LEVEL RAISING MOD 2 AND OBSTRUCTION TO RANK LOWERING

CHAO LI

ABSTRACT. Given an elliptic curve E defined over $\mathbb{Q}$, we are motivated by the 2-part of the Birch and Swinnerton-Dyer formula to study the relation between the 2-Selmer rank of E and the 2-Selmer rank of an abelian variety A obtained by Ribet's level raising theorem. For certain imaginary quadratic fields K satisfying the Heegner hypothesis, we prove that the 2-Selmer ranks of E and A over K have different parity, as predicted by the BSD conjecture. When the 2-Selmer rank of E is one, we further prove that the 2-Selmer rank of A can never be zero, revealing an obstruction to rank lowering which is unseen for p-Selmer groups for odd p.

1. INTRODUCTION

1.1. **The p-part of the BSD formula.** For an elliptic curve E defined over $\mathbb{Q}$, the Birch and Swinnerton-Dyer conjecture asserts that its Mordell–Weil rank is equal to its analytic rank $r = \mathrm{ord}_{s=1} L(E/\mathbb{Q}, s)$. It furthermore predicts a precise formula (the *BSD formula*),

$$\frac{L^{(r)}(E/\mathbb{Q},1)}{r!\Omega(E/\mathbb{Q})R(E/\mathbb{Q})} = \frac{\prod_p c_p(E/\mathbb{Q}) \cdot |Ш(E/\mathbb{Q})|}{|E(\mathbb{Q})_{\mathrm{tor}}|^2} \tag{1.1}$$

for the leading coefficient of the Taylor expansion of $L(E/\mathbb{Q}, s)$ at $s = 1$ in terms of various important arithmetic invariants of E (see [Gro11] for detailed definitions).

It is a celebrated theorem of Gross–Zagier and Kolyvagin that the rank part of the BSD conjecture holds when $r \leq 1$. In this case, both sides of the BSD formula (1.1) are known to be positive rational numbers ([Gro11, 3.3],[GZ86, V.(1.1)], [Guo96]). To prove that (1.1) is indeed an equality, it suffices to prove that it is an equality up to a p-adic unit, for each prime p. This is known as the *p-part of the BSD formula* (BSD(p) for short), for which much progress has been made:

- When $r = 0$, BSD(p) is known for a good prime $p \geq 3$ (under certain assumptions) as a consequence of the Iwasawa main conjecture for modular forms ([Kat04], [SU14], [Wan14]).
- When $r = 1$, BSD(p) is known for a good ordinary prime $p \geq 5$ (under certain assumptions) due to the recent work of W. Zhang [Zha14] (see also the follow-up work [SZ14] and [BBV16]). For semi-stable curves, Jetchev–Skinner–Wan [JSW15] have established BSD(p) for a good prime $p \geq 3$ in greater generality. See also the more recent works [Spr16] and [Cas17].

On the other hand, very little is known for BSD(2) (but see Remark 1.14). Although the case $p = 2$ is often avoided in number theory due to technical complications, BSD(2) is in fact the most interesting case: for example, one observes from computational data (e.g., [Cre97, Table 4]) that the rational number appearing in the BSD formula usually consists of only small prime factors, and most frequently, the factor 2. We remark that this phenomenon is also expected from heuristics concerning the distribution of Ш ([Del01, BKL+15]).

2010 *Mathematics Subject Classification.* 11G05 (primary), 11R34, 11G10 (secondary).
Key words and phrases. Selmer groups, elliptic curves, abelian varieties, parity conjecture.

We are thus motivated to investigate to what extent Zhang's proof of BSD(p) might work for $p = 2$. For this purpose let us briefly review Zhang's strategy. Let $E/\mathbb{Q}$ be an elliptic curve of conductor N. Let K be an imaginary quadratic field satisfying the *Heegner hypothesis for* $E/\mathbb{Q}$:

$$\text{each prime factor } \ell \text{ of } N \text{ is split in } K.$$

Under certain assumptions (including $p \geq 5$, and local Tamagawa numbers are coprime to p), Zhang shows that if E/K has p-Selmer rank one, then BSD(p) holds for E/K. Its proof roughly consists of three steps:

(A) (level raising) One uses Ribet's level raising congruence ([Rib90]) to produce an auxiliary modular abelian variety A from E.
(B) (rank lowering) When E/K has p-Selmer rank one, the parity result of Gross–Parson [GP12] together with a Chebotarev argument allow one to choose A/K with p-Selmer rank zero.
(C) Using the Jochnowitz congruence for Heegner points established by Bertolini–Darmon [BD99], one can reduce BSD(p) from the p-Selmer *rank one* case to the *rank zero* case. Thanks to the modularity of A, BSD(p) for A/K is known. So BSD(p) for E/K is proved.

1.2. **Level raising and rank lowering.** The level raising theorem (Step (A)) can be more precisely summarized as follows.

Theorem 1.3 (Ribet). *Let $E/\mathbb{Q}$ be an elliptic curve of conductor N. Let $f = \sum_{n \geq 1} a_n q^n$ be the associated newform of level N. Let p be a prime. Assume that*
(1) $\bar{\rho}_{E,p} : G_{\mathbb{Q}} \to \mathrm{Aut}(E[p])$ is surjective.
(2) E has good reduction at p.
(3) The Serre conductor $N(\bar{\rho}_{E,p})$ is equal to N.
Let q be a level raising prime *for E (mod p), i.e., $q \nmid pN$ and $a_q \equiv \pm(q+1) \pmod{p}$. Then there exists a newform $g = \sum_{n \geq 1} b_n q^n$ of level Nq and a prime ideal $\lambda | p$ of the (totally real) Hecke field $F = \mathbb{Q}(\{b_n\}_{n \geq 1})$ such that we have a congruence between the Hecke eigenvalues*

$$a_\ell \equiv b_\ell \pmod{\lambda}, \quad \textit{for every prime } \ell \neq q.$$

Remark 1.4. Under the assumption (1), Ribet's theorem [Rib90, Thm. 1] shows that $\bar{\rho}_{E,p}$ comes from a weight 2 form of level Nq that is new at q. Such a level-raised form is automatically new at any $\ell | N$ due to the assumptions (2) and (3). We also remark that the assumption (3) implies that all local Tamagawa numbers of E are coprime to p (see [GP12, Lemma 4]).

The level raised newform g, via the Eichler–Shimura construction, determines an abelian variety A over $\mathbb{Q}$ up to isogeny, of dimension $[F : \mathbb{Q}]$, with real multiplication by F (so A is of GL_2-type). We choose an A in this isogeny class so that A admits an action by the maximal order $\mathcal{O}_F$. Let $k = \mathcal{O}_F/\lambda$ be the residue field. By construction, for almost all primes ℓ, Frob_ℓ has the same characteristic polynomials on the 2-dimensional k-vector spaces $E[p] \otimes k$ and $A[\lambda]$. Hence by Chebotarev's density theorem and the Brauer-Nesbitt theorem we have

$$E[p] \otimes k \cong A[\lambda]$$

as $G_{\mathbb{Q}}$-representations.

Definition 1.5. We say the pair (A, λ) is obtained from E *via level raising at* q (mod p). We denote the p-Selmer rank of E/K and the λ-Selmer rank of A/K by (see Definitions 2.3 and 2.4)

$$s_p(E/K) := \dim_{\mathbb{F}_p} \mathrm{Sel}_p(E/K), \quad s_\lambda(A/K) := \dim_k \mathrm{Sel}_\lambda(A/K).$$

Notice when A is an elliptic curve ($F = \mathbb{Q}$, $\lambda = (p)$, $k = \mathbb{F}_p$), $s_\lambda(A/K)$ is its usual p-Selmer rank.

When the level raising prime q is inert in K, the modular forms f and g have opposite signs of functional equations. The rank part of BSD conjecture and the conjectural finiteness of Tate–Shafarevich groups then predict (as justified in Prop. 3.5) the following parity conjecture for Selmer groups.

Conjecture 1.6. *Let E, p, q be as in Theorem 1.3. Assume that*

(1) (A, λ) is obtained from E via level raising at q (mod p).
(2) K is an imaginary quadratic field satisfying the Heegner hypothesis for E.
(3) q is inert in K.

Then $s_p(E/K)$ and $s_\lambda(A/K)$ have different parity.

This conjectural parity change makes it possible to lower the Selmer rank from one to zero via level raising. The rank lowering theorem (Step (B)) can be more precisely summarized as follows.

Theorem 1.7 (Gross–Parson, Zhang)**.** *Assume we are in the situation of Conjecture 1.6 with $p \geq 5$. Assume that q further satisfies*

$$q \not\equiv \pm 1 \pmod{p}.$$

Then

(1) Conjecture 1.6 holds. In fact, in this case we have $s_p(E/K) = s_\lambda(A/K) \pm 1$.
(2) If $s_p(E/K) = 1$, then there exists a positive density set of such primes q such that

$$s_\lambda(A/K) = 0.$$

Remark 1.8. Part (1) is the parity lemma of Gross–Parson ([GP12, Lemma 9], [Zha14, Lemma 5.3]). Part (2) is a restatement of Prop. 5.4, Thm. 7.2 and Lemma 7.3 of [Zha14].

1.9. **Level raising mod 2 and obstruction to rank lowering.** To get good control over the local condition at q defining the Selmer group, the key assumption $q \not\equiv \pm 1 \pmod{p}$ in Theorem 1.7 is imposed so that Frob_q acts on $E[p]$ semi-simply with distinct eigenvalues different from $\{\pm 1\}$. This key assumption forces $p \geq 5$ and is not possible for $p = 2$. The major innovation of this article is to overcome this technical difficulty. We do so by controlling the local condition when Frob_q is the *unipotent class of order 2* acting on $E[2]$. Notice that $q \nmid 2N$ is a level raising prime (mod $p = 2$) if and only if a_q is even, if and only if $\bar\rho_{E,2}(\mathrm{Frob}_q) \sim \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ or $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ (the trivial or the order 2 class in $\mathrm{GL}_2(\mathbb{F}_2) \cong S_3$).

When Frob_q has order 2 acting on $E[2]$, we are able to verify Conjecture 1.6. However, in a contrast to Part (2) of Theorem 1.7, it turns out one can *never* lower the 2-Selmer rank to 0, revealing an obstruction to rank lowering for $p = 2$. More precisely, we have the following main theorem.

Theorem 1.10. *Assume we are in the situation of Conjecture 1.6 with $p = 2$. Assume that q further satisfies*

$$\mathrm{Frob}_q \textit{ has order 2 acting on } E[2],$$

and $\bar\rho_{E,2}|_{G_{\mathbb{Q}_2}}$ is nontrivial. Then

(1) (Theorem 6.1) Conjecture 1.6 is true. In fact, in this case we have $s_2(E/K) = s_\lambda(A/K) \pm 1$.
(2) (Theorem 7.1) If $s_2(E/K) = 1$, then for any such q we have

$$s_\lambda(A/K) = 2.$$

Remark 1.11. The obstruction to rank lowering tells us that Zhang's strategy for proving BSD(p) cannot naively work when $p = 2$. We remark that this obstruction to rank lowering over K is a phenomenon unique to $p = 2$ (see Example 7.2). On the other hand, since there is no such obstruction for $p = 3$, the new idea of using the unipotent Frobenius to control Selmer ranks can be used to prove BSD(3) when $r = 1$ under similar assumptions.

Remark 1.12. In [LHL16], we enhance Ribet's level raising theorem to raise the level at multiple primes simultaneously. With refined control over the signs (which are not detected under the mod 2 congruence, see Remark 3.2), we show that it is possible to obtain *arbitrary* $s_\lambda(A/\mathbb{Q})$ (over $\mathbb{Q}$) via level raising mod 2. In particular, the obstruction to rank lowering we discovered occurs *only* for $p = 2$ and *only* over the imaginary quadratic field K.

Remark 1.13. Analogous to the level raising family, the quadratic twist family also share the same mod 2 Galois representation. Interestingly (as pointed out to us by one of the referees), Klagsbrun [Kla12] also found a nontrivial lower bound for 2-Selmer ranks in some explicit quadratic twists families, when working over a base field with at least one complex place. His result disproved a conjecture of Mazur–Rubin in [MR10].

Remark 1.14. Although the obstruction to rank lowering prevents us from proving BSD(2) using Zhang's strategy, the same techniques used in this article are useful in *proving* BSD(2) in other contexts. In fact, we prove BSD(2) for many quadratic twists of general elliptic curves in [KL16]. Similar results for BSD(2) were previously only known for three quadratic twist families ([Tia14] for the congruent number curve $X_0(32)$, [GA97], [CLTZ15] for $X_0(49)$ and [CCL16] for $X_0(36)$).

1.15. **Remarks on the proofs and the content of each section.** In §3 we justify the parity conjecture for Selmer groups. This is familiar when p is odd (cf. [Zha14, 9.2]) since the generalized Cassels–Tate pairing on $Ш(A/K)[\lambda^\infty]$ is non-degenerate and skew-symmetric. When $p = 2$, further analysis is required since a skew-symmetric pairing in characteristic 2 may fail to be alternating. We use the argument of Poonen–Stoll [PS99] to show this failure does not occur for $Ш(A/K)[\lambda^\infty]$ (Theorem 3.3), even though it may occur for $Ш(A/\mathbb{Q})[\lambda^\infty]$ (Remark 3.4).

In §4 we determine the local conditions for the abelian variety A purely in terms of the Galois representation $A[\lambda]$. The technical heart is to determine the local condition at q (Lemma 4.3 (3)), which uses the order two Frob_q in a crucial way. We also remark it is necessary to assume that $\bar\rho_{E,2}|_{G_{\mathbb{Q}_2}}$ is nontrivial in the main theorem due to the extra uncertainty for the local condition at 2 (Remark 6.2). For the same reason, there is an extra uncertainty for the local condition at q when Frob_q is trivial acting on $E[2]$, which leaves us the order two Frob_q as the *only* option to work with.

In §5 we show that the local condition is maximal totally isotropic, not only under the local Tate pairing but also under a quadratic form giving rise to the pairing. The difference between these two notions is another subtlety in characteristic 2 (Remark 5.3). The key case is again the local condition at q. We utilize the quadratic form constructed by Zarhin [Zar74, §2] (see also [O'N02] and [PR12]) and make it explicit in the proof of Lemma 5.5.

In §6 and §7, we prove the main theorem and illustrate the obstruction to rank lowering in Example 7.2. After the preparation in §4 and §5, the proof becomes a standard application of global duality.

1.16. **Acknowledgments.** This article is a revised version of a chapter of the author's Harvard Ph.D. thesis. I am deeply grateful to my thesis advisor, B. Gross, for his constant encouragement and advice throughout this project. I am thankful to K. Cesnavicius, B. V. Le Hung and W. Zhang

for helpful conversations and to Y. Liu for useful comments on an earlier draft of this article. I am also thankful to the referees for careful reading and numerous suggestions. The examples in this article are computed using Sage ([S+13]) and Magma ([BCP97]).

2. Selmer groups

Suppose (A, λ) is obtained from E via level raising at a level raising prime $q \pmod p$. Fix an isomorphism $E[p] \otimes k \cong A[\lambda]$ and denote these two k-vector spaces by V. Let we first recall the general notion of Selmer groups cut out by local conditions.

Definition 2.1. Let K be any number field. Let v be a place of K. We define

$$H^1_{\mathrm{ur}}(K_v, V) := H^1(K_v^{\mathrm{ur}}/K_v, V^{I_v}) \subseteq H^1(K_v, V)$$

consisting of classes which are split over an unramified extension of K_v, where I_v is the inertia subgroup at v.

Definition 2.2. Let $\mathcal{L} = \{\mathcal{L}_v\}$ be the collection of k-subspaces $\mathcal{L}_v \subseteq H^1(K_v, V)$, where v runs over every place of K. We say $\mathcal{L}$ is a collection of *local conditions* if $\mathcal{L}_v = H^1_{\mathrm{ur}}(K_v, V)$ for almost all v. We define the *Selmer group* cut out by the local conditions $\mathcal{L}$ to be

$$H^1_{\mathcal{L}}(V) := \{x \in H^1(K, V) : \mathrm{res}_v(x) \in \mathcal{L}_v, \text{for all } v\}.$$

In other words, it sits in the pull-back diagram

$$\begin{tikzcd} H^1_{\mathcal{L}}(V) \arrow[r] \arrow[d] & H^1(K, V) \arrow[d, "\prod_v \mathrm{res}_v"] \\ \prod_v \mathcal{L}_v \arrow[r] & \prod_v H^1(K_v, V). \end{tikzcd}$$

Definition 2.3. We define $\mathcal{L}_v(E)$ to be the image of the local Kummer map

$$(E(K_v)/pE(K_v)) \otimes_{\mathbb{F}_p} k \to H^1(K_v, E[p]) \otimes k = H^1(K_v, V).$$

Then the Selmer group cut out by $\mathcal{L}(E) := \{\mathcal{L}_v(E)\}$ is equal to $H^1_{\mathcal{L}(E)}(V) = \mathrm{Sel}_p(E/K) \otimes k$.

Definition 2.4. Similarly, we define $\mathcal{L}_v(A)$ to be the image of the local Kummer map

$$A(K_v) \otimes_{\mathcal{O}_F} k \to H^1(K_v, A[\lambda]) = H^1(K_v, V).$$

The λ-*Selmer group* of A is defined to be the Selmer group cut out by $\mathcal{L}(A) := \{\mathcal{L}_v(A)\}$, denoted by $\mathrm{Sel}_\lambda(A/K)$. For details on descent with endomorphisms, see the appendix of [GP12].

By definition we have two short exact sequences,

$$0 \to E(K) \otimes_{\mathbb{Z}} \mathbb{F}_p \to \mathrm{Sel}_p(E/K) \to Ш(E/K)[p] \to 0, \tag{2.1}$$

and

$$0 \to A(K) \otimes_{\mathcal{O}_F} k \to \mathrm{Sel}_\lambda(A/K) \to Ш(A/K)[\lambda] \to 0. \tag{2.2}$$

3. Sign changing and the parity conjecture for Selmer groups

In this section we justify Conjecture 1.6. Let us put ourselves in the situation of Conjecture 1.6, namely, K is an imaginary quadratic field satisfying the Heegner hypothesis for E and q is inert in K. These two assumptions together give rise to the following sign-changing phenomenon.

Lemma 3.1. *The newform f of level N (associated to E) and newform g of level Nq (associated to A) have opposite signs of the functional equations over K,*

$$\varepsilon(f/K) = -1, \quad \varepsilon(g/K) = +1.$$

Proof. Recall that the sign of the functional equation $\varepsilon(f/K)$ can be written as the product of local signs $\varepsilon_v(f/K)$:

(1) For any finite place v of K not dividing the level N, $\varepsilon_v(f/K) = +1$.
(2) For $\ell|N$, ℓ splits as two places v_1, v_2 in K and $\varepsilon_{v_1}(f/K) = \varepsilon_{v_2}(f/K)$.

It follows that the product of local signs at all finite places is $+1$, and thus

$$\varepsilon(f/K) = \varepsilon_\infty(f/K) = -1.$$

Similarly, the sign of the functional equation $\varepsilon(g/K)$ can be written as the product of local signs $\varepsilon_v(g/K)$ (notice g has trivial nebentypus). Since q is inert in K, we have $\varepsilon_q(g/K) = -1$ and the same reasoning shows that

$$\varepsilon(g/K) = -\varepsilon_\infty(g/K) = +1,$$

as desired. □

Remark 3.2. When $p = 2$, both signs may occur for $\varepsilon(g/\mathbb{Q})$ (over $\mathbb{Q}$). For example, consider $E = 11a1 = X_0(11) : y^2 + y = x^3 - x^2 - 10x - 20$ (Cremona's label). It satisfies the assumptions in Theorem 1.3. Since $a_7 = -2$ is even, we know that $q = 7$ is a level raising prime. The elliptic curves $A_1 = 77a1$ and $A_2 = 77b1$ are both obtained from E via level raising at 7 (mod 2). Their first few Hecke eigenvalues are listed in Table 1.

	2	3	5	7	11	13	17	19
$11a1$	-2	-1	1	-2	1	4	-2	0
$77a1$	0	-3	-1	-1	-1	-4	2	-6
$77b1$	0	1	3	1	-1	-4	-6	2

TABLE 1. Level raising at 7

We find

$$\varepsilon(E/\mathbb{Q}) = +1, \quad \varepsilon(A_1/\mathbb{Q}) = -1, \quad \varepsilon(A_2/\mathbb{Q}) = +1.$$

Therefore there is no parity prediction *over* $\mathbb{Q}$ for level raising mod 2. For more refined control over the possible signs under level raising mod 2, see [LHL16].

Next let us show that $\dim_k Ш(A/K)[\lambda]$ "should" be even.

Theorem 3.3. *Assume* $Ш(A/K)[\lambda^\infty]$ *is finite, then* $\dim_k Ш(A/K)[\lambda]$ *is even.*

Remark 3.4. For a general modular abelian variety A of dimension ≥ 2, $\dim_k Ш(A/\mathbb{Q})[\lambda]$ (over $\mathbb{Q}$) may fail to be even when $p = 2$. For example, there is a unique modular abelian surface A of level 65 (up to isogeny). It has real multiplication by $F = \mathbb{Q}(\sqrt{3})$ and $p = 2$ is ramified in F. One can identify A as the Jacobian of the genus two curve ([GGR05, 4.2]):

$$y^2 = -x^6 - 4x^5 + 3x^4 + 28x^3 - 7x^2 - 62x + 42.$$

An explicit 2-descent shows that $Ш(A/\mathbb{Q})[2] \cong \mathbb{Z}/2\mathbb{Z}$. However, as the proof below shows, this failure disappears for the abelian variety (A, λ) obtained from level raising, after a base change to any even degree number field.

Proof. Let $A^\vee/\mathbb{Q}$ be the dual abelian variety of $A/\mathbb{Q}$. Then $A^\vee$ also admits an action by $\mathcal{O}_F$, given by the action *dual* to the $\mathcal{O}_F$-action on A. Let L be any number field. Consider the classical Cassels–Tate pairing ([PS99, §3])

$$\langle\ ,\ \rangle : Ш(A/L) \times Ш(A^\vee/L) \to \mathbb{Q}/\mathbb{Z}.$$

By the $\mathcal{O}_F$-equivariance, its restriction to the λ-primary parts

$$Ш(A/L)[\lambda^\infty] \times Ш(A^\vee/L)[\lambda^\infty] \to \mathbb{Q}/\mathbb{Z}$$

naturally induces an $\mathcal{O}_{F,\lambda}$-linear non-degenerate pairing

$$Ш(A/L)[\lambda^\infty] \times Ш(A^\vee/L)[\lambda^\infty] \to \mathrm{Hom}(\mathcal{O}_{F,\lambda}, \mathbb{Q}/\mathbb{Z}) \cong F_\lambda/\mathcal{O}_{F,\lambda},$$
$$(x, y) \mapsto (a \mapsto \langle ax, y\rangle).$$

This is known as Flach's generalized Cassels–Tate pairing ([Fla90], see also [Nek, 6.3] applied to the λ-adic Tate modules $T = T_\lambda(A)$ and $T^*(1) = T_\lambda(A^\vee)$). Now using a $\mathcal{O}_F$-linear and coprime-to-λ polarization $\phi : A \to A^\vee$ and noticing that the Rosati involution acts trivially on $\mathcal{O}_F$ (since F is totally real), we obtain a skew-symmetric non-degenerate $\mathcal{O}_{F,\lambda}$-linear pairing ([Fla90, Theorem 2],[Nek, 6.5])

$$Ш(A/L)[\lambda^\infty] \times Ш(A/L)[\lambda^\infty] \to F_\lambda/\mathcal{O}_{F,\lambda}.$$

Hence $Ш(A/L)[\lambda^\infty] = Y \oplus Y$ for some maximal totally isotropic $\mathcal{O}_{F,\lambda}$-submodule Y if $p \neq 2$ ([Nek, 6.5]). In particular, we know that $Ш(A/L)[\lambda]$ is an even dimensional k-vector space for any number field L if $p \neq 2$.

When $p = 2$, further analysis is required since a skew-symmetric pairing may fail to be alternating in characteristic 2. Recall that Poonen–Stoll [PS99] defined a class $c_L = \phi^{-1}(c_\phi) \in Ш(A/L)[2]$ with the property that $\langle a, a\rangle = \langle a, c_L\rangle$ for any $a \in Ш(A/L)[2]$. Moreover, by construction, the class c_L is the image of $c_\mathbb{Q}$ under the restriction map

$$\mathrm{res} : Ш(A/\mathbb{Q})[2] \to Ш(A/L)[2],$$

since the polarization ϕ is defined over $\mathbb{Q}$. Now recall that for $a, a' \in Ш(A/L)[2]$, the pairing $\langle a, a'\rangle$ is defined as a sum

$$\langle a, a'\rangle = \sum_v \mathrm{inv}_v(b_v),$$

where v runs over all places of L, $\mathrm{inv}_v : H^2(L_v, \mathbb{F}_2(1))) \cong \mathbb{F}_2$ is the local invariant map and b_v is a certain class in $H^2(L_v, \mathbb{F}_2(1))$ constructed from a and a'. It follows that for $a, a' \in Ш(A/\mathbb{Q})[2]$, we have the relation

$$\langle \mathrm{res}(a), \mathrm{res}(a')\rangle = [L : \mathbb{Q}] \cdot \langle a, a'\rangle.$$

Therefore when $[L : \mathbb{Q}]$ is even, we have $\langle c_L, c_L\rangle = 0$.

On the other hand, when $\langle c_L, c_L\rangle = 0$, the endomorphism σ of $Ш(A/L)$ defined by

$$\sigma(a) = \begin{cases} a, & \text{if } \langle a, c_L\rangle = 0, \\ a + c_L, & \text{if } \langle a, c_L\rangle = 1/2, \end{cases}$$

is an automorphism of order 2, and the modified pairing $\langle a, a'\rangle^\sigma := \langle a, \sigma(a')\rangle$ on $Ш(A/L)$ is non-degenerate and alternating ([PS99, p.1122]). This modified pairing induces a $\mathcal{O}_{F,\lambda}$-linear non-degenerate and alternating pairing on the λ-primary part $Ш(A/L)[\lambda^\infty]$. In particular, we know that $Ш(A/L)[\lambda]$ is an even dimensional k-vector space for any even degree number field L if $p = 2$. $\square$

Now we can justify the parity conjecture for Selmer groups (Conjecture 1.6), as it is predicted by the rank part of the BSD conjecture and the finiteness of Ш. More precisely,

Proposition 3.5. *Assume that*

(1) the rank part of BSD conjecture is true for E/K and A/K.
(2) $Ш(E/K)[p^\infty]$ and $Ш(A/K)[\lambda^\infty]$ are finite.

Then $s_p(E/K)$ and $s_\lambda(A/K)$ have different parity.

Proof. By the short exact sequences (2.1) and (2.2), we have

$$s_p(E/K) = \operatorname{rank} E(K) + \dim_{\mathbb{F}_p} E(K)[p] + \dim_{\mathbb{F}_p} Ш(E/K)[p],$$

and

$$s_\lambda(A/K) = \dim_F A(K) \otimes_{\mathcal{O}_F} F + \dim_k A(K)[\lambda] + \dim_k Ш(A/K)[\lambda].$$

By Lemma 3.1, the rank part of the BSD conjecture implies that $\operatorname{rank} E(K)$ and $\dim_F A(K) \otimes_{\mathcal{O}_F} F$ have different parity. Since $\bar\rho_{E,p}$ is assumed to be surjective, we know that it remains irreducible when restricted to any quadratic extension of $\mathbb{Q}$, hence

$$E(K)[p] = 0, \quad A(K)[\lambda] = 0.$$

Since the Cassels–Tate pairing on $Ш(E/K)[p]$ is non-degenerate and alternating, we know that $\dim_{\mathbb{F}_p} Ш(E/K)[p]$ is even. By Theorem 3.3, we know that $\dim_k Ш(A/K)[\lambda]$ is also even. The result the follows. □

4. Local conditions

In the rest of this article, we will prove Theorem 1.10. In fact we will prove it in Theorems 6.1 and 7.1 under the following slightly weaker assumptions (allowing multiplicative reduction at $p = 2$):

Assumption 4.1. Let $E/\mathbb{Q}$ be an elliptic curve of conductor N. Let $f = \sum_{n\geq 1} a_n q^n$ be the associated newform of level N. Let $\bar\rho_{E,2} : G_\mathbb{Q} \to \mathrm{Aut}(E[2])$ be its mod 2 Galois representation. Assume:

(1) $\bar\rho_{E,2}$ is surjective.
(2) E has good or multiplicative reduction at 2 (i.e., $4 \nmid N$).
(3) The Serre conductor $N(\bar\rho_{E,2})$ is equal to the odd part of N. If $2 \mid N$, $\bar\rho_{E,2}$ is ramified at 2.
(4) If $2 \nmid N$, then $\bar\rho_{E,2}|_{G_{\mathbb{Q}_2}}$ is nontrivial.
(5) q is a level raising prime for E (mod 2) (i.e., $q \nmid 2N$ and a_q is even).
(6) K is an imaginary quadratic field satisfying the Heegner hypothesis for E (i.e., every prime factor of N splits in K).
(7) q is inert K.

Remark 4.2. Recall that the Serre conductor $N(\bar\rho_{E,2})$ ([Ser87, 1.2]) measures the ramification of the mod 2 Galois representation $\bar\rho_{E,2}$. In particular, all the level raised forms will be automatically new at $\ell \mid N$ due to assumption (3). Assumption (3) is also equivalent to saying that the component group of the Néron model of E at any $\ell \mid N$ has odd order (see [GP12, Lemma 4]), which in particular implies that all local Tamagawa numbers of E are odd.

Under Assumption 4.1 (1-5), Ribet's level raising theorem (Theorem 1.3) and its extension when E is multiplicative at 2 (see Theorem 1.1 and Remark 2.3 of [LHL16]) ensure that there exists a newform $g = \sum_{n\geq 1} b_n q^n$ of level Nq and a prime ideal $\lambda|2$ of the (totally real) Hecke field

$F = \mathbb{Q}(\{b_n\}_{n\geq 1})$ such that we have a congruence between the Hecke eigenvalues

$$a_\ell \equiv b_\ell \pmod{\lambda}, \quad \text{for every prime } \ell \neq q.$$

Recall this level raised newform g, via the Eichler–Shimura construction, determines an abelian variety A over $\mathbb{Q}$ up to isogeny, of dimension $[F : \mathbb{Q}]$, with real multiplication by F (so A is of GL_2-type). We choose an A in this isogeny class so that A admits an action by the maximal order $\mathcal{O}_F$. We say the pair (A, λ) is obtained from E via level raising at q (mod 2) (Definition 1.5). We fix an isomorphism $E[2] \otimes k \cong A[\lambda]$ ($k = \mathcal{O}_F/\lambda$) and denote these two k-vector spaces by V.

The following lemma identifies the local conditions for the abelian variety A purely in terms of the Galois representation V, which is the key to controlling the Selmer rank under level raising.

Lemma 4.3. *Suppose (A, λ) is obtained from E via level raising at q (mod 2) (we allow $A = E$ and view $q = 1$ in this case). Let $\mathcal{L} = \mathcal{L}(A)$ be the local conditions defining $\mathrm{Sel}_\lambda(A/K)$. Then*

(1) For $v \nmid 2q\infty$,

$$\mathcal{L}_v = H^1_{\mathrm{ur}}(K_v, V).$$

(2) For $v = \infty$,

$$\mathcal{L}_v = H^1(K_v, V) = 0.$$

(3) For $v = q$, if $\mathrm{Frob}_q \in G_{\mathbb{Q}_q}$ has order 2 acting on V, then there is a unique $G_{\mathbb{Q}_q}$-stable line $W \subseteq V$ as $\bar\rho_{E,2}(\mathrm{Frob}_q)$ is conjugate to $\left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right)$. We have $H^1(K_v, V)$ is 4-dimensional and

$$\mathcal{L}_v = \mathrm{im}(H^1(K_v, W) \to H^1(K_v, V))$$

is 2-dimensional. Moreover,

$$\mathcal{L}_v \cap H^1_{\mathrm{ur}}(K_v, V) = H^1_{\mathrm{ur}}(K_v, W)$$

is 1-dimensional, where we identify $H^1_{\mathrm{ur}}(K_v, W)$ with its image in $H^1(K_v, V)$.

(4) If E has good reduction at $v|2$, then

$$\mathcal{L}_v = H^1_{\mathrm{fl}}(\mathrm{Spec}\,\mathcal{O}_v, \mathcal{E}[2]) \otimes k,$$

where $\mathcal{E}/\mathcal{O}_v$ is the Néron model of E/K_v and $H^1_{\mathrm{fl}}(\mathrm{Spec}\,\mathcal{O}_v, \mathcal{E}[2])$ is the flat cohomology group, viewed as a subspace of $H^1_{\mathrm{fl}}(\mathrm{Spec}\,K_v, E[2]) = H^1(K_v, E[2])$.

(5) If E has multiplicative reduction at $v|2$, then there is a unique $G_{\mathbb{Q}_2}$-stable line $W \subseteq V$ by Assumption 4.1 (3) that $\bar\rho_{E,2}$ is ramified at 2. We have

$$\mathcal{L}_v = \mathrm{im}(H^1(\mathbb{Q}_2, W) \to H^1(\mathbb{Q}_2, V)).$$

Proof. For $v \nmid 2qN\infty$, $\mathcal{L}_v = H^1_{\mathrm{ur}}(K_v, V)$ by [GP12, Lemma 6]. For $v|2N$, since v is split in K, the items (1), (4) and (5) follow from the corresponding items (1), (4) and (5) in [LHL16, Lemma 6.6]. The item (2) is clear since K is imaginary. It remains to prove (3), which is the key difference from the case over $\mathbb{Q}$ considered in [LHL16, Lemma 6.6].

Our argument closely follows the proof of [GP12, Lemma 8]. Let $\mathcal{A}/\mathbb{Z}_q$ be the Néron model of $A/\mathbb{Q}_q$. Let $\mathcal{A}^0/\mathbb{F}_q$ be the identity component of the special fiber of $\mathcal{A}$. Since A is an isogeny factor of the new quotient of $J_0(Nq)$, it has purely toric reduction at q: $\mathcal{A}^0/\mathbb{F}_q$ is a torus that is split over $\mathbb{F}_{q^2}$ and it is split over $\mathbb{F}_q$ if and only if $\varepsilon_q(g/\mathbb{Q}) = -1$. By the Néron mapping property, $\mathcal{O}_F$ acts on $\mathcal{A}^0$ and makes the character group $X^*(\mathcal{A}^0/\mathbb{F}_q) \otimes \mathbb{Q}$ a 1-dimensional F-vector space.

Let $T/\mathbb{Q}_q$ be the split torus with character group $X^*(\mathcal{A}^0/\mathbb{F}_q)$. Let $\chi : \mathrm{Gal}(K_q/\mathbb{Q}_q) \to \{\pm 1\}$ be the trivial or nontrivial quadratic character according to whether $\mathcal{A}^0/\mathbb{F}_p$ splits over $\mathbb{F}_q$ or not. Let $T(\chi)/\mathbb{Q}_q$ be the twist of $T/\mathbb{Q}_q$ by χ. Then $\mathcal{O}_F$ naturally acts on T (dual to the action on the character group). By the theory of q-adic uniformization (cf. [BL91]), we have a $G_{\mathbb{Q}_q}$-equivariant exact sequence

$$0 \to \Lambda \to T(\chi)(\overline{\mathbb{Q}_q}) \to A(\overline{\mathbb{Q}_q}) \to 0,$$

where Λ is a free $\mathbb{Z}$-module with the $G_{\mathbb{Q}_q}$-action by χ. Since $\mathcal{O}_F$ is a maximal order, Λ is a locally free $\mathcal{O}_F$-module of rank one. Consider the following commutative diagram

$$\begin{tikzcd} T(\chi)(K_q) \otimes \mathcal{O}_F/\lambda \arrow[r] \arrow[d] & H^1(K_q, T(\chi)[\lambda]) \arrow[d] \\ A(K_q) \otimes \mathcal{O}_F/\lambda \arrow[r] & H^1(K_q, A[\lambda]). \end{tikzcd}$$

Here, the horizontal arrows are the local Kummer maps and the vertical maps are induced by the q-adic uniformization. The left vertical map is surjective since its cokernel lies in $H^1(K_q, \Lambda) = \mathrm{Hom}(G_{K_q}, \Lambda)$, which is zero as Λ is torsion-free. The top horizontal map is also surjective since its cokernel maps into $H^1(K_q, T(\chi))$, which is zero by Hilbert 90 as $T(\chi)$ is a split torus over K_q. It follows that

$$\mathcal{L}_q = \mathrm{im}\left(H^1(K_q, T(\chi)[\lambda]) \to H^1(K_q, A[\lambda])\right).$$

Also, because Λ has no λ-torsion, we see that $T(\chi)[\lambda] \to A[\lambda]$ is a $G_{\mathbb{Q}_q}$-equivariant injection (for this we need the twist $T(\chi)$ rather than T). But since $\mathrm{Frob}_q \in G_{\mathbb{Q}_q}$ is assumed to have order 2 acting on $V = A[\lambda]$, V has a unique $G_{\mathbb{Q}_q}$-stable line W. Therefore

$$\mathcal{L}_q = \mathrm{im}(H^1(K_q, W) \to H^1(K_q, V)).$$

Since q is inert in K, we know that $\mathrm{Frob}_q \in G_{K_q}$ acts on V trivially. Hence $H^1(K_q, V)$ is 4-dimensional and $H^1_{\mathrm{ur}}(K_q, V)$ is 2-dimensional. The intersection $\mathcal{L}_q \cap H^1_{\mathrm{ur}}(V) = H^1_{\mathrm{ur}}(K_q, W)$ consists of unramified homomorphisms $\mathrm{Gal}(K_q^{\mathrm{ur}}/K_q) \to W$, hence is 1-dimensional. □

5. $\mathcal{L}_v(A)$ is maximal totally isotropic for the quadratic form Q_v

Since we are working in characteristic 2, to prove Conjecture 1.6, we need not only the perfect local Tate pairing

$$\langle\ ,\ \rangle_v : H^1(K_v, V) \times H^1(K_v, V) \to k(1),$$

but also a quadratic form Q_v giving rise to it. To define Q_v, first recall that the line bundle $\mathcal{L} = \mathcal{O}_E(2\infty)$ on E induces a degree 2 map

$$E \to \mathbb{P}^1 = \mathbb{P}(H^0(E, \mathcal{L})).$$

For $P \in E$, let τ_P be the translation by P on E. Since for $P \in E[2]$, $\tau_P^*\mathcal{L} \cong \mathcal{L}$, the translation by $E[2]$ induces an action of $E[2]$ on $\mathbb{P}^1$, i.e., a homomorphism $E[2] \to \mathrm{PGL}_2$.

Definition 5.1. For a place v of K, we define

$$Q_v : H^1(K_v, E[2]) \to H^1(K_v, \mathrm{PGL}_2) \to H^2(K_v, \mathbb{G}_m),$$

where the first map is induced by the above homomorphism $E[2] \to \mathrm{PGL}_2$ and the second map is induced by the short exact sequence

$$1 \to \mathbb{G}_m \to \mathrm{GL}_2 \to \mathrm{PGL}_2 \to 1.$$

By local class field theory, $H^2(K_v, \mathbb{G}_m) \cong \mathbb{Q}/\mathbb{Z}$ and so Q_v takes value in $H^2(K_v, \mathbb{G}_m)[2] \cong \mathbb{Z}/2\mathbb{Z}$. By [O'N02, §4], Q_v is a quadratic form and extending scalars we obtain a quadratic form

$$Q_v : H^1(K_v, V) \to k.$$

By [O'N02, 4.3], the associated bilinear form $(x,y) \mapsto Q_v(x+y) - Q_v(x) - Q_v(y)$ is equal to the local Tate pairing $\langle\ ,\ \rangle_v$.

Definition 5.2. We say a subspace $W \subseteq H^1(K_v, V)$ is *totally isotropic for* Q_v if $Q_v|_W = 0$. We say W is *maximal totally isotropic for* Q_v if it is totally isotropic and $W = W^\perp$ (orthogonal complement under $\langle\ ,\ \rangle_v$).

Remark 5.3. As $\mathrm{char}(k) = 2$, the requirement $Q_v|_W = 0$ is stronger than $\langle\ ,\ \rangle_v|_W = 0$. For example, for the 2-dimensional quadratic space (k^2, Q) with $Q((x,y)) = xy$, the associated bilinear form is given by

$$\langle (x_1, y_1), (x_2, y_2) \rangle = x_1 y_2 + x_2 y_1.$$

In particular $\langle (x,y), (x,y) \rangle = 2xy = 0$ and hence all three lines in k^2 are maximal totally isotropic for the bilinear form $\langle\ ,\ \rangle$. But only the two lines $x = 0$ and $y = 0$ are maximal totally isotropic for the quadratic form Q.

Remark 5.4. The local condition $\mathcal{L}_v(E)$ for the elliptic curve E is maximal totally isotropic for Q_v by [PR12, Prop. 4.11] (this is also implicit in [O'N02, Prop. 2.3]).

Lemma 5.5. *Suppose* $\mathrm{Frob}_q \in G_{\mathbb{Q}_q}$ *has order 2 acting on* V*. Then for any place* v *of* K*,* $\mathcal{L}_v(A)$ *is maximal totally isotropic for* Q_v*.*

Proof. The claim for $v \neq q$ follows immediately from Lemma 4.3 and Remark 5.4. It remains to check the case $v = q$. We provide an explicit way to compute the image of a cocycle $c \in H^1(K_q, E[2])$ under Q_q. Recall that $H^1(K_q, \mathrm{PGL}_2)$ classifies forms of $\mathbb{P}^1$, i.e., algebraic varieties S/K_q which become isomorphic to $\mathbb{P}^1$ over $\overline{K_q}$. For any cocycle c, the corresponding form S can be described as follows. As a set, $S = \mathbb{P}^1(\overline{K_q})$. The Galois action of $g \in G_{K_q}$ on $x \in S$ is given by $g.x = c(g).g(x)$. The cocycle c gives the trivial class in $H^1(K_q, \mathrm{PGL}_2)$ if and only if $S(K_q) \neq \varnothing$.

Since $\mathrm{Frob}_q \in G_{\mathbb{Q}_q}$ has order 2 acting on V (i.e., $\bar\rho_{E,2}(\mathrm{Frob}_q)$ is conjugate to $\left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right)$), we know that $E[2](\mathbb{Q}_q) \cong \mathbb{Z}/2\mathbb{Z}$. Let P be the generator of $E[2](\mathbb{Q}_q)$. Let $\sigma \in G_{K_q}$ be a Frobenius and let τ be a generator of the tame quotient $\mathrm{Gal}(K_q^t/K_q^{\mathrm{ur}})$. Then by Lemma 4.3 (3), $\mathcal{L}_q(A)$ is generated by the two cocycles

$$c(\sigma) = 0, \quad c(\tau) = P$$

and

$$c'(\sigma) = P, \quad c'(\tau) = 0.$$

For the cocycle c, the corresponding form S has a K_q-rational point if and only if there exists $x \in \mathbb{P}^1(K_q^t)$ such that

$$\sigma(x) = x, \quad P.\tau(x) = x.$$

Suppose E has a Weierstrass equation $y^2 = F(x)$, where $F(x) \in \mathbb{Q}[x]$ is an irreducible cubic polynomial. Let $\alpha_1, \alpha_2, \alpha_3$ be the three roots of $F(x)$. Without loss of generality, we may assume that $\alpha_1 \in \mathbb{Q}_q$ and thus $P = (\alpha_1, 0)$. Then the action of P on $\mathbb{P}^1$ is an involution that swaps $\alpha_1 \leftrightarrow \infty$, $\alpha_2 \leftrightarrow \alpha_3$. One can compute explicitly that this involution is given by the linear fractional transformation

$$x \mapsto \frac{\alpha_1 x + (\alpha_2\alpha_3 - \alpha_1\alpha_2 - \alpha_1\alpha_3)}{x - \alpha_1}.$$

Therefore $Q_q(c) = 0$ if and only if there exists $x \in \mathbb{P}^1(K_q^t)$ such that

$$\sigma(x) = x, \quad (\tau(x) - \alpha_1)(x - \alpha_1) = (\alpha_2 - \alpha_1)(\alpha_3 - \alpha_1). \tag{5.1}$$

The right hand side is the image of $\alpha_1 - \alpha_2$ under the norm map $K_q^\times \to \mathbb{Q}_q^\times$, hence has even valuation. Thus $\beta = \sqrt{(\alpha_2 - \alpha_1)(\alpha_3 - \alpha_1)}$ lies in K_q and $x = \alpha_1 + \beta \in K_q$ satisfies (5.1). It follows that $Q_q(c) = 0$. Similarly, $Q_q(c') = 0$ if and only if there exists $x \in \mathbb{P}^1(K_q^{\mathrm{ur}})$ such that

$$(\sigma(x) - \alpha_1)(x - \alpha_1) = (\alpha_2 - \alpha_1)(\alpha_3 - \alpha_1).$$

Again $x = \alpha_1 + \beta \in K_q$ is a solution and we see that $Q_q(c') = 0$.

It follows that $\mathcal{L}_q(A)$ is totally isotropic for Q_q. By Lemma 4.3 (3), the dimension of $\mathcal{L}_q(A)$ is half of the dimension of $H^1(K_q, V)$, hence $\mathcal{L}_q$ is maximally totally isotropic for Q_q. □

Remark 5.6. The local condition $\mathcal{L}_q(A)$ may fail to be maximal totally isotropic for Q_q when working *over* $\mathbb{Q}$ instead of *over* K. This is expected since there is no parity prediction over $\mathbb{Q}$ (Remark 3.2).

6. Parity of 2-Selmer ranks

Now we are ready to prove the parity conjecture on 2-Selmer ranks.

Theorem 6.1. *Assume Assumption 4.1. Suppose* $\mathrm{Frob}_q \in G_{\mathbb{Q}_q}$ *has order 2 acting on* V. *Then*

$$s_2(E/K) = s_\lambda(A/K) \pm 1.$$

Moreover,

$$s_2(E/K) = s_\lambda(A/K) - 1$$

if and only if $\mathrm{res}_q(\mathrm{Sel}_2(E/K) \otimes k) \subseteq H^1_{\mathrm{ur}}(K_q, W)$, *where* W *is the unique* $G_{\mathbb{Q}_q}$*-stable line in* V.

Proof. Define the strict local conditions $\mathcal{S}$ by $\mathcal{S}_v = \mathcal{L}_v(E) = \mathcal{L}_v(A)$ for $v \neq q$ and

$$\mathcal{S}_q = \mathcal{L}_q(E) \cap \mathcal{L}_q(A) = H^1_{\mathrm{ur}}(K_q, W).$$

The second equality is by Lemma 4.3 (3), where we identified $H^1_{\mathrm{ur}}(K_q, W)$ with its image in $H^1(K_q, V)$. Similarly, define the relaxed local conditions $\mathcal{R}$ by $\mathcal{R}_v = \mathcal{L}_v(E) = \mathcal{L}_v(A)$ for $v \neq q$ and $\mathcal{R}_q = \mathcal{S}_q^\perp$. Then we have

$$H^1_{\mathcal{S}}(V) \subseteq H^1_{\mathcal{L}(E)}(V) \subseteq H^1_{\mathcal{R}}(V), \quad H^1_{\mathcal{S}}(V) \subseteq H^1_{\mathcal{L}(A)}(V) \subseteq H^1_{\mathcal{R}}(V).$$

Since $\mathcal{S}^\perp = \mathcal{R}$, we use [DDT97, Theorem 2.18] to compare the dual Selmer groups:

$$\frac{\# H^1_{\mathcal{S}}(V)}{\# H^1_{\mathcal{R}}(V)} = \prod_v \frac{\# \mathcal{S}_v}{\# H^0(K_v, V)}, \quad \frac{\# H^1_{\mathcal{R}}(V)}{\# H^1_{\mathcal{S}}(V)} = \prod_v \frac{\# \mathcal{R}_v}{\# H^0(K_v, V)},$$

where v runs over all places of K. It follows that

$$\dim H^1_{\mathcal{R}}(V) - \dim H^1_{\mathcal{S}}(V) = \frac{1}{2}(\dim \mathcal{R}_q - \dim \mathcal{S}_q) = 1,$$

since $\mathcal{S}_q$ is 1-dimensional and $\mathcal{R}_q$ is 3-dimensional. By global class field theory, for any class $c \in H^1_{\mathcal{R}}(V)$, we have

$$\sum_v Q_v(\mathrm{res}_v(c)) = 0.$$

Since $\mathcal{R}_v$ is totally isotropic for Q_v for any $v \neq q$ by Remark 5.4, we know that $Q_q(\mathrm{res}_q(c)) = 0$. In other words, the image $\mathrm{res}_q(H^1_{\mathcal{R}}(V))$ is also a totally isotropic subspace for Q_q. It follows that the quotient space $(\mathrm{res}_q(H^1_{\mathcal{R}}(V)) + \mathcal{S}_q)/\mathcal{S}_q$ is a nonzero totally isotropic subspace of $\mathcal{R}_q/\mathcal{S}_q$ under (the quadratic form induced by) Q_q.

Since $\mathcal{R}_q/\mathcal{S}_q$ is a 2-dimensional quadratic space obtained by extending scalars from a 2-dimensional quadratic space over $\mathbb{F}_2$ and $\mathcal{R}_q/\mathcal{S}_q$ contains an isotropic line under Q_q, we know that it must have Arf invariant 0 and thus is isomorphic to (k^2, xy) as a quadratic space. By Remark 5.3, there are exactly two maximal totally isotropic subspaces of $\mathcal{R}_q$ containing $\mathcal{S}_q$. On the other hand, we already have two such maximal totally isotropic subspaces by Remark 5.4 and Lemma 5.5: namely $\mathcal{L}_q(E)$

and $\mathcal{L}_q(A)$. It follows that either $H^1_{\mathcal{R}}(V) = H^1_{\mathcal{L}(E)}(V)$ or $H^1_{\mathcal{R}}(V) = H^1_{\mathcal{L}(A)}(V)$. The two cases cannot hold simultaneously since

$$H^1_{\mathcal{L}(A)}(V) \cap H^1_{\mathcal{L}(E)}(V) = H^1_{\mathcal{S}}(V) \subsetneq H^1_{\mathcal{R}}(V).$$

So either

$$H^1_{\mathcal{L}(A)}(V) = H^1_{\mathcal{R}}(V), \quad H^1_{\mathcal{L}(E)}(V) = H^1_{\mathcal{S}}(V),$$

or

$$H^1_{\mathcal{L}(E)}(V) = H^1_{\mathcal{R}}(V), \quad H^1_{\mathcal{L}(A)}(V) = H^1_{\mathcal{S}}(V).$$

Moreover, the first case happens if and only if $\mathrm{res}_q(H^1_{\mathcal{L}(E)}(V)) \subseteq \mathcal{S}_q$. The desired result then follows. □

Remark 6.2. The conclusion of Theorem 6.1 may fail when dropping the assumption that $\bar\rho_{E,2}|_{G_{\mathbb{Q}_2}}$ is nontrivial, due to the uncertainty of the local condition at 2. For example, the elliptic curve

$$E = 2351a1 : y^2 + xy + y = x^3 - 5x - 5$$

has trivial $\bar\rho_{E,2}|_{G_{\mathbb{Q}_2}}$. The elliptic curve

$$A = 25861i1 : y^2 + xy + y = x^3 + x^2 - 17x + 30$$

is obtained from E via level raising at $q = 11 \pmod 2$. For $K = \mathbb{Q}(\sqrt{-111})$, we have

$$\operatorname{rank} E(K) = s_2(E/K) = 1 \text{ and } \operatorname{rank}(A/K) = s_2(A/K) = 4$$

differ by 3 (rather than 1).

7. OBSTRUCTION TO RANK LOWERING

It follows from Theorem 6.1 that if $s_2(E/K) = 1$, then $s_\lambda(A/K) = 0$ or 2. However, the Chebotarev density argument for $p \geq 5$ in [Zha14, Lemma 7.3] fails in this case and does not show that one can always get $s_\lambda(A/K) = 0$. In fact, we prove the following obstruction to rank lowering: $s_\lambda(A/K)$ can never be lowered to zero!

Theorem 7.1. *Assume Assumption 4.1. Suppose* $\mathrm{Frob}_q \in G_{\mathbb{Q}_q}$ *has order 2 acting on* V*. Then*

$$s_2(E/K) = 1 \Longrightarrow s_\lambda(A/K) = 2.$$

Proof. By Theorem 6.1, we need to show that $\mathrm{res}_q(\mathrm{Sel}_2(E/K) \otimes k) \subseteq H^1_{\mathrm{ur}}(K_q, W)$, where W is the unique $G_{\mathbb{Q}_q}$-stable line in V. By definition, the Galois group $\mathrm{Gal}(K/\mathbb{Q})$ acts on $\mathrm{Sel}_2(E/K)$. By assumption, we have $\mathrm{Sel}_2(E/K) \cong \mathbb{Z}/2\mathbb{Z}$, so the action of $\mathrm{Gal}(K/\mathbb{Q})$ on $\mathrm{Sel}_2(E/K)$ must be *trivial*. It follows that

$$\mathrm{res}_q(\mathrm{Sel}_2(E/K) \otimes k) \subseteq H^1_{\mathrm{ur}}(K_q, V)^{\mathrm{Gal}(K_q/\mathbb{Q}_q)}.$$

The right hand side is nothing but $H^1_{\mathrm{ur}}(K_q, W)$, as desired. □

We end with an example illustrating Theorem 7.1.

Example 7.2. Consider $E = 11a1 = X_0(11)$. In Table 2 we list the first few level raising primes q and corresponding level raising abelian varieties A (all of which are elliptic curves). For each choice of $K = \mathbb{Q}(\sqrt{d_K})$, we find that $s_2(A/K) = 2$ always! In many cases, this is explained by the fact that $\operatorname{rank} A(K) = 2$. In the remaining cases, we have

$$\dim_{\mathbb{F}_2} Ш(A/K)[2] = 2,$$

q	A	d_K	$\operatorname{rank} A(K)$	$\dim Ш(A/K)[2]$	$s_2(A/K)$
7	$77a$	-8	2	0	2
7	$77b$	-8	0	2	2
13	$143a$	-7	2	0	2
13	$143a$	-8	2	0	2
17	$187a$	-7	2	0	2
17	$187a$	-24	0	2	2
19	$209a$	-7	2	0	2
19	$209a$	-19	2	0	2
29	$319a$	-8	2	0	2
29	$319a$	-19	0	2	2

Table 2. obstruction to rank lowering

though in all such cases the 2-part of Ш for $A/\mathbb{Q}$ and its quadratic twist $A^K/\mathbb{Q}$ are both trivial,

$$Ш(A/\mathbb{Q})[2] = 0, \quad Ш(A^K/\mathbb{Q})[2] = 0.$$

Notice that this is a phenomenon unique to $p = 2$ because for odd p it is always true that

$$Ш(A/K)[p] \cong Ш(A/\mathbb{Q})[p] \oplus Ш(A^K/\mathbb{Q})[p].$$

References

[BBV16] A. Berti, M. Bertolini and R. Venerucci, Congruences between modular forms and the Birch and Swinnerton-Dyer conjecture, in *Elliptic curves, modular forms and Iwasawa theory*, volume 188 of *Springer Proc. Math. Stat.*, pages 1–31, Springer, Cham, 2016.

[BCP97] W. Bosma, J. Cannon and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24**(3-4), 235–265 (1997), Computational algebra and number theory (London, 1993).

[BD99] M. Bertolini and H. Darmon, *Euler systems and Jochnowitz congruences*, Amer. J. Math. **121**(2), 259–281 (1999).

[BKL+15] M. Bhargava, D. M. Kane, H. W. Lenstra, jr., B. Poonen and E. Rains, *Modeling the distribution of ranks, Selmer groups, and Shafarevich-Tate groups of elliptic curves*, Camb. J. Math. **3**(3), 275 – 321 (2015).

[BL91] S. Bosch and W. Lütkebohmert, *Degenerating abelian varieties*, Topology **30**(4), 653–698 (1991).

[Cas17] F. Castella, *On the p-part of the Birch-Swinnerton-Dyer formula for multiplicative primes*, ArXiv e-prints (April 2017), 1704.06608.

[CCL16] L. Cai, Y. Chen and Y. Liu, *Heegner Points on Modular Curves*, ArXiv e-prints (January 2016), 1601.04415.

[CLTZ15] J. Coates, Y. Li, Y. Tian and S. Zhai, *Quadratic twists of elliptic curves*, Proc. Lond. Math. Soc. (3) **110**(2), 357–394 (2015).

[Cre97] J. E. Cremona, *Algorithms for modular elliptic curves*, Cambridge University Press, Cambridge, second edition, 1997.

[DDT97] H. Darmon, F. Diamond and R. Taylor, Fermat's last theorem, in *Elliptic curves, modular forms & Fermat's last theorem (Hong Kong, 1993)*, pages 2–140, Int. Press, Cambridge, MA, 1997.

[Del01] C. Delaunay, *Heuristics on Tate-Shafarevitch groups of elliptic curves defined over* $\mathbb{Q}$, Experiment. Math. **10**(2), 191–196 (2001).

[Fla90] M. Flach, *A generalisation of the Cassels-Tate pairing*, J. Reine Angew. Math. **412**, 113–127 (1990).

[GA97] C. D. Gonzalez-Avilés, *On the conjecture of Birch and Swinnerton-Dyer*, Trans. Amer. Math. Soc. **349**(10), 4181–4200 (1997).

[GGR05] J. González, J. Guàrdia and V. Rotger, *Abelian surfaces of* GL_2*-type as Jacobians of curves*, Acta Arith. **116**(3), 263–287 (2005).

[GP12] B. H. Gross and J. A. Parson, On the local divisibility of Heegner points, in *Number theory, analysis and geometry*, pages 215–241, Springer, New York, 2012.

[Gro11] B. H. Gross, Lectures on the conjecture of Birch and Swinnerton-Dyer, in *Arithmetic of L-functions*, volume 18 of *IAS/Park City Math. Ser.*, pages 169–209, Amer. Math. Soc., Providence, RI, 2011.

[Guo96] J. Guo, *On the positivity of the central critical values of automorphic L-functions for* GL(2), Duke Math. J. **83**(1), 157–190 (1996).

[GZ86] B. H. Gross and D. B. Zagier, *Heegner points and derivatives of L-series*, Invent. Math. **84**(2), 225–320 (1986).

[JSW15] D. Jetchev, C. Skinner and X. Wan, *The Birch and Swinnerton-Dyer Formula for Elliptic Curves of Analytic Rank One*, ArXiv e-prints (December 2015), 1512.06894.

[Kat04] K. Kato, *p-adic Hodge theory and values of zeta functions of modular forms*, Astérisque (295), ix, 117–290 (2004), Cohomologies p-adiques et applications arithmétiques. III.

[KL16] D. Kriz and C. Li, *Congruences between Heegner points and quadratic twists of elliptic curves*, ArXiv e-prints (June 2016), 1606.03172.

[Kla12] Z. Klagsbrun, *Elliptic curves with a lower bound on 2-Selmer ranks of quadratic twists*, Math. Res. Lett. **19**(5), 1137–1143 (2012).

[LHL16] B. V. Le Hung and C. Li, *Level raising* mod 2 *and arbitrary 2-Selmer ranks*, Compos. Math. **152**(8), 1576–1608 (2016).

[MR10] B. Mazur and K. Rubin, *Ranks of twists of elliptic curves and Hilbert's tenth problem*, Invent. Math. **181**(3), 541–575 (2010).

[Nek] J. Nekovar, *Compatibility of arithmetic and algebraic local constants II. The tame abelian potentially Barsotti-Tate case.*, `https://webusers.imj-prg.fr/~jan.nekovar/pu/tame.pdf`.

[O'N02] C. O'Neil, *The period-index obstruction for elliptic curves*, J. Number Theory **95**(2), 329–339 (2002).

[PR12] B. Poonen and E. Rains, *Random maximal isotropic subspaces and Selmer groups*, J. Amer. Math. Soc. **25**(1), 245–269 (2012).

[PS99] B. Poonen and M. Stoll, *The Cassels-Tate pairing on polarized abelian varieties*, Ann. of Math. (2) **150**(3), 1109–1149 (1999).

[Rib90] K. A. Ribet, Raising the levels of modular representations, in *Séminaire de Théorie des Nombres, Paris 1987–88*, volume 81 of *Progr. Math.*, pages 259–271, Birkhäuser Boston, Boston, MA, 1990.

[S$^+$13] W. Stein et al., *Sage Mathematics Software (Version 5.11)*, The Sage Development Team, 2013, `http://www.sagemath.org`.

[Ser87] J.-P. Serre, *Sur les représentations modulaires de degré* 2 *de* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, Duke Math. J. **54**(1), 179–230 (1987).

[Spr16] F. Sprung, *The Iwasawa Main Conjecture for elliptic curves at odd supersingular primes*, ArXiv e-prints (October 2016), 1610.10017.

[SU14] C. Skinner and E. Urban, *The Iwasawa main conjectures for* GL_2, Invent. Math. **195**(1), 1–277 (2014).

[SZ14] C. Skinner and W. Zhang, *Indivisibility of Heegner points in the multiplicative case*, ArXiv e-prints (July 2014), 1407.1099.

[Tia14] Y. Tian, *Congruent numbers and Heegner points*, Camb. J. Math. **2**(1), 117–161 (2014).

[Wan14] X. Wan, *Iwasawa Main Conjecture for Supersingular Elliptic Curves*, ArXiv e-prints (November 2014), 1411.6352.

[Zar74] J. G. Zarhin, *Noncommutative cohomology and Mumford groups*, Mat. Zametki **15**, 415–419 (1974).

[Zha14] W. Zhang, *Selmer groups and the indivisibility of Heegner points*, Camb. J. Math. **2**(2), 191 – 253 (2014).

E-mail address: `chaoli@math.columbia.edu`

Department of Mathematics, Columbia University, 2990 Broadway, New York, NY 10027