr{O}_{\mathfrak{p}}. \tag{6.5}$$

The integrality follows from the following reformulation of the formula in Theorem 6.1:

Corollary 6.2. *Up to a $\mathfrak{p}$-adic unit, we have*

$$(\phi(x_K))^2 = L^{\mathrm{alg}}(g/K, 1). \tag{6.6}$$

6.3. Local Tamagawa numbers

Let g be a new form of level N as above, and $A = A_g$ the attached GL_2-type abelian variety over $\mathbb{Q}$ with $\mathscr{O}$-multiplication. We now define the $\mathfrak{p}$-component of the local Tamagawa number of A at a prime $\ell|N$. Let $\mathcal{O}_{K_\ell}$ be the integer ring of K_ℓ and k_ℓ the residue field ($\mathbb{F}_\ell \times \mathbb{F}_\ell$ if ℓ is split in K). For a prime ℓ, let $\mathcal{A}_\ell/\mathcal{O}_{K_\ell}$ be the Néron model of A/K_ℓ and $\mathcal{A}_{k_\ell}$ its special fiber. Let $\mathcal{A}^0_{k_\ell}$ be the connected component containing the identity of $\mathcal{A}_{k_\ell}$. We consider the component group scheme

$$\Phi(A/K_\ell) := \mathcal{A}_{k_\ell}/\mathcal{A}^0_{k_\ell}.$$

It is a finite étale group scheme over k_ℓ with an action by $\mathscr{O}_g$. Let $\Phi(A/K_\ell)_\mathfrak{p}$ be the $\mathfrak{p}$-adic completion, which then carries an action of $\mathscr{O}_\mathfrak{p} = \mathscr{O}_{g,\mathfrak{p}}$. The the $\mathfrak{p}$-part of the local Tamagawa number at ℓ is defined as the length of the k_ℓ-points of the group scheme $\Phi(A/K_\ell)_\mathfrak{p}$:

$$t_g(\ell) = \mathrm{lg}_{\mathscr{O}_\mathfrak{p}} \Phi(A/K_\ell)_\mathfrak{p}(k_\ell). \tag{6.7}$$

This depends on $\mathfrak{p}$ implicitly. One may deduce the vanishing of $t_g(\ell)$ under a simple condition:

Lemma 6.3. *If $V^{\mathrm{Gal}_\ell} = 0$, then $\Phi(A/K_\ell)_\mathfrak{p}(k_\ell)$ is trivial, and hence $t_g(\ell) = 0$.*

Proof. By [16, Lemma 4], the space of inertia invariants $A[\mathfrak{p}]^{I_\ell}$ is, as a Gal_{k_ℓ}-module, an extension of $\Phi(A/K_\ell)[\mathfrak{p}]$ by $\mathcal{A}^0_{k_\ell}[\mathfrak{p}]$. Note that $A[\mathfrak{p}]^{I_\ell} = V_k^{I_\ell}$. Under the hypothesis $V^{\mathrm{Gal}_\ell} = 0$, we deduce that $A[\mathfrak{p}]^{I_\ell} = 0$, and hence the Gal_{k_ℓ}-invariants of $\mathcal{A}^0_{k_\ell}[\mathfrak{p}]$ and $\Phi(A/K_\ell)[\mathfrak{p}]$ are trivial. In particular, $\Phi(A/K_\ell)[\mathfrak{p}](k_\ell) = \Phi(A/K_\ell)[\mathfrak{p}]^{\mathrm{Gal}_{k_\ell}} = 0$. It follows that $\Phi(A/K_\ell)_\mathfrak{p}(k_\ell) = 0$. This completes the proof. □

Now we consider the case $\ell||N$. If $\overline{\rho}_{g,\mathfrak{p}}$ is ramified at $\ell||N$, then $\Phi(A/K_\ell)_\mathfrak{p}$ is trivial and in particular $t_g(\ell) = 0$. If a prime ℓ is inert in K, $\Phi(A/K_\ell)$ is a constant group scheme since k_ℓ is a genuine quadratic extension of $\mathbb{F}_\ell$:

$$\Phi(A/K_\ell)(k_\ell) = \Phi(A/K_\ell)(\overline{k_\ell}).$$

Therefore when $\ell||N$ is inert in K (i.e., $\ell|N^-$), the length $\mathrm{lg}_{\mathscr{O}_\mathfrak{p}} \Phi(A/K_\ell)_\mathfrak{p}$ of the $\mathscr{O}_\mathfrak{p}$-module $\Phi(A/K_\ell)_\mathfrak{p}(\overline{k_\ell})$ is the same as $t_g(\ell)$. One can describe the length in terms of the $\mathfrak{p}$-adic Galois representation restricted to the inertia I_ℓ

$$\rho_{g,\mathfrak{p}} : \mathrm{Gal}_\mathbb{Q} \to \mathrm{GL}_{\mathscr{O}_\mathfrak{p}}(T_\mathfrak{p}(A)) \simeq \mathrm{GL}_2(\mathcal{O}_\mathfrak{p}).$$

The restriction to the inertia $\rho_{g,\mathfrak{p}}|_{I_\ell}$ at ℓ is of the form

$$\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}.$$

Then the length $\mathrm{lg}_{\mathscr{O}_\mathfrak{p}} \Phi(A/K_\ell)_\mathfrak{p}$ for inert ℓ is the same as either

- The maximal integer t such that $\mathrm{Gal}_\mathbb{Q}$-module $A[\mathfrak{p}^t]$ is unramified at ℓ, or
- The maximal integer t such that the $(*)$-part of the above matrices lies in the ideal $\mathfrak{p}^t$ of $\mathscr{O}_\mathfrak{p}$.

For a proof of this well-known description, see [22, p.210].

Theorem 6.4 (Ribet–Takahashi [35], Khare [22], Pollack–Weston,[33])**.** *Let g be as above (particularly N^- has odd number of factors). Assume that Hypothesis $\heartsuit$ holds for $(g, \mathfrak{p}, K)$. Then we have*

$$v_\mathfrak{p}(\eta_{g,N^+,N^-}) = \sum_{\ell | N^-} \mathrm{lg}_{\mathscr{O}_\mathfrak{p}} \Phi(A/K_\ell)_\mathfrak{p}.$$

Proof. This equality is proved in [33, Theorem 6.8] for square-free N under Hypothesis $\heartsuit$ (note that our η_{g,N^+,N^-} defined by (6.4) is the ratio in [33, Theorem 6.8]). The proof of [33, Theorem 6.8] relies on

- the result of Helm [18] on the multiplicity one of $J[\mathfrak{m}]$ to show [33, Theorem 6.2], and
- the last equality in the proof of [33, Theorem 6.8]. This equality is deduced from the result on modular degrees established for elliptic curves by Ribet–Takahashi [35] and Takahashi [38], and for GL_2-type abelian varieties over $\mathbb{Q}$ attached to g by Khare in [22].

The result of Helm [18] does not need to assume the square-freeness of N and indeed holds if we only assume that $\mathrm{Ram}(\overline{\rho}_{g,\mathfrak{p}})$ contains all $q | N^-$ with $q \equiv \pm 1 \mod p$. If N is not square-free, one checks the proof of Ribet–Takahashi (the second assertion of [35, Theorem 1]) and Khare [22] to see that the last equality in the proof of [33, Theorem 6.8] holds if we only assume that

- $\#\mathrm{Ram}(\overline{\rho}_{g,\mathfrak{p}}) \geq 1$, namely there is at least one $\ell || N$ such that $\overline{\rho}_{g,\mathfrak{p}}$ is ramified at ℓ, and
- either $\mathrm{Ram}(\overline{\rho}_{g,\mathfrak{p}})$ contains a prime $\ell || N^-$ or there are at least two primes factors $\ell || N^+$.

Therefore [33, Theorem 6.8] holds under our Hypothesis $\heartsuit$ for $(g, \mathfrak{p}, K)$. This completes the proof.

$\square$

6.4. Jochnowitz congruence

We now switch to the setting at the beginning of §5: g is a newform of level $N = N^+N^-$ and g' a level-raising newform of level Nq where q is an admissible prime. We have a prime $\mathfrak{p}'$ of $\mathscr{O}_{g'}$ above p and the residue filed $\mathscr{O}_{g'}/\mathfrak{p}' = k'$ (cf. §2).

Assume that N^- has *even* number of factor. Then the root number of $L(A/K, s)$ ($L(A'/K, s)$, resp.) is -1 (1, resp.). We may now state the *Jochnowitz congruence*. It provides a local invariant to test the non-vanishing of Heegner point $y_K \in A(K)$ (cf. (3.22)). Recall that $c(1) \in H^1(K, V \otimes_{k_0} k)$ is the Kummer image of y_K. The following result has been essentially known to other authors [43] and [4].

Theorem 6.5. *Assume that g is as in "Notations" and $(g, \mathfrak{p}, K)$ satisfies Hypothesis $\heartsuit$. Assume that $\nu(N^-)$ is even. Then the class $c(1) \in H^1(K, V \otimes_{k_0} k)$ is locally non-trivial at q if and only if the algebraic part $L^{alg}(g'/K, 1)$ (defined by (6.5)) is a $\mathfrak{p}'$-adic unit.*

Proof. By Theorem 3.1, the reduction at q of the Heegner point $x_1(n) \in \mathscr{C}_{1,K}$ on the Shimura curve X is given under the chosen identification $X_m \simeq X^{\mathrm{ss}}_{\mathbb{F}_{q^2}}$ in (3.12)

$$\mathrm{Red}_q(x_1(n)) = x_q(n).$$

Then the Heegner divisor on X

$$x_{1,K} = \sum_{\sigma \in \mathrm{Gal}(K[1]/K)} \sigma(x_1(1))$$

has reduction given by

$$x_{q,K} = \sum_{\sigma \in \mathrm{Gal}(K[1]/K)} \sigma(x_q(1)) \in \mathbb{Z}[X_q].$$

Let ϕ' be the normalized function on the Shimura set X_q, obtained from the Jacquet-Langlands correspondence of g' as in (6.1) applied to g'. The reduction

$$\phi' \bmod \mathfrak{p}' : X_q \to \mathscr{O}_{g'}/\mathfrak{p}' = k'$$

is a Hecke eigenform, hence equal to a multiple of the function ϕ in (4.7) (applied to the Shimura set X_q) by the multiplicity-one (4.8). Possibly replacing it by a multiple in $k'^{\times}$ we may assume that $\phi' \bmod \mathfrak{p}' = \phi$. In particular, we have

$$\phi'(x_{q,K}) \bmod \mathfrak{p}' = \phi\,(x_{q,K})\,. \tag{6.8}$$

As in §4, we fix an isomorphism:

$$H^1_{fin}(K_q, V) = H^1(K_q, k_0) \simeq k_0.$$

By (4.9) we have

$$\mathrm{loc}_q(c(1)) = \phi(x_{q,K}) \in k_0.$$

By the Gross formula (Corollary 6.2) for ϕ' and (6.8), we have

$$(\mathrm{loc}_q(c(1)))^2 = L^{\mathrm{alg}}(g'/K, 1) \mod \mathfrak{p}',$$

where both sides take values in k_0. The desired result follows. □

7. The rank one case

7.1. The B-SD formula in the rank zero case

We need the results of Kato and Skinner–Urban on the B-SD formula in the rank zero case. This is the only place we need to impose the ordinariness assumption.

Theorem 7.1 (Kato, Skinner–Urban)**.** *Let g be a modular form of level N where $\mathfrak{p}$ a prime of $\mathscr{O}_g$ above $p \geq 3$. Assume that:*

- *p is a good ordinary prime.*
- *The image of $\overline{\rho}_{A_g,\mathfrak{p}}$ contains $\mathrm{SL}_2(\mathbb{F}_p)$.*
- *There is a place $\ell || N$ such that the residue Galois representation $\overline{\rho}_{A_g,\mathfrak{p}}$ is ramified at ℓ.*

Then $L(g/K, 1) \neq 0$ if and only if $\mathrm{Sel}_{\mathfrak{p}^\infty}(A_g/K)$ is finite, in which case we have

$$v_{\mathfrak{p}}\left(\frac{L(g/K,1)}{\Omega_g^{can}}\right) = \mathrm{lg}_{\mathscr{O}_{\mathfrak{p}}} \mathrm{Sel}_{\mathfrak{p}^\infty}(A_g/K) + \sum_{\ell | N} t_g(\ell), \tag{7.1}$$

where $t_g(\ell) = \mathrm{lg}_{\mathscr{O}_{\mathfrak{p}}} \Phi(A/K_\ell)(k_\ell)$ is the local Tamagawa number at ℓ defined in (6.7).

Proof. This follows from the $\mathfrak{p}$-adic part of the B-SD formula for A and its quadratic twist A^K separately (cf. [29, p.182, Theorem 1]). Or rather, we use the corresponding statement for the modular form g and its quadratic twist g^K.

For A and its quadratic twist A^K, one applies the variant of [37, Theorem 2] for GL_2-type abelian varieties to show the $\mathfrak{p}$-adic part of the B-SD formula for A and its quadratic twist A^K. We note:

- In [37, Theorem 2], the authors only stated the result for elliptic curves. But clearly the results extend to the setting of a modular form g with a prime $\mathfrak{p}$ of $\mathscr{O}_g$ above p. To deduce the formula from the Iwasawa Main conjecture [37, Theorem 1], they invoke a result of Greenberg which was stated only for elliptic curves, but clearly holds for the GL_2-type abelian variety A_g (cf. the proof of [37, Theorem 3.35]).
- Note that in the proof of [37, Theorem 2], one needs to choose an auxiliary imaginary quadratic field, which needs not to be the K in our paper.
- The image of $\overline{\rho}_{A_g,\mathfrak{p}} \supset \mathrm{SL}_2(\mathbb{F}_p)$ implies that the image of $\rho_{A_g,\mathfrak{p}} \supset \mathrm{SL}_2(\mathbb{Z}_p)$, a condition required to apply Kato's result in [37].

Finally we also note that the canonical period Ω_g^{can} is the product $\Omega_g^+\Omega_g^-$ in [37] up to a $\mathfrak{p}$-adic unit.

□

Remark 14. Note that the theorem does not assume that N^- has odd number of factors. If N^- has even number of factors, then the root number of $L(g/K,s)$ is -1 and the theorem says that the Selmer group $\mathrm{Sel}_{\mathfrak{p}^\infty}(A_g/K)$ can not be finite.

Remark 15. We will only use that the left hand side is at most as large as the right hand side in (7.1).

7.2. The rank one case

Theorem 7.2. *Let $(g,\mathfrak{p},K)$ be a newform of level N as in "Notations", satisfying Hypothesis ♡. If $\dim_k \mathrm{Sel}_{\mathfrak{p}}(A/K) = 1$, then the class $c(1) \in H^1(K,V)$ is nonzero.*

Proof. We need to choose a suitable admissible prime q. We record the following well-known lemma.

Lemma 7.3. *Assume $p \geq 5$. Let $c \in H^1(K,V)$ be a non-zero class. Then there exists a positive density of admissible primes q such that the localization $\mathrm{loc}_q(c)$ is nonzero.*

Proof. This is a routine application of Čebotarev density theorem, cf. [4, Theorem 3.2]. ☐

We return to prove Theorem 7.2. Let c be a generator of $\mathrm{Sel}_{\mathfrak{p}_0}(A/K) \subset H^1(K, V)$. We apply the lemma to c to choose an admissible prime q such that $\mathrm{loc}_q(c) \neq 0$. By Theorem 2.1, there exists a level-raising modular form g' of level Nq. Note that Hypothesis ♡ is stable under level-raising. Let $A' = A_{g'}$ be an associated GL_2-type abelian variety with $\mathscr{O}' = \mathscr{O}_{g'}$-multiplication. Then clearly the localization

$$\mathrm{loc}_q : \mathrm{Sel}_{\mathfrak{p}_0}(A/K) \to H^1_{fin}(K_q, V)$$

is surjective. By Proposition 5.4, we have $\dim_{k'} \mathrm{Sel}_{\mathfrak{p}'}(A'/K) = 0$. In particular,

$$\mathrm{Sel}_{\mathfrak{p}'^\infty}(A'/K) = 0.$$

Therefore by the B-SD formula in Theorem 7.1, we have

$$v_{\mathfrak{p}}\left(\frac{L(g'/K,1)}{\Omega_{g'}^{can}}\right) = 0 + \sum_{\ell | Nq} t_{g'}(\ell). \tag{7.2}$$

If $\ell || N^+$, under our assumption, $\overline{\rho}_{g,\mathfrak{p}} \simeq \overline{\rho}_{g',\mathfrak{p}'}$ is ramified at ℓ, and hence $t_{g'}(\ell) = 0$. If $\ell^2 | N^+$, then $V^{\mathrm{Gal}_\ell} = 0$ by the item (3) of Hypothesis ♡. We then have that for $\ell^2 | N^+$, by Lemma 6.3

$$t_{g'}(\ell) = \mathrm{lg}_{\mathscr{O}'_{\mathfrak{p}'}} \Phi(A'/K_\ell)(k_\ell) = 0.$$

The formula (7.2) is then reduced to

$$v_{\mathfrak{p}}\left(\frac{L(g'/K,1)}{\Omega_{g'}^{can}}\right) = \sum_{\ell | N^- q} t_{g'}(\ell). \tag{7.3}$$

We now compare the formula (7.2) with

- Gross formula (Corollary 6.2 applied to g'), and
- Theorem 6.4 (note that since our admissible $q \neq \pm 1 \mod p$, the form g' remains to satisfy the assumption).

We see that the local Tamagawa factors at $N^- q$ exactly cancels the factor $\eta_{g,N^+,N^- q}$ in (6.5). We conclude that

$$L^{\mathrm{alg}}(g'/K, 1) \neq 0 \mod \mathfrak{p}'.$$

By Theorem 6.5, this is equivalent to the non vanishing of the localization of $c(1) \in H^1(K, V \otimes_{k_0} k)$ at q. In particular, the cohomology class $c(1) \in H^1(K, V)$ is nonzero. □

8. Triangulization of Selmer group

We recall some basic property of Kolyvagin system

$$\kappa_m = \{c(n,m) \in H^1(K, V) : n \in \Lambda\}$$

defined in §3. For their proofs, we refer to [15, 23, 24, 28]. Since we will be working with a fixed $m \in \Lambda'^{+}$, we simply write $c(n, m)$ as $c(n)$. We will construct a triangular basis of Selmer group in Lemma 8.4. Such triangular basis for elliptic curves was constructed before by Kolyvagin in [24, Theorem 3] (under the condition that $\kappa^\infty \neq 0$).

8.1. Basic properties of $\boldsymbol{\kappa}$.

There is an alternating $\mathrm{Gal}_{\mathbb{Q}}$-equivariant pairing

$$V \times V \to k_0(1).$$

This induces the local Tate pairing for every prime ℓ:

$$H^1(K_\ell, V) \times H^1(K_\ell, V) \to k_0.$$

For every prime $\ell \in \Lambda$, the local cohomology group $H^1(K_\ell, V)$ is always 4-dimensional (cf. [15]). Define the transverse part $H^1_{tr}(K, V)$ as the subspace of $H^1(K_\ell, V)$ from the inflation of $H^1(K[\ell]_\ell/K_\ell, V)$ (note that Gal_{K_ℓ} acts trivially on V). Then we have a splitting of the finite/singular exact sequence:

$$H^1(K_\ell, V) = H^1_{fin}(K_\ell, V) \oplus H^1_{tr}(K, V),$$

where each component is two-dimensional and totally maximal isotropic under local Tate pairing. The complex conjugation $\tau \in \mathrm{Gal}(K/\mathbb{Q})$ acts on both components and each of the eigenspace $H^1_{fin}(K_\ell, V)^\pm, H^1_{tr}(K, V)^\pm$ is one-dimensional. The local Tate pairing then induces perfect pairings between one-dimensional spaces:

$$H^1_{fin}(K_\ell, V)^\pm \times H^1_{tr}(K, V)^\pm \to k_0.$$

In general, for every prime ℓ (not necessarily in Λ), the finite part $H^1_{fin}(K_\ell, V)$ is, by definition, the local condition $\mathscr{L}_{\ell,A,0} \subset H^1(K_\ell, V)$ (cf. Theorem 5.2).

The collection $\kappa = \{c(n) \in H^1(K, V) : n \in \Lambda\}$ has the following properties:

(1) For every prime ℓ (not only those in Λ) and $n \in \Lambda$, we have (cf. [15])

$$\mathrm{loc}_\ell(c(n)) \in \begin{cases} H^1_{fin}(K_\ell, V) & (\ell, n) = 1; \\ H^1_{tr}(K_\ell, V) & \ell | n. \end{cases}$$

(2) For each prime $\ell \in \Lambda$, there is a finite/singular homomorphism:

$$\psi_\ell : H^1_{fin}(K_\ell, V) \to H^1_{tr}(K_\ell, V),$$

which is an isomorphism (cf. [28, Prop. 4.4]) such that for all $n \in \Lambda$ with $(n, \ell) = 1$

$$\mathrm{loc}_\ell(c(n\ell)) = \psi_\ell(\mathrm{loc}_\ell(c(n))). \tag{8.1}$$

Recall that we assume that the residue Galois representation $\overline{\rho}_{g,\mathfrak{p}_0} : \mathrm{Gal}_{\mathbb{Q}} \to \mathrm{GL}(V) \simeq \mathrm{GL}_2(k_0)$ is surjective. Under this assumption we have a Čebotarev-type density theorem.

Lemma 8.1. *Let c_1, c_2 be two k_0-linear independent elements in $H^1(K, V)$. Then there exists a positive density of primes $\ell \in \Lambda$ such that*

$$\mathrm{loc}_\ell(c_i) \neq 0, \quad i = 1, 2.$$

Proof. This is a special case of [28, Prop. 3.1], noting that $\overline{\rho}_{g,\mathfrak{p}_0} : \mathrm{Gal}_{\mathbb{Q}} \to \mathrm{GL}(V) \simeq \mathrm{GL}_2(k_0)$ is assumed to be surjective. □

The following lemma allows us to pick up an element with a prescribed set of "singular" places.

Lemma 8.2. *Let $\ell \in \Lambda$ and S a finite subset of Λ not containing ℓ. Then there exists $c \in H^1(K, V)^\pm$ such that*

- *$c \neq 0$,*
- *$\mathrm{loc}_v c \in H^1_{fin}(K_v, V)$ for all v outside $S \cup \{\ell\}$.*
- *$\mathrm{loc}_v c \in H^1_{tr}(K_v, V)$ for all $v \in S$.*

Proof. The same proof as [28, Lemma 5.3] still works. □

8.2. Triangulization of Selmer group

Let $(g, \mathfrak{p}, K)$ be as in "Notations" satisfying Hypothesis $\heartsuit$. Assume that N^- has even number of factors. Let $\kappa = \kappa_g$ be the associated Kolyvagin system.

Definition 8.3.
- *The vanishing order ν of κ is defined to be the minimal $\nu(n)$ such that $c(n) \neq 0$ for some $n \in \Lambda$. If $\kappa = \{0\}$, we take $\nu = \infty$.*
- *A prime ℓ is called a base point of κ if ℓ does not divide $D_K N p$ and we have $\mathrm{loc}_\ell(c(n)) = 0$ for all $n \in \Lambda$ (or, simply, $\mathrm{loc}_\ell(\kappa) = 0$). The set of all base points is called the base locus of κ, denote by $\mathscr{B}(\kappa)$.*

The following lemma provides one of the eigenspace of Selmer group with a "triangular basis" entirely consisting of Kolyvagin classes. The existence of such "explicit" triangular basis seems to be the key to our argument later on. The following result, can be proved with the techniques, though not stated explicitly, in [23, 28].

Lemma 8.4. *Assume that $\kappa \neq \{0\}$, i.e., the vanishing order ν of κ is finite. Then we have*

(1) *The ϵ_ν-eigenspace $\mathrm{Sel}_{\mathfrak{p}}^{\epsilon_\nu}(A/K)$ is of dimension $(\nu+1)$:*

$$\dim \mathrm{Sel}_{\mathfrak{p}}^{\epsilon_\nu}(A/K) = \nu + 1,$$

and

$$\dim \mathrm{Sel}_{\mathfrak{p}}^{-\epsilon_\nu}(A/K) \leq \nu.$$

(2) *There exist $2\nu+1$ distinct primes $\ell_1, ..., \ell_{2\nu+1} \in \Lambda_1$ such that the classes*

$$c(n_i) \in H^1(K, V), \quad n_i := \ell_i \ell_{i+1} ... \ell_{i+\nu-1}, \quad 1 \leq i \leq \nu+1$$

form a basis of $\mathrm{Sel}_{\mathfrak{p}}^{\epsilon_\nu}(A/K)$ with the property that, for all $1 \leq j \leq \nu+1$:

$$\mathrm{loc}_{\ell_{\nu+j}}(c(n_i)) \begin{cases} = 0, & i > j. \\ \neq 0, & i = j. \end{cases} \tag{8.2}$$

In other words, the $(\nu+1)\times(\nu+1)$-matrix $(\mathrm{loc}_{\ell_{\nu+j}}(c(n_i)))_{i,j}$ is invertible and upper triangular.

(3) *Let $\mathrm{Sel}^{\pm}_{\mathfrak{p},\mathscr{B}(\kappa)}(A/K)$ be the relaxed Selmer group at the base locus $\mathscr{B}(\kappa)$, i.e., the set of $c \in H^1(K, V \otimes k)^{\pm}$ such that $\mathrm{loc}_v(c) \in \mathscr{L}_{v,A}$ for all v*

outside $\mathscr{B}(\kappa)$ *and no restriction on* $\mathrm{loc}_v(c) \in H^1(K_v, V \otimes k)$ *if* $v \in \mathscr{B}(\kappa)$*. Then we have* $\mathrm{Sel}^{\epsilon_\nu}_{\mathfrak{p},\mathscr{B}(\kappa)}(A/K) = \mathrm{Sel}^{\epsilon_\nu}_{\mathfrak{p}}(A/K)$ *and*

$$\dim \mathrm{Sel}^{-\epsilon_\nu}_{\mathfrak{p},\mathscr{B}(\kappa)}(A/K) \leq \nu.$$

Proof. We first prove by induction that, if $0 \leq j \leq \nu$, there exist a sequence of primes $\ell_1, ..., \ell_{\nu+j} \in \Lambda$ such that

- For all $1 \leq i \leq j+1$, we have $c(n_i) \neq 0$, where $n_i = \ell_i ... \ell_{\nu+i-1}$.
- For all $1 \leq i \leq j$, we have $\mathrm{loc}_{\ell_{\nu+i}} c(n_i) \neq 0$.

When $j = 0$, it follows from the definition of ν that there exists $n_1 = \ell_1 ... \ell_\nu \in \Lambda_\nu$ such that

$$c(n_1) \neq 0.$$

This proves the case $j = 0$ since the second requirement is void in this case.

Now suppose that we have found $\ell_1, ..., \ell_{\nu+j}$ with the desired property and $0 \leq j \leq \nu - 1$. We apply Lemma 8.2 to $S = \{\ell_{j+2}, ..., \ell_{\nu+j}\}$ and $\ell = \ell_{j+1}$ to obtain $c \in H^1(K, V)^{-\epsilon_\nu}$ such that

- $c \neq 0$,
- $\mathrm{loc}_v c \in H^1_{fin}(K_v, V)$ for all v outside $\{\ell_{j+1}, ..., \ell_{\nu+j}\}$.
- $\mathrm{loc}_v c \in H^1_{tr}(K_v, V)$ for all $v \in \{\ell_{j+2}, ..., \ell_{\nu+j}\}$.

In particular, c lies in the opposite eigenspace to $c(n_{j+1})$ under the complex conjugation. Apply Lemma 8.1 to obtain a prime denoted by $\ell_{\nu+j+1}$, distinct from $\ell_1, ..., \ell_{\nu+j}$, such that

$$\mathrm{loc}_{\ell_{\nu+j+1}}(c) \neq 0, \quad \mathrm{loc}_{\ell_{\nu+j+1}}(c(n_{j+1})) \neq 0. \tag{8.3}$$

We now calculate the Tate paring, as a sum of the local Tate pairing over all places:

$$0 = \langle c, c(n_{j+1}\ell_{\nu+j+1}) \rangle = \sum_v \langle c, c(n_{j+1}\ell_{\nu+j+1}) \rangle_v. \tag{8.4}$$

We first note that both c and $c(n_{j+1}\ell_{\nu+j+1})$ lie in the same eigenspace. The (possibly) nonzero contribution only comes from $v \in \{\ell_{j+1}, ..., \ell_{\nu+j+1}\}$. When $v \in \{\ell_{j+2}, ..., \ell_{\nu+j}\}$, both $\mathrm{loc}_v c$ and $\mathrm{loc}_v c(n_{j+1}\ell_{\nu+j+1})$ lie in the transverse part $H^1_{tr}(K_v, V)$. Hence the local pairing yields zero. When $v = \ell_{\nu+j+1}$, by (8.3) we have $\mathrm{loc}_{\ell_{\nu+j+1}} c \neq 0$ in $H^1_{fin}(K_{\ell_{\nu+j+1}}, V)^{\epsilon_{\nu+1}}$ and

$$\mathrm{loc}_{\ell_{\nu+j+1}} c(n_{j+1}\ell_{\nu+j+1}) = \psi_{\ell_{\nu+j+1}}(\mathrm{loc}_{\ell_{\nu+j+1}} c(n_{j+1})) \neq 0,$$

in $H^1_{tr}(K_{\ell_{\nu+j+1}}, V)^{\epsilon_{\nu+1}}$. It follows that the local contribution at $v = \ell_{\nu+j+1}$ is nonzero. Hence by (8.4), both $\mathrm{loc}_{\ell_{j+1}} c$ and $\mathrm{loc}_{\ell_{j+1}} c(n_{j+1}\ell_{\nu+j+1})$ are nonzero. Hence we have

$$\mathrm{loc}_{\ell_{j+1}} c(n_j \ell_{\nu+j+1}/\ell_{j+1}) \neq 0,$$

or equivalently,

$$\mathrm{loc}_{\ell_{j+1}} c(n_{j+2}) \neq 0, \quad n_{j+2} = \ell_{j+2}...\ell_{\nu+j+1}.$$

In particular, we have

$$c(n_{j+2}) \neq 0. \tag{8.5}$$

By (8.3) and (8.5) we complete the induction.

We finally add a prime $\ell_{2\nu+1} \in \Lambda$ such that

$$\mathrm{loc}_{\ell_{2\nu+1}} c(n_{\nu+1}) \neq 0.$$

Such a prime exists since $c(n_{\nu+1}) \neq 0$. Now we have found $\{\ell_1, ..., \ell_{2\nu+1}\}$ satisfying the property (8.2).

It is clearly $c(n_i)$, $1 \leq i \leq \nu + 1$, are linearly independent and in the Selmer group $\mathrm{Sel}^{\epsilon_\nu}_{\mathfrak{p}}(A/K)$. To show that they actually generate the entire space $\mathrm{Sel}^{\epsilon_f}_{\mathfrak{p}}(K, V)$, it suffices to show the stronger statement that they generate the relaxed Selmer $\mathrm{Sel}^{\epsilon_\nu}_{\mathfrak{p},\mathscr{B}(\kappa)}(A/K)$.

Let $c \in \mathrm{Sel}^{\epsilon_\nu}_{\mathfrak{p},\mathscr{B}(\kappa)}(A/K)$. We may further assume that, perhaps subtracting c by a suitable linear combination of $c(n_i)$'s:

$$\mathrm{loc}_{\ell_{\nu+j}}(c) = 0, \quad 1 \leq j \leq \nu + 1.$$

Set

$$n' = \ell_{\nu+1}...\ell_{2\nu}\ell_{2\nu+1} \in \Lambda_{\nu+1}.$$

Then $c(n')$ is non-zero since it's locally nonzero at $\ell_{2\nu+1}$. In particular, the classes c and $c(n')$ are in difference eigenspaces.

Assume that $c \neq 0$. By Lemma 8.1, there exists a prime $\ell_{2\nu+2} \notin \{\ell_i : 1 \leq i \leq 2\nu + 1\}$ such that

$$\mathrm{loc}_{\ell_{2\nu+2}}(c) \neq 0, \quad \mathrm{loc}_{\ell_{2\nu+2}} c(n') \neq 0. \tag{8.6}$$

Set

$$n'' = n'\ell_{2\nu+2} \in \Lambda_{\nu+2}.$$

Then $c(n'')$ is nonzero since (8.6) implies that

$$\mathrm{loc}_{\ell_{2\nu+2}}(c) \neq 0, \quad \mathrm{loc}_{\ell_{2\nu+2}} c(n'') \neq 0. \tag{8.7}$$

Moreover, the class $c(n'')$ lies in the same eigenspace as c.

We calculate the Tate pairing as a sum of local terms:

$$0 = \langle c, c(n'')\rangle = \sum_{v \in \mathscr{B}(\kappa)} \langle c, c(n'')\rangle_v + \sum_{\ell | n''} \langle c, c(n'')\rangle_\ell.$$

By definition of base locus $\mathscr{B}(\kappa)$, we have $\mathrm{loc}_v \kappa = 0$. Hence the first sum is zero since $c(n'') \in \kappa$.

Since $\mathrm{loc}_{\ell_i}(c) = 0$ for all $\nu + 1 \leq i \leq 2\nu + 1$, by (8.6) and (8.7) we have

$$\sum_{\ell | n''} \langle c, c(n'')\rangle_\ell = \langle c, c(n'')\rangle_{\ell_{2\nu+2}} \neq 0.$$

Contradiction! Hence $c = 0$ and it follows that $\mathrm{Sel}^{\epsilon_\nu}_{\mathfrak{p}, \mathscr{B}(\kappa)}(A/K) = \mathrm{Sel}^{\epsilon_\nu}_{\mathfrak{p}}(A/K)$ is generated by $c(n_i), 1 \leq i \leq \nu + 1$.

To complete the proof of Lemma 8.4, it remains to show that

$$\dim \mathrm{Sel}^{-\epsilon_\nu}_{\mathfrak{p}, \mathscr{B}(\kappa)}(A/K) \leq \nu.$$

Suppose that $\dim \mathrm{Sel}^{-\epsilon_\nu}_{\mathfrak{p}, \mathscr{B}(\kappa)}(A/K) \geq \nu + 1$. Then by a dimension counting, there exists a class $0 \neq d \in \mathrm{Sel}^{-\epsilon_\nu}_{\mathfrak{p}}(A/K)$ such that

$$\mathrm{loc}_{\ell_{\nu+i}} d = 0, \quad 1 \leq i \leq \nu.$$

Since d and $c(n_{\nu+1})$ lie in different eigenspaces, by Lemma 8.1, we may (re-)choose $\ell_{2\nu+1}$ such that

$$\mathrm{loc}_{\ell_{\nu+1}} d \neq 0, \quad \mathrm{loc}_{\ell_{\nu+1}} c(n_{\nu+1}) \neq 0.$$

Then, as before, we calculate the Tate paring $\langle d, c(n_{\nu+1}\ell_{2\nu+1})\rangle$, to get a contradiction.

□

9. Kolyvagin's conjecture

9.1. Nonvanishing of κ.

We resume the notation in §3 and consider the non-vanishing of κ.

Theorem 9.1. *Let g be a newform of weight two of level N with trivial nebentypus, $\mathfrak{p}$ a prime ideal of $\mathscr{O}_g$ above p, and K an imaginary quadratic field of discriminant D_K such that $(D_K, N) = 1$. Assume*

- *N^- is square-free with even number of prime factors.*
- *$\overline{\rho}_{g,\mathfrak{p}_0} : \mathrm{Gal}_{\mathbb{Q}} \to \mathrm{GL}(V) \simeq \mathrm{GL}_2(k_0)$ is surjective.*
- *Hypothesis $\heartsuit$ holds for $(g, \mathfrak{p}, K)$.*
- *$p \nmid D_K N$ and $p \geq 5$ is an ordinary prime.*

Then we have

$$\kappa = \{c(n) \in H^1(K, V) : n \in \Lambda\} \neq \{0\}.$$

Proof. We prove this by induction on the rank

$$r = \dim_{\mathscr{O}/\mathfrak{p}} \mathrm{Sel}_{\mathfrak{p}}(A_g/K).$$

We first assume that the parity conjecture (for Selmer group) holds for E/K (cf. [32]), i.e., that r is always *odd*. We will remove this assumption later, as to be shown by our method.

The case $r = 1$ has been treated by Theorem 7.2. Suppose now that the rank $r \geq 3$. Suppose that $\mu \in \{\pm 1\}$ is chosen such that $\mathrm{Sel}^{\mu}_{\mathfrak{p}}(A_g/K)$ has *higher* rank than $\mathrm{Sel}^{-\mu}_{\mathfrak{p}}(A_g/K)$. In particular, we have $\dim \mathrm{Sel}^{\mu}_{\mathfrak{p}}(A_g/K) \geq 2$.

We proceed as follows.

- Choose a non-zero $c_1 \in \mathrm{Sel}^{\mu}_{\mathfrak{p}}(A_g/K)$. We may and will require that $c_1 \in H^1(K, V \otimes_{k_0} k)$ is k_0-rational, i.e., in $H^1(K, V)$. And choose an admissible prime q_1 such that the image of c_1 under homomorphism

$$\mathrm{loc}_{q_1} : \mathrm{Sel}_{\mathfrak{p}}(A_g/K) \to H^1_{fin}(K_{q_1}, V)$$

  is nonzero. In particular, the homomorphism is surjective. Then we apply level-raising theorem 2.1 to obtain a newform g_1 of level Nq_1 together with a prime $\mathfrak{p}_1$. Then by Proposition 5.4, we have

$$\dim_{\mathscr{O}_1/\mathfrak{p}_1} \mathrm{Sel}_{\mathfrak{p}_1}(A_1/K) = \dim_{\mathscr{O}/\mathfrak{p}} \mathrm{Sel}_{\mathfrak{p}}(A/K) - 1,$$

  and the k_0-rational Selmer group is equal to the kernel of loc_{q_1}:

$$\mathrm{Sel}_{\mathfrak{p}_{1,0}}(A_1/K) = \mathrm{Ker}(\mathrm{loc}_{q_1} : \mathrm{Sel}_{\mathfrak{p}_0}(A/K) \to H^1_{fin}(K_{q_1}, V)).$$

- Choose a non-zero $c_2 \in \mathrm{Sel}^{\mu}_{\mathfrak{p}_1}(A_1/K)$. Since $\mathrm{Sel}^{\mu}_{\mathfrak{p}_1}(A_1/K) \geq 2$, such c_2 exists. We may and will require that $c_2 \in H^1(K, V)$. We use again the level-raising theorem 2.1 to obtain a newform g_2 of level Nq_1q_2. Then by Proposition 5.4, we have

$$\begin{aligned}\dim_{\mathscr{O}_2/\mathfrak{p}_2} \mathrm{Sel}_{\mathfrak{p}_2}(A_2/K) &= \dim_{\mathscr{O}_1/\mathfrak{p}_1} \mathrm{Sel}_{\mathfrak{p}_1}(A_1/K) - 1\\ &= \dim_{\mathscr{O}/\mathfrak{p}} \mathrm{Sel}_{\mathfrak{p}}(A/K) - 2,\end{aligned}$$

and the k_0-rational Selmer group is equal to the kernel of loc_{q_2}:

$$\mathrm{Sel}_{\mathfrak{p}_{2,0}}(A_2/K) = \mathrm{Ker}(\mathrm{loc}_{q_2} : \mathrm{Sel}_{\mathfrak{p}_{1,0}}(A_1/K) \to H^1_{fin}(K_{q_2}, V)).$$

Moreover, the process is compatible with the action of complex conjugation. We hence have for $i = 1, 2$

$$\dim_{\mathscr{O}_i/\mathfrak{p}_i} \mathrm{Sel}^{\mu}_{\mathfrak{p}_i}(A_i/K) = \dim_{\mathscr{O}/\mathfrak{p}} \mathrm{Sel}^{\mu}_{\mathfrak{p}}(A/K) - i, \tag{9.1}$$

and

$$\dim_{\mathscr{O}_i/\mathfrak{p}_i} \mathrm{Sel}^{-\mu}_{\mathfrak{p}_i}(A_i/K) = \dim_{\mathscr{O}/\mathfrak{p}} \mathrm{Sel}^{-\mu}_{\mathfrak{p}}(A/K). \tag{9.2}$$

By induction hypothesis, noting that g_2 still satisfies the hypothesis of Theorem 9.1, we may assume that the collection

$$\kappa_{q_1q_2} = \{c(n, q_1q_2) \in H^1(K, V) : n \in \Lambda\} \neq \{0\}.$$

By the cohomological congruence of Heegner points (Theorem 4.3), we have for all $n \in \Lambda$

$$\mathrm{loc}_{q_1} c(n, 1) = \mathrm{loc}_{q_2} c(n, q_1q_2).$$

To finish the proof of $\kappa = \{c(n, 1) : n \in \Lambda\} \neq \{0\}$, it suffices to show that q_2 is not a base point of the Kolyvagin system $\kappa_{q_1q_2}$.

We show this by contradiction. Suppose that q_2 is a base point of $\kappa_{q_1q_2}$. We note that the local condition from A_2 differs from that from A_1 only at the place q_2. We then have a trivial inclusion into the relaxed Selmer group:

$$\mathrm{Sel}^{\pm}_{\mathfrak{p}_{1,0}}(A_1/K) \subset \mathrm{Sel}^{\pm}_{\mathfrak{p}_{2,0},\mathscr{B}(\kappa_{q_1q_2})}(A_2/K). \tag{9.3}$$

We have two cases

(1) $\dim \mathrm{Sel}^{\mu}_{\mathfrak{p}_2}(A_2/K)$ remains larger than $\dim \mathrm{Sel}^{-\mu}_{\mathfrak{p}_2}(A_2/K)$.
(2) $\dim \mathrm{Sel}^{\mu}_{\mathfrak{p}_2}(A_2/K)$ is smaller than $\dim \mathrm{Sel}^{-\mu}_{\mathfrak{p}_2}(A_2/K)$. This happens exactly when

$$\dim \mathrm{Sel}^{\mu}_{\mathfrak{p}}(A/K) = \dim \mathrm{Sel}^{-\mu}_{\mathfrak{p}}(A/K) + 1. \tag{9.4}$$

In the first case, by Lemma 8.4 we have an equality

$$\mathrm{Sel}^{\mu}_{\mathfrak{p}_2}(A_2/K) = \mathrm{Sel}^{\mu}_{\mathfrak{p}_2,\mathscr{B}(\kappa_{q_1q_2})}(A_2/K).$$

Hence $\mathrm{Sel}^{\mu}_{\mathfrak{p}_{1,0}}(A_1/K) \subset \mathrm{Sel}^{\mu}_{\mathfrak{p}_2}(A_2/K)$ by (9.3). But, by our choice, the class c_2 lies in the first space but not in the second. A contradiction!

In the second case, let $\nu = \nu_{g_2}$ be the vanishing order of $\kappa_{q_1q_2}$. Then we know by Lemma 8.4 that

$$\dim \mathrm{Sel}^{-\mu}_{\mathfrak{p}_{2,0}}(A_2/K) = \nu + 1, \quad \dim \mathrm{Sel}^{\mu}_{\mathfrak{p}_{2,0},\mathscr{B}(\kappa_{q_1q_2})}(A_2/K) \leq \nu.$$

However, by (9.3), the dimension of $\mathrm{Sel}^{\mu}_{\mathfrak{p}_{2,0},\mathscr{B}(\kappa_{q_1q_2})}(A_2/K)$ is at least that of $\mathrm{Sel}^{\mu}_{\mathfrak{p}_{1,0}}(A_1/K)$ which is $\nu+1$ by (9.1), (9.2), (9.3) and (9.4).

□

Remark 16. Heuristically, the two cases are treated similar to the proof that $\mathrm{Sel}^{\pm}_{p}(E/K)$ is rank 0 or 1 under the assumption that p does not divide the Heegner point $y_K \in E(K)$ (cf. the proof of [15, Claim 10.1, 10.3]).

9.2. The parity conjecture for Selmer groups.

We finally remark how to avoid the use of parity conjecture (for $\mathfrak{p}$-Selmer group) and actually deduce the parity conjecture from our argument.

Theorem 9.2. *Let $(g, \mathfrak{p}, K)$ be as in Theorem 9.1. Then $\dim_k \mathrm{Sel}_{\mathfrak{p}}(A/K)$ is odd and hence $\mathrm{Sel}_{\mathfrak{p}^\infty}(A/K)$ has odd $\mathscr{O}_{g,\mathfrak{p}}$-corank.*

Proof. First of all we note that under the hypothesis that N^- is square-free with even number of prime factors, the root number of A_g/K is -1, hence $L(g/K,1) = 0$. Therefore $r = 0$ does not occur since by Theorem 7.1, we know that $L(g/K,1) \neq 0$ if $r = 0$.

Suppose that $\dim \mathrm{Sel}_{\mathfrak{p}}(A) = r \geq 2$ is even. If one eigenspace $\dim \mathrm{Sel}^{\nu}_{\mathfrak{p}}(A)$ is strictly larger that the other, the same argument above will produce A_2 with $\dim \mathrm{Sel}_{\mathfrak{p}_2}(A_2) = r-2$. Otherwise, the two eigenspaces have the same dimension $\dim \mathrm{Sel}^{\nu}_{\mathfrak{p}}(A) = \dim \mathrm{Sel}^{-\nu}_{\mathfrak{p}}(A) \geq 1$. We may then modify the choice of c_2 in the proof above and insist $c_2 \in \dim \mathrm{Sel}^{-\nu}_{\mathfrak{p}}(A_1)$. Then we again produce A_2 with $\dim \mathrm{Sel}_{\mathfrak{p}_2}(A_2) = r-2$. Therefore, by induction, we have a contradiction! We thus deduce the parity under the hypothesis that N^- has even number of factors:

$$\dim_k \mathrm{Sel}_{\mathfrak{p}}(A_g/K) \equiv 1 \mod 2.$$

Note that under our hypothesis, the k-vector space $\mathrm{Sel}_{\mathfrak{p}}(A/K)$ can be identified with the $\mathfrak{p}$-torsion of $\mathrm{Sel}_{\mathfrak{p}^\infty}(A/K)$. By the non-degeneracy of the Cassels–Tate pairing on the indivisible quotient of the $\mathscr{O}_{\mathfrak{p}}$-module $Ш(A/K)$, the $\mathscr{O}_{g,\mathfrak{p}}$-corank of $\mathrm{Sel}_{\mathfrak{p}^\infty}(A/K)$ has the same parity as $\mathrm{Sel}_{\mathfrak{p}}(A/K)$. This shows that $\mathrm{Sel}_{\mathfrak{p}^\infty}(A/K)$ has odd $\mathscr{O}_{g,\mathfrak{p}}$-corank. □

9.3. Nonvanishing of $\boldsymbol{\kappa}^\infty$

Now we return to the setting of §2 and confirm Kolyvagin's conjecture 3.2 on non-vanishing of κ^∞.

Theorem 9.3. *Let g be a newform of weight two of level N with trivial nebentypus, $\mathfrak{p}$ a prime ideal of $\mathscr{O}_g$ above p, and K an imaginary quadratic field of discriminant D_K with $(D_K, N) = 1$. Assume that*

- *N^- is square-free with even number of prime factors.*
- *The residue representation $\overline{\rho}_{g,\mathfrak{p}_0}$ is surjective.*
- *Hypothesis ♡ holds for the triple $(g, \mathfrak{p}, K)$.*
- *The prime $p \geq 5$ is ordinary and $p \nmid D_K N$.*

Then we have

$$\kappa^\infty = \{c_M(n) \in H^1(K, A_{g,M(n)}) : n \in \Lambda, M \leq M(n)\} \neq \{0\}.$$

Indeed we have

$$\mathscr{M}_\infty = 0.$$

Proof. This follows trivially from Theorem 9.1. □

Theorem 9.3 implies Theorem 1.1 since, by Lemma 5.1 (2), the item (3) in Hypothesis ♡ for $(g, \mathfrak{p}, K)$ holds automatically for the weight two newform g associated to $E/\mathbb{Q}$ and $\mathfrak{p} = (p)$.

10. B-SD formula in the rank one case

In this section we prove the p-part of the B-SD formula in the rank one case for nice p (in a precise way depending on the residue representation). For simplicity, we will restrict ourselves to the case of elliptic curves.

We recast the situation. Let E be an elliptic curve over $\mathbb{Q}$ of conductor N. We will assume that $\overline{\rho}_{E,p}$ is irreducible. Then there is only one isomorphism class of E up to prime-to-p isogeny. We fix E as the strong Weil curve.

Let K an imaginary quadratic field. Suppose that in the decomposition $N = N^+N^-$, N^- is square-free and has *even* number of prime factors. Let

$\delta(N^+, N^-)$ be the modular degree of (the isogeny class of) E parameterized by X_{N^+,N^-}. More precisely, in the isogeny class of E, consider an optimal quotient E' of the Jacobian J_{N^+,N^-} of X_{N^+,N^-}:

$$\pi : J_{N^+,N^-} \to E'.$$

Then the modular degree η_{N^+,N^-} is defined as the integer $\pi \circ \pi^\vee \in \mathrm{End}_{\mathbb{Q}}(E') \simeq \mathbb{Z}$. Similarly, we simply denote $\delta(N, 1) = \delta(N)$ which is the modular degree using the modular curve $X_0(N)$. Set

$$\delta_{N^+,N^-} = \frac{\delta(N, 1)}{\delta(N^+, N^-)}.$$

Let c be the Manin constant associated to (the strong Weil curve in the isogeny class of) $E/\mathbb{Q}$. It is conjectured to be equal to one. Let c_ℓ be the local Tamagawa numbers of $E/\mathbb{Q}_\ell$ (E/K_ℓ, resp.) if ℓ is split (if ℓ is nonspit, resp.) in $K/\mathbb{Q}$. Under a prime-to-p isogeny $E' \to E$, the Heegner point $y_K \in E'(K)$ is mapped to $E(K)$ (still denoted by y_K).

Lemma 10.1. *Assume that $\overline{\rho}_{E,p}$ is irreducible.*

1. *If* $\mathrm{ord}_{s=1} L(E/K, s) = 1$*, then the p-part of the B-SD formula for E/K is equivalent to the following identity*

$$[E(K) : \mathbb{Z}y_K]^2 \cdot \delta_{N^+,N^-} = c^2 \# Ш(E/K) \prod_{\ell | N^+} c_\ell^2 \prod_{\ell | N^-} c_\ell,$$

up to a p-adic unit.

2. *If* $\mathrm{ord}_{s=1} L(E/K, s) = 1$ *and (E, p, K) satisfies Hypothesis ♠, then the p-part of the B-SD formula for E/K is equivalent to*

$$[E(K) : \mathbb{Z}y_K]^2 = \# Ш(E/K) \prod_{\ell | N^+} c_\ell^2, \tag{10.1}$$

up to a p-adic unit.

Remark 17. When $N^- \neq 1$, we have defined the point $y_K = y(1)$ by (3.2). This can be viewed as an element in $E(K) \otimes \mathbb{Z}_p$. In this case we understand the index $[E(K) : \mathbb{Z}y_K]$ as $[E(K) \otimes \mathbb{Z}_p : \mathbb{Z}_p y_K]$, well-defined up to a p-adic unit.

Proof. Under the square-freeness of N^-, the Gross–Zagier formula for (E, K) on Shimura curve X_{N^+,N^-} ([45], as specialized to the current case by [41]) simplifies

$$u_K^2 \frac{L'(E/K,1)}{\Omega^{can}|D_K|^{-1/2}} \frac{1}{\delta(N,1)} = \frac{1}{\delta(N^+,N^-)} \frac{\langle y_K, y_K\rangle_{E/K}}{c^2}.$$

This formula can be deduced from [45, Theorem 1.2] in a way analogous to [17, Theorem (2.1), p.311].

The B-SD formula for E/K states (cf. [17, p.311])

$$\frac{L'(E/K,1)}{\Omega^{can}|D_K|^{-1/2}} = \frac{\langle y_K, y_K\rangle}{[E(K):\mathbb{Z}y_K]^2} \#\text{Ш}(E/K) \prod_{\ell|N^+} c_\ell^2 \prod_{\ell|N^-} c_\ell. \tag{10.2}$$

The first result follows by comparison:

$$[E(K):\mathbb{Z}y_K]^2 \delta_{N^+,N^-} = u_K^2 c^2 \#\text{Ш}(E/K) \prod_{\ell|N^+} c_\ell^2 \prod_{\ell|N^-} c_\ell.$$

Note that $u_K = \frac{1}{2}\#\mathcal{O}_K^\times \leq 3$. By a result of Mazur [25, Cor. 3.1], if p divides the Manin constant c, then $p^2|4N$. When $\overline{\rho}_{E,p}$ is irreducible and Hypothesis ♠ holds, by the theorem of Ribet–Takahashi (the second part of [35, Theorem 1], cf. the proof of Theorem 6.4), we have, up to a p-adic unit:

$$\delta_{N^+,N^-} = \prod_{\ell|N^-} c_\ell.$$

The second result then follows. □

Theorem 10.2. *Let $E/\mathbb{Q}$ be an elliptic curve of conductor N, K an imaginary quadratic field. Let $p \geq 5$ be a prime such that:*

(1) N^- is square-free with even number of prime factors.
(2) $\overline{\rho}_{E,p}$ is surjective.
(3) Hypothesis ♠ holds for (E,p,K).
(4) $p \nmid D_K N$ is an ordinary prime.

If $\mathrm{ord}_{s=1} L(E/K,s) = 1$, then the p-part of the B-SD formula for E/K holds, i.e.:

$$\left|\frac{L'(E/K,1)}{\Omega^{can}|D_K|^{-1/2}\mathrm{Reg}(E/K)}\right|_p = \left|\#\text{Ш}(E/K) \prod_{\ell|N^+} c_\ell^2 \prod_{\ell|N^-} c_\ell\right|_p. \tag{10.3}$$

where the regulator is defined as $\mathrm{Reg}(E/K) := \frac{\langle y,y\rangle_{NT}}{[E(K):\mathbb{Z}y]^2}$ for any non-torsion $y \in E(K)$, $\langle y,y\rangle_{NT}$ is the Néron-Tate height pairing.

Proof. Under Hypothesis ♠, all local Tamagawa numbers c_ℓ are p-adic units when $\ell|N^+$. By (10.1), it suffices to show, up to a p-adic unit,

$$[E(K):\mathbb{Z}y_K]^2 = \#\text{Ш}(E/K).$$

When $\mathrm{ord}_{s=1}L(E/K,s)=1$, by Kolyvagin's theorem ([23, 28] for modular curves) on the structure of $\text{Ш}(E/K)$, we have

$$\#\text{Ш}(E/K)[p^\infty] = p^{2(\mathscr{M}_0-\mathscr{M}_\infty)}.$$

By Theorem 9.3, we have

$$\mathscr{M}_\infty = 0.$$

The result follows from that $\mathscr{M}_0$ is the p-part of the index $[E(K):\mathbb{Z}y_K]$ by definition. □

Remark 18. Let $\widetilde{\text{Ш}}(E/K)[p^\infty]$ denote the quotient of $\text{Ш}(E/K)[p^\infty]$ by its maximal divisible subgroup. If $\text{Ш}(E/K)[p^\infty]$ is finite, then $\text{Ш}(E/K)[p^\infty]$ is the same as $\widetilde{\text{Ш}}(E/K)[p^\infty]$. Kolyvagin in [24, Theorem 1] proved that, under the condition $\kappa^\infty\neq 0$, the structure of $\widetilde{\text{Ш}}(E/K)[p^\infty]$ is determined in terms of the sequence $\mathscr{M}_i$:

$$\widetilde{\text{Ш}}(E/K)^{\pm}[p^\infty] \simeq \bigoplus_{i\geq 1}(\mathbb{Z}/p^{a_i^{\pm}}\mathbb{Z})^2, \quad a_1^{\pm}\geq a_2^{\pm}\geq ...,$$

where, setting $\nu=\nu^\infty$,

$$\begin{cases} a_i^{\epsilon_\nu} = \mathscr{M}_{\nu+2i-1}-\mathscr{M}_{\nu+2i}, & i\geq 1,\\ a_{i+(\nu-r_p^{-\epsilon_\nu})}^{-\epsilon_\nu} = \mathscr{M}_{\nu+2i-2}-\mathscr{M}_{\nu+2i-1}, & i\geq 1.\end{cases}$$

In particular, we have a bound

$$\#\widetilde{\text{Ш}}(E/K)[p^\infty] \geq p^{2(\mathscr{M}_\nu-\mathscr{M}_\infty)},$$

where the equality holds if $\nu = r_p^{-\epsilon_\nu}$ (for example, if $\nu=0$).

Now recall that $\mathrm{Ram}(\overline{\rho}_{E,p})$ is the set of primes $\ell||N$ such that $\overline{\rho}_{E,p}$ is ramified at ℓ.

Theorem 10.3. *Let $E/\mathbb{Q}$ be an elliptic curve of conductor N. Let $p\geq 5$ be a prime such that:*

(1) $\overline{\rho}_{E,p}$ is surjective.
(2) If $\ell\equiv\pm 1 \mod p$ and $\ell||N$, then $\overline{\rho}_{E,p}$ is ramified at ℓ.

(3) If N is not square-free, then $\#\mathrm{Ram}(\overline{\rho}_{E,p}) \geq 1$ and when $\#\mathrm{Ram}(\overline{\rho}_{E,p}) = 1$, there are even number of prime factors $\ell || N$.
(4) The prime p is good ordinary.

If $\mathrm{ord}_{s=1} L(E/\mathbb{Q}, s) = 1$, then the p-part of the B-SD formula for $E/\mathbb{Q}$ holds, i.e.:

$$\left|\frac{L'(E,1)}{\Omega_E \cdot \mathrm{Reg}(E/\mathbb{Q})}\right|_p = \left|\#Ш(E/\mathbb{Q}) \cdot \prod_{\ell | N} c_\ell\right|_p .$$

Proof. By the same argument in the proof of Theorem 1.4, we may choose an auxiliary imaginary quadratic field K using [6, 31] such that (E, p, K) satisfies the conditions of Theorem 10.2. It follows that the p-part of the B-SD formula for E/K holds. Since $L(E^K, 1) \neq 0$, the p-part of the B-SD formula for $E^K/\mathbb{Q}$ holds by [37, Theorem 2] (cf. Theorem 7.1). Then the p-part of the B-SD formula for $E/\mathbb{Q}$ also follows. □

11. Construction of Selmer groups

We first construct the $\mathfrak{p}$-Selmer group $\mathrm{Sel}_{\mathfrak{p}}(A/K)$, and then all of $\mathrm{Sel}_{p^\infty}(E/\mathbb{Q})$ for an elliptic curve $E/\mathbb{Q}$.

Theorem 11.1. *Let $(g, \mathfrak{p}, K)$ be as in Theorem 9.1 and ν the vanishing order of κ.*

1. *The k-vector space $\mathrm{Sel}_{\mathfrak{p}}^{\epsilon_\nu}(A/K)$ is contained in the subspace of $H^1(K, V_k)$ spanned by all $c(n, 1)$ where $n \in \Lambda$.*
2. *The k-vector space $\mathrm{Sel}_{\mathfrak{p}}(A/K)$ is contained in the subspace of $H^1(K, V_k)$ spanned by all $c(n, m)$ where $n \in \Lambda$ and $m \in \Lambda'^{+}$.*

Proof. The first part is a consequence of Lemma 8.4 and the non-vanishing of κ by Theorem 9.1. For the second part, it suffices to show that the other eigenspace $\mathrm{Sel}_{\mathfrak{p}}^{-\epsilon_\nu}(A/K)$ is generated by $c(n, m)$'s. We may prove it by induction on the dimension of $\mathrm{Sel}_{\mathfrak{p}}(A/K)$ as in the proof of Theorem 9.1. We see that $\dim \mathrm{Sel}_{\mathfrak{p}_2}(A_2/K) = \dim \mathrm{Sel}_{\mathfrak{p}}(A/K) - 2$ and by induction hypothesis we may assume that $\mathrm{Sel}_{\mathfrak{p}_2}(A_2/K)$ is generated by $c(n, q_1q_2m), n \in \Lambda, m \in \Lambda'^{+}$. In particular, the subspace $\mathrm{Sel}_{\mathfrak{p}_2}^{-\epsilon_\nu}(A_2/K)$ is generated by $c(n, q_1q_2m), n \in \Lambda, m \in \Lambda'^{+}$. The result follows from the fact that the spaces $\mathrm{Sel}_{\mathfrak{p}}^{-\epsilon_\nu}(A/K)$ and $\mathrm{Sel}_{\mathfrak{p}_2}^{-\epsilon_\nu}(A_2/K)$ have the same underlying k_0-vector subspace. □

Now we consider the p^∞-Selmer group. We will now consider only elliptic curves $E/\mathbb{Q}$ since the result we will use is only written down in the literature for elliptic curves. We would like to construct all elements in the group

$\mathrm{Sel}^{\pm}_{p^\infty}(E/K)$ by the cohomology classes from Heegner points defined over ring class fields.

We recall a result of Kolyvagin [24, Theorem 2 and 3], which does not assume our Hypothesis ♠. Under the irreducibility of $\overline{\rho}_{E,p}$, we have an injection

$$H^1(K, E[p^M]) \hookrightarrow H^1(K, E[p^{M+M'}]), \quad M, M' \geq 1.$$

The group $H^1(K, E[p^M])$ can be viewed as the kernel of the multiplication by p^M on $H^1(K, E[p^{M+M'}])$. If an element $c \in H^1(K, E[p^{M+M'}])$ is killed by p^M, we will view c as an element in $H^1(K, E[p^M])$. More generally, we have a short exact sequence:

$$0 \longrightarrow H^1(K, E[p^M]) \longrightarrow H^1(K, E[p^\infty]) \xrightarrow{p^M} H^1(K, E[p^\infty]).$$

In this way we will view $c_M(n) \in H^1(K, E[p^M])$ as an element of $H^1(K, E[p^\infty])$.

Theorem 11.2 (Kolyvagin)**.** *Let $E/\mathbb{Q}$ be an elliptic curve of conductor N, K an imaginary quadratic field, p a prime, such that*

- *$(p, DN) = 1$ and N^- is square-free with even number of factors.*
- *The residue Galois representation $\overline{\rho}_{E,p}$ is surjective.*

Assume that $\mathscr{M}_\infty$ is finite and denote by ν^∞ the vanishing order of κ^∞. Then we have

(i) The $\mathbb{Z}_p$-coranks of $\mathrm{Sel}^{\pm}_{p^\infty}(E/K)$ satisfy

$$r_p^{\epsilon_{\nu^\infty}}(E/K) = \nu^\infty + 1,$$

and

$$0 \leq \nu^\infty - r_p^{-\epsilon_{\nu^\infty}}(E/K) \equiv 0 \mod 2.$$

(ii) The Selmer group $\mathrm{Sel}^{\epsilon_{\nu^\infty}}_{p^\infty}(E/K) \subset H^1(K, E[p^\infty])$ is contained in the subgroup of $H^1(K, E[p^\infty])$ generated by all $c_M(n)$, $n \in \Lambda, M \leq M(n)$.

Proof. Kolyvagin only considered the case of parameterization of E by modular curves. But his argument obviously works in the case where the elliptic curve is parameterized by Shimura curve (cf. [42]). □

Corollary 11.3. *Let $E/\mathbb{Q}$ be an elliptic curve of conductor N. Let $p \geq 5$ be a prime such that:*

(1) $\overline{\rho}_{E,p}$ is surjective.
(2) If $\ell \equiv \pm 1 \mod p$ and $\ell || N$, then $\overline{\rho}_{E,p}$ is ramified at ℓ.

(3) If N is not square-free, then $\#\mathrm{Ram}(\overline{\rho}_{E,p}) \geq 1$ and when $\#\mathrm{Ram}(\overline{\rho}_{E,p}) = 1$, there are even number of prime factors $\ell || N$.
(4) The prime p is good ordinary.

Then there exists an imaginary quadratic field K such that the Selmer group $\mathrm{Sel}_{p^\infty}(E/\mathbb{Q})$ is contained in the subgroup of $H^1(K, E[p^\infty])$ generated by all $c_M(n) \in H^1(K, E[p^\infty])$, $n \in \Lambda, M \leq M(n)$.

Proof. As in the proof of Theorem 10.3, we may choose K such that E/K satisfies the assumption of Theorem 11.2 and such that the quadratic twist E^K has non vanishing $L(E^K, 1)$ (if $\epsilon(E/\mathbb{Q}) = -1$) or $L'(E^K, 1)$ (if $\epsilon(E/\mathbb{Q}) = 1$). Then by Theorem 11.2, if $\mathrm{Sel}_{p^\infty}(E/\mathbb{Q})$ has positive $\mathbb{Z}_p$-corank, it will be the eigenspace $\mathrm{Sel}_{p^\infty}^{\epsilon_\nu \infty}(E/K)$ with larger corank, and hence generated by the classes $c_M(n) \in H^1(K, E[p^\infty])$, $n \in \Lambda, M \leq M(n)$. It remains to treat the case when $\mathrm{Sel}_{p^\infty}(E/\mathbb{Q})$ is finite, which is then isomorphic to $Ш(E/\mathbb{Q})[p^\infty]$. But in that case, we must have $\mathrm{ord}_{s=1} L(E/K, s) = 1$ and Kolyvagin has shown that the group $Ш(E/K)[p^\infty]$ are generated by the classes $c_M(n) \in H^1(K, E[p^\infty])$, $n \in \Lambda, M \leq M(n)$. This completes the proof. □

Remark 19. In [8], the authors prove that every element in $Ш(E/\mathbb{Q})[p^\infty]$ splits in a solvable extension of $\mathbb{Q}$, for every semistable $E/\mathbb{Q}$ and every prime p. Our result gives a new proof when (E, p) is as in Corollary 11.3. Indeed, our result shows that one may choose the solvable extension to be unramified at p. It is then easy to see that, for an element in $Ш(E/\mathbb{Q})[p^\infty]$ where (E, p) is as in Corollary 11.3, one may choose the solvable extension to be unramified at any given finite set of primes. This was achieved in [8] only when the analytic rank is at most one.

Acknowledgement

The author thanks H. Darmon, B. Gross, V. Kolyvagin, C. Skinner, Y. Tian, E. Urban, X. Wan, S. Zhang and the anonymous referee for helpful suggestions. The author is grateful to the hospitality of the Morningside Center of Mathematics, Bejing, where part of the paper was written. The author was supported in part by NSF Grant DMS #1301848, and a Sloan research fellowship.

References

[1] J.-F. Boutot, H. Carayol, *Uniformisation p-adique des courbes de Shimura: les théorèmes de Čerednik et de Drinfel'd.* Courbes modulaires et courbes de Shimura (Orsay, 1987/1988). Astérisque No. 196-197 (1991), 7, 45–158 (1992).

[2] M. Bertolini, H. Darmon, *Heegner points on Mumford-Tate curves.* Invent. Math. 126 (1996), no. 3, 413–456

[3] M. Bertolini, H. Darmon, *Euler systems and Jochnowitz congruences.* Amer. J. Math. 121 (1999), no. 2, 259–281.

[4] M. Bertolini, H. Darmon, *Iwasawa's main conjecture for elliptic curves over anticyclotomic $\mathbb{Z}_p$-extensions.* Ann. of Math. (2) 162 (2005), no. 1, 1–64.

[5] M. Bertolini, H. Darmon, and K. Prasanna, *Generalized Heegner cycles and p-adic Rankin L-series.* Duke Math. J. 162 (2013), no. 6, 1033–1148

[6] D. Bump, S. Friedberg, and J. Hoffstein, *Nonvanishing theorems for L-functions of modular forms and their derivatives.* Invent. Math. 102 (1990), no. 3, 543–618.

[7] H. Carayol, *Formes modulaires et représentations galoisiennes valeurs dans un anneau local complet.* p-adic monodromy and the Birch and Swinnerton-Dyer conjecture (Boston, MA, 1991), 213–237.

[8] M. Ciperiani, A. Wiles, *Solvable points on genus one curves.* Duke Math. J. 142 (2008), no. 3, 381–464.

[9] C. Cornut, *Mazur's conjecture on higher Heegner points.* Invent. Math. 148 (2002), no. 3, 495-523.

[10] F. Diamond, R. Taylor, *Nonoptimal levels of mod l modular representations.* Invent. Math. 115 (1994), no. 3, 435-462.

[11] F. Diamond, R. Taylor, *Lifting modular mod l representations.* Duke Math. J. 74 (1994), no. 2, 253-269.

[12] H. Darmon, *A refined conjecture of Mazur-Tate type for Heegner points.* Invent. Math. 110 (1992), no. 1, 123-146.

[13] R. Greenberg, *Iwasawa theory for elliptic curves.* Arithmetic theory of elliptic curves (Cetraro, 1997), 51-144, Lecture Notes in Math., 1716, Springer, Berlin, 1999.

[14] B. Gross, *Heights and the special values of L-series.* Number theory (Montreal, Que., 1985), 115-187, CMS Conf. Proc., 7, Amer. Math. Soc., Providence, RI, 1987.

[15] B. Gross, *Kolyvagin's work on modular elliptic curves.* L-functions and arithmetic (Durham, 1989), 235-256, London Math. Soc. Lecture Note Ser., 153, Cambridge Univ. Press, Cambridge, 1991.

[16] B. Gross, J. Parson, *On the local divisibility of Heegner points.* Number theory, analysis and geometry, 215-241, Springer, New York, 2012.

[17] B. Gross, D. Zagier, *Heegner points and derivatives of L-series.* Invent. Math. 84 (1986), no. 2, 225–320.

[18] D. Helm, *On maps between modular Jacobians and Jacobians of Shimura curves.* Israel J. Math. 160 (2007), 61–117.

[19] B. Howard, *The Heegner point Kolyvagin system.* Compos. Math. 140 (2004), no. 6, 1439-1472.

[20] B. Howard, *Bipartite Euler systems.* J. Reine Angew. Math. 597 (2006), 1–25.

[21] K. Kato, *p-adic Hodge theory and values of zeta functions of modular forms.* Cohomologies p-adiques et applications arithmétiques. III. Astérisque No. 295 (2004), ix, 117–290.

[22] C. Khare, *On isomorphisms between deformation rings and Hecke rings.* Invent. Math. 154 (2003), no. 1, 199–222.

[23] V. A. Kolyvagin, *On the structure of Shafarevich-Tate groups.* Algebraic geometry (Chicago, IL, 1989), 94–121, Lecture Notes in Math., 1479, Springer, Berlin, 1991.

[24] V. A. Kolyvagin, *On the structure of Selmer groups.* Math. Ann. 291 (1991), no. 2, 253–259.

[25] B. Mazur, *Rational isogenies of prime degree* (with an appendix by D. Goldfeld). Invent. Math. 44 (1978), no. 2, 129–162.

[26] B. Mazur, K. Rubin, *Kolyvagin systems.* Mem. Amer. Math. Soc. 168 (2004), no. 799, viii+96 pp.

[27] B. Mazur, J. Tate, *Refined conjectures of the "Birch and Swinnerton-Dyer type".* Duke Math. J. 54 (1987), no. 2, 711-750.

[28] W. McCallum, *Kolyvagin's work on Shafarevich-Tate groups.* L-functions and arithmetic (Durham, 1989), 295-316, London Math. Soc. Lecture Note Ser., 153, Cambridge Univ. Press, Cambridge, 1991.

[29] J. S. Milne, *On the arithmetic of abelian varieties.* Invent. Math. 17 (1972), 177-190.

[30] J. S. Milne, *Arithmetic duality theorems.* Perspectives in Mathematics, 1. Academic Press, Inc., Boston, MA, 1986. x+421 pp.

[31] M. R. Murty, V. K. Murty, *Mean values of derivatives of modular L-series.* Ann. of Math. (2) 133 (1991), no. 3, 447–475.

[32] J. Nekovář, *On the parity of ranks of Selmer groups. II.* C. R. Acad. Sci. Paris Sér. I Math. 332 (2001), no. 2, 99–104.

[33] R. Pollack, T. Weston, *On anticyclotomic μ-invariants of modular forms.* Compos. Math. 147 (2011), no. 5, 1353–1381.

[34] K. Ribet, *On modular representations of* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ *arising from modular forms.* Invent. Math. 100 (1990), no. 2, 431–476.

[35] K. Ribet, S. Takahashi, *Parametrizations of elliptic curves by Shimura curves and by classical modular curves.* Elliptic curves and modular forms (Washington, DC, 1996).

[36] C. Skinner, *A converse to a theorem of Gross, Zagier, and Kolyvagin.* preprint 2013.

[37] C. Skinner, E. Urban, *The Iwawasa main conjectures for* GL_2, Invent. Math. 195 (2014), no. 1, 1–277.

[38] S. Takahashi, *Degrees of parametrizations of elliptic curves by Shimura curves.* J. Number Theory 90 (2001), no. 1, 74–88.

[39] Y. Tian, *Congruent numbers and Heegner points.* Cambridge Journal of Mathematics, Vol 2 (2014), Number 1, 117-161.

[40] Y. Tian, *Congruent numbers with many prime factoirs.* PNAS, Vol 109, no. 52. 21256–21258.

[41] Y. Tian, X. Yuan, and S. Zhang, *Genus periods, Genus points and Congruent number problem.* preprint, 2014.

[42] Y. Tian, S. Zhang, *Euler system on Shimura curves.* in preparation.

[43] V. Vatsal, *Special values of anticyclotomic L-functions.* Duke Math. J., 116 (2003), no. 2, 219–261.

[44] X. Wan, *Iwasawa main conjecture for Rankin-Selberg p-adic L-functions.* preprint 2013.

[45] X. Yuan, S. Zhang, W. Zhang, *The Gross–Zagier formula on Shimura curves. Annals of Mathematics Studies* #184, Princeton University Press, 2012, ISBN: 9781400845644, 266 pp..

[46] S. Zhang, *Heights of Heegner points on Shimura curves.* Ann. of Math. (2) 153 (2001), no. 1, 27–147.

[47] S. Zhang, *Gross–Zagier formula for* GL_2. Asian J. Math. 5 (2001), no. 2, 183–290.

[48] S. Zhang, *Gross–Zagier formula for* GL(2)*. II.* Heegner points and Rankin L-series, 191–214, Math. Sci. Res. Inst. Publ., 49, Cambridge Univ. Press, Cambridge, 2004.

[49] W. Zhang, *A Birch–Swinnerton-Dyer type conjecture for Selmer groups.* preprint, 2014.

Wei Zhang
Department of Mathematics
Columbia University
2990 Broadway, New York, NY 10027
USA
E-mail address: wzhang@math.columbia.edu

Received February 1, 2014