LEVEL RAISING MOD 2 AND OBSTRUCTION FOR 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 $A$. This abelian variety $A$ is associated to a modular form $g$ of weight 2 and level $Nq$ that is obtained by Ribet’s level raising theorem from the modular form $f$ of level $N$ associated to $E$.

Over an imaginary quadratic field $K$ satisfying the Heegner hypothesis for $E$ such that $q$ is inert in $K$, the two modular forms $f$ and $g$ have opposite signs of functional equations. 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 a surprising obstruction for rank lowering which is unseen for $p$-Selmer groups for odd $p$.

1. Introduction

1.1. The $p$-part of the BSD formula. Given an elliptic curve $E$ defined over $\mathbb{Q}$, the rational points $E(\mathbb{Q})$ form a finitely generated abelian group by the Mordell–Weil theorem. It is a central question in number theory to understand the rank of $E(\mathbb{Q})$, known as the algebraic rank

$$r_{\text{alg}}(E/\mathbb{Q}) := \text{rank } E(\mathbb{Q}).$$

Another important invariant of $E$ is the analytic rank

$$r_{\text{an}}(E/\mathbb{Q}) := \text{ord}_{s=1} L(E/\mathbb{Q}, s),$$

defined as the order of vanishing of its $L$-function $L(E/\mathbb{Q}, s)$ at the central point $s = 1$. The remarkable Birch and Swinnerton-Dyer conjecture asserts that the algebraic rank is equal to the analytic rank. It furthermore predicts a precise formula (the BSD formula)

$$L^{(r)}(E/\mathbb{Q}, 1) = \frac{\prod_p c_p(E/\mathbb{Q}) \cdot |\Sha(E/\mathbb{Q})|}{|E(\mathbb{Q})_{\text{tor}}|^2}$$

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 $r_{\text{an}} \leq 1$. In this case, both sides of the BSD formula (1.1) are known to be positive rational numbers. 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 (denoted by BSD($p$) for short), for which much progress has been made:

- When $r_{\text{an}} = 0$, BSD($p$) is known for $p \geq 3$ (under certain assumptions) as a consequence of the Iwasawa main conjecture for modular forms ([Kat04], [SU14], [Wan14]).

2010 Mathematics Subject Classification. 11G05 (primary), 11R34, 11G10 (secondary).

Key words and phrases. Selmer groups, elliptic curves, abelian varieties.
When \( r_{an} = 1 \), BSD\((p)\) is known for \( p \geq 5 \) (under certain assumptions) due to the recent work of W. Zhang [Zha14], as a consequence of his proof of Kolyvagin’s conjecture on \( p \)-indivisibility of derived Heegner points (see also [SZ14] for an extension of this result).

On the other hand, very little is known for BSD\((2)\) (but see Remark 1.8). 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 factors, and most frequently, the factor 2. We remark that this phenomenon is also expected from heuristics concerning the distribution of small prime factors.

1.2. \( p \)-Selmer groups and W. Zhang’s strategy. We are 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. Recall that for a number field \( K \), the \( p \)-Selmer group \( \text{Sel}_p(E/K) \) is a subspace of the Galois cohomology group \( H^1(K, E[p]) \), cut out by local conditions coming from local points \( E(K_v) \) for each place \( v \) of \( K \). Namely, it sits in the pull-back diagram

\[
\begin{align*}
\text{Sel}_p(E/K) & \longrightarrow H^1(K, E[p]) \\
\prod_v E(K_v)/pE(K_v) & \longrightarrow \prod_v H^1(K_v, E[p]).
\end{align*}
\]

Its \( \mathbb{F}_p \)-dimension is called the \( p \)-Selmer rank of \( E/K \) and is denoted by \( s_p(E/K) \). By the \( p \)-descent exact sequence

\[ 0 \to E(K)/pE(K) \to \text{Sel}_p(E/K) \to \text{III}(E/K)[p] \to 0, \]

the \( p \)-Selmer rank \( s_p(E/K) \) gives an upper bound of the algebraic rank \( r_{alg}(E/K) \) and the defect is measured by the \( p \)-part of the Tate–Shafarevich group \( \text{III}(E/K) \).

Zhang’s key strategy reduces BSD\((p)\) from the \( p \)-Selmer rank one case to the rank zero case and roughly consists of three steps:

A: Let \( f \in S_2(N) \) be the newform associated to \( E/\mathbb{Q} \). Find a congruence \( f \equiv g \pmod{p} \) between \( f \) and another newform \( g \in S_2(Nq) \) with level raised at some prime \( q \) (level raising mod \( p \)).

B: Let \( K \) be an imaginary quadratic field satisfying the Heegner hypothesis for \( E \) (so that there exists a Heegner point \( y_K \in E(K) \)). Assume the level raising prime \( q \) is inert in \( K \). Let \( A \) be the elliptic curve associated to \( g \). Show that (in the minimally ramified case)

\[ y_K \notin pE(K_q) \iff s_p(A/K) = 0. \]

C: Notice that \( E/K \) and \( A/K \) have opposite signs of functional equations (sign changing), so the BSD conjecture predicts that their \( p \)-Selmer ranks have different parity. Prove that one can always find a choice of \( q \) and \( g \) in Step B such that \( s_p(A/K) = s_p(E/K) - 1 \) (rank lowering). In particular, when \( s_p(E/K) = 1 \), we have \( s_p(A/K) = 0 \). It then follows from Step B that the Heegner point \( y_K \notin pE(K_q) \), hence \( y_K \notin pE(K) \). The latter global \( p \)-indivisibility is indeed equivalent to BSD\((p)\) for \( E/K \) by the Gross–Zagier formula.

\[ ^1 \text{When } g \text{ does not have rational Fourier coefficients, one works with the corresponding modular abelian variety instead, see 2.6} \]
Remark 1.3. Step A is ensured by the level raising theorem of Ribet [Rib90] for any $p$ as long as $E[p]$ is an absolutely irreducible $G_Q$-representation. The proof of Step B combines the Jochnowitz congruence established by Bertolini–Darmon [BD99] for $p \geq 5$, Gross’ explicit Waldspurger formula [Gro87], and (one divisibility of) BSD($p$) in the case $r_{an} = 0$ due to Skinner–Urban [SU14] for $p \geq 3$. Step C is achieved by a parity argument of Gross–Parson [GP12] for $p \geq 5$, which verifies the parity prediction on $p$-Selmer ranks for some good choice of $q$ by showing that $s_p(A/K) = s_p(E/K) \pm 1$, and by a Chebotarev density argument.

Remark 1.4. One can interpret this strategy as a congruence between (suitably defined algebraic parts of) $L'(E/K)$ and $L(A/K)$:

- the $p$-part of $L'(E/K)$ is related to the $p$-divisibility of the Heegner point $y_K$ by the Gross–Zagier formula for $E/K$;
- the $p$-part of $L(A/K)$ is related to $s_p(A/K)$ by BSD for $A/K$.

We depict the three steps as follows.

\[
\begin{array}{ccc}
E & A & C: \text{Rank lowering} \\
\downarrow & \downarrow & \\
\downarrow & \downarrow & \\
f & \equiv & g \pmod{p} \\
\downarrow & \downarrow & \\
L'(f/K,1) & \equiv & L(g/K,1) \pmod{p} \\
\downarrow & \downarrow & \\
y_K \notin pE(K) & s_p(A/K) = 0 \\
\end{array}
\]

1.5. Level raising mod 2 and obstruction for rank lowering. Now we specialize the previous discussion to the case $p = 2$ and explain our main results.

After introducing the necessary background on Ribet’s level raising theorem in Step A (§2) and Selmer groups (§3), we state the parity conjecture (Conjecture 4.3) on the 2-Selmer ranks of $E/K$ and $A/K$ as predicted by BSD. Using the results on local conditions proved in §5–6, we verify this parity conjecture in §7, in a way similar to [GP12] and [Zha14] for $p \geq 5$.

Theorem 1.6 (Theorem 7.1). Assume Assumption 2.1 and 4.1. Suppose Frob$_q$ has order 2 acting on $E[2]$. Then

\[s_2(E/K) = s_2(A/K) \pm 1.\]

Remark 1.7. To get good control over the local condition at $q$, in [GP12] and [Zha14] the level raising prime $q$ is chosen so that Frob$_q$ acts on $E[p]$ semi-simply with distinct eigenvalues different from $\{-1,1\}$. This requirement forces $p \geq 5$ and is not possible for $p = 2$. We overcome this difficulty by choosing Frob$_q$ to be a unipotent element of order 2 acting on $E[2]$ (see also the introduction of [LL15]). Since Frob$_q$ becomes trivial after base changing to the quadratic field $K$, the local condition at $q$ is even harder to determine. Lemma 5.1 and Lemma 6.5 are essential to resolve this issue.

It follows that if $s_2(E/K) = 1$, then $s_2(A/K) = 0$ or 2. Though one can establish an analogue of the Jochnowitz congruence (in Step B) for $p = 2$, the usual Chebotarev density
argument (in Step C) fails and does not show that one can always get $s_2(A/K) = 0$. In fact, in §8 we prove the following surprising obstruction for rank lowering: $s_2(A/K)$ can never be lowered to zero!

**Theorem 1.8** (Theorem 8.1). Assume Assumption 2.1 and 4.1. Suppose $\text{Frob}_q$ has order 2 acting on $E[2]$. Then

$$s_2(E/K) = 1 \implies s_2(A/K) = 2.$$  

**Remark 1.9.** Theorem 1.8 tells us that Step C of proving BSD($p$) cannot naively work for $p = 2$. In joint work with B. Le Hung [LL15], 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 4.4), we show that it is possible to obtain arbitrary $s_2(A/Q)$ via level raising mod 2. In particular, there is no obstruction for rank lowering over $\mathbb{Q}$ in contrast to the situation over $K$. We remark that this obstruction for rank lowering over $K$ is a phenomenon unique to $p = 2$, since the odd part of $\Sha$ never jumps under a quadratic base change! (see Example 8.2.) On the other hand, since there is no such obstruction for $p = 3$, the idea of using the unipotent Frobenius to control Selmer ranks can be used to prove BSD(3) when $r_{an} = 1$ under similar assumptions. We hope to return to this idea in a future work.

**Remark 1.10.** Exciting progress on BSD(2) has been made recently for some explicit families of elliptic curves: see [Tia14], [TYZ14] for many quadratic twists of the congruent number curve $y^2 = x^3 - x$ (in the case $r_{an} = 0$ or 1) and [CLTZ15] for many quadratic twists of $X_0(49)$ (in the case $r_{an} = 0$). In a forthcoming work [KL15], we prove BSD(2) for many quadratic twists of some general classes of elliptic curves (in the case $r_{an} = 0$ or 1), using a new method based on the $p$-adic Waldspurger formula ([BDP13], [LZZ14]) for $p = 2$.

1.11. **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, Benedict Gross, for his constant encouragement and advice throughout this project. I am also thankful to Kestutis Cesnavicius, Bao Le Hung and Wei Zhang for helpful conversations and to Yifeng Liu for useful comments on an earlier draft of this article. The examples in this article are computed using Sage ([S+13]) and Magma ([BCP97]).

2. **Level raising mod 2**

Let $E/\mathbb{Q}$ be an elliptic curve of conductor $N$. Let $\bar{\rho} = \bar{\rho}_{E,2} : G_{\mathbb{Q}} \to \text{Aut}(E[2]) \cong \text{GL}_2(\mathbb{F}_2)$ be the Galois representation on the 2-torsion points. By the modularity theorem, $\bar{\rho}$ comes from a weight 2 cusp newform of level $N$. We make the following mild assumptions.

**Assumption 2.1.**

(1) $E$ has good or multiplicative reduction at 2 (i.e., $4 \nmid N$).

(2) $\bar{\rho}$ is surjective.

(3) The Serre conductor $N(\bar{\rho})$ is equal to the odd part of $N$. If $2 \mid N$, $\bar{\rho}$ is ramified at 2.

(4) If $2 \nmid N$, $\bar{\rho}|_{G_{\mathbb{Q}_2}}$ is nontrivial.

**Remark 2.2.** The assumptions (1-3) are analogous to the ones imposed in [Zha14] and [SZ14] for $p \geq 5$. The assumption (4) is only used in Lemma 5.1 (4) (see Remark 7.2).
Under the above assumptions, $E[2]$ (as a $G_\mathbb{Q}$-module) together with the knowledge of reduction type at a prime $q$ pins down the local condition defining $\text{Sel}_2(E/K)$ at $q$ (see Lemma 5.1 for more precise statements). We would like to keep $E[2]$, but at a prime $q \nmid 2N$ of choice, switch good reduction to multiplicative reduction and thus change the local condition at $q$. For this to happen, a necessary condition is that $\bar{\rho}(\text{Frob}_q) = \left( \begin{smallmatrix} q^* & 0 \\ 0 & 1 \end{smallmatrix} \right) \pmod{2}$ (up to conjugation). Namely, $\bar{\rho}(\text{Frob}_q) = \left( \begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix} \right)$ or $\left( \begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix} \right)$ (order 1 or 2 in $\text{GL}_2(\mathbb{F}_2) \cong S_3$).

**Definition 2.3.** We call $q \nmid 2N$ a level raising prime for $E$ if $\text{Frob}_q$ is of order 1 or 2 acting on $E[2]$. Notice that there are lots of level raising primes: by the Chebotarev density theorem, they make up 2/3 of all primes. If we write $f = \sum_{n \geq 1} a_n q^n \in S_2(N)$ (normalized so that $a_1 = 1$) to be the newform associated to the elliptic curve $E$. Then by definition $q \nmid 2N$ is a level raising prime for $E$ if and only if $a_q$ is even.

Ribet’s level raising theorem [Rib90, Theorem 1] ensures that this necessary condition is also sufficient.

**Theorem 2.4.** Let $E/\mathbb{Q}$ be an elliptic curve satisfying (1-3) of Assumption 2.1. Let $q$ be a level raising prime. Then $\bar{\rho}$ comes from a weight 2 newform of level $Nq$.

**Remark 2.5.** All the level-raised forms will be automatically new at $p \mid N$ due to Assumption 2.1 (3).

So whenever $q$ is a level raising prime, there exists a newform $g = \sum_{n \geq 1} b_n q^n \in S_2(Nq)$ of level $Nq$ such that $g \equiv f \pmod{2}$. More precisely, there exists a prime $\lambda \mid 2$ of the (totally real) Hecke field $F = \mathbb{Q}(\{b_n\}_{n \geq 1})$ such that we have a congruence between the Hecke eigenvalues

$$b_p \equiv a_p \pmod{\lambda}, \quad p \neq q.$$  

**Definition 2.6.** 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 $F$. We choose an $A$ in this isogeny class so that $A$ admits an action by the maximal order $\mathcal{O}_F$. By Assumption 2.1 (2), $A$ is unique up to a prime-to-$\lambda$ isogeny.

Let $k = \mathcal{O}_F/\lambda$ be the residue field. By construction, for almost all primes $p$, $\text{Frob}_p$ has the same characteristic polynomials on the 2-dimensional $k$-vector spaces $E[2] \otimes k$ and $A[\lambda]$. Hence by Chebotarev’s density theorem and the Brauer-Nesbitt theorem we have

$$E[2] \otimes k \cong A[\lambda]$$

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

**Definition 2.7.** We say that $A$ is obtained from $E$ via level raising at $q$.

**Example 2.8.** Consider $E = 11a1 = X_0(11) : y^2 + y = x^3 - x^2 - 10x - 20$. It satisfies Assumption 2.1. Since $a_7 = -2$ is even, we know that $q = 7$ is a level raising prime (so are $q = 13, 17, 19$). The space of newforms of level 77 has dimension 5, which corresponds to three isogeny classes of elliptic curves (77a, 77b, 77c) and one isogeny class of abelian surfaces (77d). Among them (77a, 77b) are obtained from $E$ via level raising at 7. Their first few Hecke eigenvalues are listed in Table 1.
3. Selmer groups

Suppose $A$ is obtained from $E$ via level raising at a level raising prime $q$. Fix an isomorphism between $A[\lambda] \cong E[2] \otimes k$ and denote them by $V$. In this section we first recall the general notion of Selmer groups cut out by local conditions.

**Definition 3.1.** Let $K$ be a number field. Let $v$ be a place of $K$. We define

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

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

**Definition 3.2.** Let $L = \{L_v\}$ be the collection of $k$-subspaces $L_v \subseteq H^1(K_v, V)$, where $v$ runs over every place of $K$. We say $L$ is a collection of local conditions if $L_v = H_{ur}^1(K_v, V)$ for almost all $v$. We define the Selmer group cut out by the local conditions $L$ to be

$$H_L^1(V) := \{x \in H^1(K, V) : \text{res}_v(x) \in L_v, \text{for all } v\}.$$ 

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

$$\begin{array}{ccc}
H_L^1(V) & \longrightarrow & H^1(K, V) \\
\downarrow & & \downarrow \text{res}_v \\
\prod_v L_v & \longrightarrow & \prod_v H^1(K_v, V).
\end{array}$$

**Definition 3.3.** We define $L_v(E)$ to be the image of the local Kummer map

$$(E(K_v)/2E(K_v)) \otimes_{\mathbb{Z}_2} k \to H^1(K_v, E[2]) \otimes k = H^1(K_v, V).$$

Then the Selmer group cut out by $L(E) := \{L_v(E)\}$ is equal to $H_{L(E)}^1(V) = \text{Sel}_2(E/K) \otimes k$.

**Definition 3.4.** Similarly, we define $L_v(A)$ 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 $\lambda$-Selmer group of $A$ is defined to be the Selmer group cut out by $L(A) := \{L_v(A)\}$, denoted by $\text{Sel}_\lambda(A/K)$. For details on descent with endomorphisms, see the appendix of [GP12].

**Definition 3.5.** We denote the 2-Selmer ranks of $E/K$ and $A/K$ by

$$s_2(E/K) := \dim_{\mathbb{F}_2} \text{Sel}_2(E/K), \quad s_2(A/K) := \dim_k \text{Sel}_\lambda(A/K)$$

respectively. Notice that the prime $\lambda|2$ of $K$ is implicit in the notation $s_2(A/K)$ for brevity.

4. Sign changing the parity conjecture

Following [GP12] and [Zha14], in this section deduce a parity prediction on the 2-Selmer ranks of $E/K$ and $A/K$ for certain imaginary quadratic fields $K$. Recall that an imaginary
quadratic field $K$ satisfies the Heegner hypothesis for $E/Q$ if $p$ is split in $K$ for any $p \mid N$, where $N$ is the conductor of $E/Q$. From now on we assume the following assumption.

**Assumption 4.1.**

(1) $K$ is an imaginary quadratic field satisfying the Heegner hypothesis for $E/Q$.

(2) $q$ is a level raising prime for $E$, which is inert in $K$.

**Proposition 4.2.** Assume Assumption 2.1 and 4.1. Then the newform $f$ of level $N$ and newform $g$ of level $Nq$ 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 $\varepsilon_v(f/K)$. For any finite place $v$ of $K$ not dividing the level $N$, $\varepsilon_v(f/K) = +1$. For $p \mid N$, $p$ splits as $p_1p_2$ in $K$ and $\varepsilon_{p_1}(f/K) = \varepsilon_{p_2}(f/K)$, so $\varepsilon_{p_1}(f/K) \cdot \varepsilon_{p_2}(f/K) = +1$. It follows that

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

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. \qed

By Proposition 4.2, the BSD conjecture predicts that $\text{rank} E(K)$ and $\text{rank}_F A(K)$ have different parity. Moreover, $\dim_{\mathbb{F}_2} \text{III}(E/K)[2]$ and $\dim_k \text{III}(A/K)[\lambda]$ should be even. So the BSD conjecture predicts the following

**Conjecture 4.3.** Assume 2.1 and 4.1. Then $s_2(E/K)$ and $s_2(A/K)$ have different parity.

Our next goal is to prove this parity conjecture (Theorem 7.1), as least when $\overline{\rho}(\text{Frob}_q)$ is non-trivial.

**Remark 4.4.** Over $\mathbb{Q}$, the signs $\varepsilon(f/Q)$ and $\varepsilon(g/Q)$ are not necessarily opposite. For example, consider $E = 11a_1$ in Example 2.8. Both $A_1 = 77a$ and $A_2 = 77b$ are obtained from $E$ via level raising at 7 and

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

Therefore level raising mod 2 does not necessarily change the signs of the functional equations over $\mathbb{Q}$ and thus there is no parity prediction. For more refined control over the possible signs under level raising mod 2, see [LL15].

**Remark 4.5.** Notice that $\dim_k \text{III}(A/Q)[\lambda]$ is not necessarily even when $\dim A > 1$: the Cassels–Tate pairing is always skew-symmetric but may fail to be alternating. So even when $\varepsilon(g/Q)$ and $\varepsilon(f/Q)$ are opposite, there is no parity prediction for 2-Selmer groups over $\mathbb{Q}$. This is again a phenomenon unique to $p = 2$. When $A$ has an odd degree polarization, Poonen–Stoll [PS99] constructed an element $c \in \text{III}(A/Q)[2]$ with Cassels–Tate pairing $\langle c, c \rangle = 0$ or $1/2 \in \mathbb{Q}/\mathbb{Z}$, so that $\langle \cdot, \cdot \rangle$ on $\text{III}(A/Q)[2]$ is alternating if and only if $\langle c, c \rangle = 0$. Notice that a quadratic base change $K/Q$ kills the latter obstruction and so the parity prediction is available over $K$ (see, e.g., [Ces14 §3.1]).
5. Local conditions

Under Assumption 2.1 and 4.1, the following lemma identifies the local conditions of 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 5.1.** Suppose $A$ is obtained from $E$ via level raising at $q$ (we allow $A = E$ and view $q = 1$ in this case). Let $\mathcal{L} = \mathcal{L}(A)$ be the local conditions defining $\text{Sel}_\lambda(A/K)$. Then

1. For $v \nmid 2q\infty$, $$\mathcal{L}_v = H^1_{\text{ur}}(K_v, V).$$

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

3. For $v = q$, if $\text{Frob}_q \in G_{Q_q}$ has order 2 acting on $V$, then $H^1(K_v, V)$ is 4-dimensional and $$\mathcal{L}_v = \text{im}(H^1(K_v, W) \to H^1(K_v, V))$$

is 2-dimensional. Here $W$ is the unique $G_{Q_q}$-stable line in $V$. Moreover, $$\mathcal{L}_v \cap H^1_{\text{ur}}(K_v, V) = H^1_{\text{ur}}(K_v, W)$$

is 1-dimensional.

4. If $E$ is good at $v|2$, then $$\mathcal{L}_v = H^1_{\text{fl}}(\text{Spec } O_v, E[2]) \otimes k,$$

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

5. If $E$ is multiplicative at $v|2$, then $$\mathcal{L}_v = \text{im}(H^1(Q_2, W) \to H^1(Q_2, V)).$$

Here $W$ is the unique $G_{Q_2}$-stable line in $V$.

**Proof.** For $v \nmid 2qN\infty$, $\mathcal{L}_v = H^1_{\text{ur}}(K_v, V)$ 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 [LL15, Lemma 5.6]. 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 [LL15, Lemma 5.6].

Our argument closely follows the proof of [GP12, Lemma 8]. Let $A/\mathbb{Z}_q$ be the Néron model of $A/Q_q$. Let $A^0/F_q$ be the identity component of the special fiber of $A$. Since $A$ is an isogeny factor of the new quotient of $J_0(Nq_1 \cdots q_m)$, it has purely toric reduction at $q$: $A^0/F_q$ is a torus that is split over $F_{q^2}$ and it is split over $F_q$ if and only if $\varepsilon_q(g/Q) = -1$. By the Néron mapping property, $O_F$ acts on $A^0$ and makes the character group $X^*(A^0/F_q) \otimes \mathbb{Q}$ a 1-dimensional $F$-vector space.

Let $T/Q_q$ be the split torus with character group $X^*(A^0/F_q)$. Let $\chi : \text{Gal}(K_q/Q_q) \to \{\pm 1\}$ be the trivial or nontrivial quadratic character according to whether $A^0/F_p$ splits over $F_q$ or not. Let $T(\chi)/Q_q$ be the twist of $T/Q_q$ by $\chi$. Then $O_F$ naturally acts on $T$ (dual to the action on the character group). By the theory of $q$-adic uniformization, we have a $G_{Q_q}$-equivariant exact sequence

$$0 \to \Lambda \to T(\chi)(\overline{Q_q}) \to A(\overline{Q_q}) \to 0,$$
where $\Lambda$ is a free $\mathbb{Z}$-module with the $G_{Q_q}$-action by $\chi$. Since $O_F$ is a maximal order, $\Lambda$ is a locally free $O_F$-module of rank one. Consider the following commutative diagram

$$
\begin{array}{ccc}
T(\chi)(K_q) \otimes O_F/\lambda & \longrightarrow & H^1(K_q, T(\chi)[\lambda]) \\
\downarrow & & \downarrow \\
A(K_q) \otimes O_F/\lambda & \longrightarrow & H^1(K_q, A[\lambda]).
\end{array}
$$

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 $H^1(K_q, \Lambda) = \text{Hom}(G_{K_q}, \Lambda)$, which is zero as $\Lambda$ 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

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

Also, because $\Lambda$ has no $\lambda$-torsion, we see that $T(\chi)[\lambda] \to A[\lambda]$ is a $G_{Q_q}$-equivariant injection. But since $\text{Frob}_q \in G_{Q_q}$ is assumed to have order 2 acting on $V = A[\lambda]$, $V$ has a unique $G_{Q_q}$-stable line $W$. Therefore

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

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

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

Since we are working in characteristic 2, to prove the parity conjecture we not only need 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 $\mathcal{L} = O_E(2\infty)$ on $E$ induces a degree 2 map

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

For $P \in E$, let $\tau_P$ 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 $E[2] \to \text{PGL}_2$.

**Definition 6.1.** For a place $v$ of $K$, we define

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

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

$$
0 \to \mathbb{G}_m \to \text{GL}_2 \to \text{PGL}_2 \to 0.
$$

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 [ON02, 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 6.2.** 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 6.3.** As \(\text{char}(k) = 2\), 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
\[
\langle (x_1, y_1), (x_2, y_2) \rangle = x_1y_2 + x_2y_1.
\]
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 6.4.** The local condition \(L_v(E)\) for the elliptic curve \(E\) is maximal totally isotropic for \(Q_v\) by [PR12, Prop. 4.11] (this is also implicit in [ON02, Prop. 2.3]).

**Lemma 6.5.** Suppose \(\text{Frob}_q \in G_{\mathbb{Q}_q}\) has order 2 acting on \(V\). Then for any place \(v\) of \(K\), \(L_v(A)\) is maximal totally isotropic for \(Q_v\).

**Proof.** The claim for \(v \neq q\) follows immediately from Lemma 5.1 and Remark 6.4. 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 \(H^1(K_q, \text{PGL}_2)\) 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 \(H^1(K_q, \text{PGL}_2)\) if and only if \(S(K_q) \neq \emptyset\).

Since \(\text{Frob}_q \in G_{\mathbb{Q}_q}\) has order 2 acting on \(V\), 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 \(\tau\) be a generator of the tame quotient \(\text{Gal}(K'_q/K'_q)^{ur}\). Then by Lemma 5.1 (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 \(x \in \mathbb{P}^1(K'_q)\) 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 \(F(x)\). We fix an embedding \(\overline{K} \hookrightarrow \overline{K}_q\) and view \(\alpha_i\) as elements in \(\overline{K}_q\). Without loss of generality, we may assume that \(\alpha_1 \in K_q\) 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 \(x \in \mathbb{P}^1(K'_q)\) such that
\[
(6.1) \quad \sigma(x) = x, \quad (\tau(x) - \alpha_1)(x - \alpha_1) = (\alpha_2 - \alpha_1)(\alpha_3 - \alpha_1).
\]
The right hand side is the image of $\alpha_1 - \alpha_2$ under the norm map $K_q^* \to \mathbb{Q}_q^*$, hence has even valuation. Thus $\beta = \sqrt{(\alpha_2 - \alpha_1)(\alpha_3 - \alpha_1)}$ lies in $K_q$ and $x = \alpha_1 + \beta$ satisfies (6.1). It follows that $Q_q(c) = 0$.

Similarly, $Q_q(c') = 0$ if and only if there exists $x \in \mathbb{P}^1(K_q^{ur})$ such that
\[
(\sigma(x) - \alpha_1)(x - \alpha_1) = (\alpha_2 - \alpha_1)(\alpha_3 - \alpha_1).
\]
Taking the solution $x = \alpha_2 \in K_q^*$ we see that $Q_q(c') = 0$. Hence $\mathcal{L}_q(A)$ is maximal totally isotropic for $Q_v$.

Remark 6.6. 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 4.4).

7. Parity of 2-Selmer ranks

Now we are ready to prove the parity conjecture 4.3 on the 2-Selmer ranks.

Theorem 7.1. Assume Assumption 2.1 and 4.1. Suppose $\text{Frob}_q \in G_{\mathbb{Q}_q}$ has order 2 acting on $V$. Then
\[
s_2(E/K) = s_2(A/K) \pm 1.
\]
Moreover,
\[
s_2(E/K) = s_2(A/K) - 1
\]
if and only if $\text{res}_q(\text{Sel}_2(E/K) \otimes k) \subseteq H^1_{ur}(K_q, W)$, where $W$ is the unique $G_{\mathbb{Q}_q}$-stable line in $V$.

Proof. Define the strict local conditions $S$ by $S_v = \mathcal{L}_v(E) = \mathcal{L}_v(A)$ for $v \neq q$ and
\[
S_q = \mathcal{L}_v(E) \cap \mathcal{L}_v(A) = H^1_{ur}(K_q, W)
\]
(the second equality is by Lemma 5.1). 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 $\mathcal{R}_q = S_q^{\perp}$. Then we have
\[
H^1_S(V) \subseteq H^1_L(E)(V) \subseteq H^1_R(V), \quad H^1_S(V) \subseteq H^1_L(A)(V) \subseteq H^1_R(V).
\]
Since $S^{\perp} = \mathcal{R}$, we use [DDT97, Theorem 2.18] to compare the dual Selmer groups:
\[
\frac{\#H^1_S(V)}{\#H^1_R(V)} = \prod_v \frac{\#S_v}{\#H^0(K_v, V)}, \quad \frac{\#H^1_L(V)}{\#H^1_S(V)} = \prod_v \frac{\#R_v}{\#H^0(K_v, V)}.
\]
It follows that
\[
\dim H^1_R(V) - \dim H^1_S(V) = \frac{1}{2}(\dim \mathcal{R}_q - \dim S_q) = 1,
\]
since $S_q$ is 1-dimensional and $\mathcal{R}_q$ is 3-dimensional. By global class field theory, for any class $c \in H^1_R(V)$, we have
\[
\sum_v Q_v(\text{res}_v(c)) = 0.
\]
Since $\mathcal{R}_v$ is totally isotropic for $Q_v$ for any $v \neq q$ by Remark 6.4, we know that $Q_q(\text{res}_q(c)) = 0$.

In other words, the image $\text{res}_q(H^1_R(V))$ is also a totally isotropic subspace for $Q_q$. It follows that the quotient space $(\text{res}_q(H^1_R(V)) + S_q)/S_q$ is a nonzero totally isotropic subspace of $\mathcal{R}_q/S_q$ under (the quadratic form induced by) $Q_q$.

Since $\mathcal{R}_q/S_q$ is a 2-dimensional quadratic space obtained by extending scalars from a 2-dimensional quadratic space over $\mathbb{F}_2$ and $\mathcal{R}_q/S_q$ 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 6.3, 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 6.4 and Lemma 6.5, namely \( \mathcal{L}_q(E) \) and \( \mathcal{L}_q(A) \). It follows that either \( H^1_R(V) = H^1_{L(E)}(V) \) or \( H^1_R(V) = H^1_{L(A)}(V) \). The two cases cannot hold simultaneously since

\[
H^1_{L(A)}(V) \cap H^1_{L(E)}(V) = H^1_S(V) \subseteq H^1_R(V).
\]

So either

\[
H^1_{L(A)}(V) = H^1_R(V), \quad H^1_{L(E)}(V) = H^1_S(V),
\]

or

\[
H^1_{L(E)}(V) = H^1_R(V), \quad H^1_{L(A)}(V) = H^1_S(V).
\]

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

**Remark 7.2.** The conclusion of Theorem 7.1 may fail when Assumption 2.1 (4) is not satisfied 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 \( \hat{\rho}|_{G_{Q_2}} \). The elliptic curve

\[ A = 25861a1 : y^2 + xy + y = x^3 + x^2 - 17x + 30 \]

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

\[ r_{\text{alg}}(E/K) = s_2(E/K) = 1 \quad \text{and} \quad r_{\text{alg}}(A/K) = s_2(A/K) = 4 \]

differ by 3 (rather than 1).

8. OBSTRUCTION FOR RANK LOWERING

It follows from Theorem 7.1 that if \( s_2(E/K) = 1 \), then \( s_2(A/K) = 0 \) or 2. However, the Chebotarev density argument for \( p \geq 5 \) in [Zha14] fails in this case and does not show that one can always get \( s_2(A/K) = 0 \). In fact, we prove the following very surprising obstruction for rank lowering: \( s_2(A/K) \) can never be lowered to zero!

**Theorem 8.1.** Assume Assumption 2.1 and 4.1. Suppose \( \text{Frob}_q \in G_{Q_2} \) has order 2 acting on \( V \). Then

\[ s_2(E/K) = 1 \iff s_2(A/K) = 2. \]

**Proof.** By Theorem 7.1, we need to show that \( \text{res}_q(\text{Sel}_2(E/K) \otimes k) \subseteq H^1_{\text{ur}}(K_q, W) \), where \( W \) is the unique \( G_{Q_2} \)-stable line in \( V \). By definition, the Galois group \( \text{Gal}(K/Q) \) acts on \( \text{Sel}_2(E/K) \). By assumption, we have \( \text{Sel}_2(E/K) \cong \mathbb{Z}/2\mathbb{Z} \). So the action of \( \text{Gal}(K/Q) \) on \( \text{Sel}_2(E/K) \) must be trivial. It follows that

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

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

We end with an example illustrating Theorem 8.1.

**Example 8.2.** Consider \( E = X_0(11) \). 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 $r_{\text{alg}}(A/K) = 2$. In the remaining cases, there is a jump coming from the 2-part

<table>
<thead>
<tr>
<th>$q$</th>
<th>$A$</th>
<th>$d_K$</th>
<th>$r_{\text{alg}}(A/K)$</th>
<th>$\dim(\Sha(A/K))[2]$</th>
<th>$s_2(A/K)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>77a</td>
<td>$-8$</td>
<td>2</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>7</td>
<td>77b</td>
<td>$-8$</td>
<td>0</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>13</td>
<td>143a</td>
<td>$-7$</td>
<td>2</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>13</td>
<td>143a</td>
<td>$-8$</td>
<td>2</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>17</td>
<td>187a</td>
<td>$-7$</td>
<td>2</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>17</td>
<td>187a</td>
<td>$-24$</td>
<td>0</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>19</td>
<td>209a</td>
<td>$-7$</td>
<td>2</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>19</td>
<td>209a</td>
<td>$-19$</td>
<td>2</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>29</td>
<td>319a</td>
<td>$-8$</td>
<td>2</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>29</td>
<td>319a</td>
<td>$-19$</td>
<td>0</td>
<td>2</td>
<td>2</td>
</tr>
</tbody>
</table>

Table 2. Obstruction for rank lowering

of III for the base change $A/K$,

$$\dim(\Sha(A/K))[2] = 2,$$

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

$$\Sha(A/Q)[2] = 0, \quad \Sha(A^K/Q)[2] = 0.$$

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

$$\Sha(A/K)[p] = \Sha(A/Q)[p] \oplus \Sha(A^K/Q)[p].$$

REFERENCES


E-mail address: chaoli@math.harvard.edu

Department of Mathematics, Harvard University, 1 Oxford Street, Cambridge, MA 02138