# RANKS OF ABELIAN VARIETIES OVER INFINITE EXTENSIONS OF THE RATIONALS

ÁLVARO LOZANO-ROBLEDO

Abstract. Let $S$ be an infinite set of rational primes and, for some $p \in S$, let $\mathbb{Q}_S^{(p)}$ be the compositum of all extensions unramified outside $S$ of the form $\mathbb{Q}(\mu_p, \sqrt[p]{d})$, for $d \in \mathbb{Q}^\times$. If $(\sigma) = (\sigma_1, \dots, \sigma_n) \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})^n$, let $(\mathbb{Q}_S^{(p)})^{(\sigma)}$ be the intersection of the fixed fields by $\langle \sigma_i \rangle$, for $i = 1, \dots, n$. We provide a wide family of elliptic curves $E/\mathbb{Q}$ such that the rank of $E((\mathbb{Q}_S^{(p)})^{(\sigma)})$ is infinite for all $n \geq 0$ and all $(\sigma) \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})^n$, subject to the parity conjecture.

Similarly, let $(A/\mathbb{Q}, \phi)$ be a polarized abelian variety, let $K$ be a quadratic number field fixed by $(\sigma) \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})^n$, let $S$ be an infinite set of primes of $\mathbb{Q}$ and let $K_S^{p\text{-dihe}}$ be the maximal abelian $p$-elementary extension of $K$ unramified outside primes of $K$ lying over $S$ and dihedral over $\mathbb{Q}$. We show that, under certain hypotheses, the $\mathbb{Z}_p$-corank of $\mathrm{Sel}_{p^\infty}(A/F)$ is unbounded over finite extensions $F/K$ contained in $(K_S^{p\text{-dihe}})^{(\sigma)}/K$.

As a consequence, we prove a strengthened version of a conjecture of M. Larsen in a large number of cases.

## 1. Introduction

Let $A$ be an abelian variety defined over $\mathbb{Q}$, let $\overline{\mathbb{Q}}$ be a fixed algebraic closure, let $\mathbb{Q}^{ab}$ be the maximal abelian extension of $\mathbb{Q}$ and let $L/\mathbb{Q}$ be an extension with $L \subseteq \overline{\mathbb{Q}}$. If $L/\mathbb{Q}$ is finite then the group of $L$-rational points of $A$, denoted as usual by $A(L)$, is finitely generated by the Mordell-Weil Theorem. On the other hand, $A(\overline{\mathbb{Q}})$ has an infinite free rank (see [5] for example). These two facts prompt the following:

**Question 1.1.** *For what infinite extensions $L/\mathbb{Q}$ is $A(L)$ of infinite rank?*

The torsion subgroup of $A(\mathbb{Q}^{ab})$ is finite for any abelian variety $A/\mathbb{Q}$ (this is a theorem due to K. Ribet [21]). Y. G. Zarhin ([30], see also [27]) has also shown that if $K$ is a number field then the torsion subgroup of $A(K^{ab})$ is finite if and only if $A$ has no abelian subvariety with complex multiplication over $K$. An interesting consequence of the deep work of K. Kato ([10]) and D. Rohrlich ([23],[25]), together with Ribet's theorem, provides some information about the question above:

**Theorem 1.2.** *(Kato, Ribet, Rohrlich) Let $E/\mathbb{Q}$ be an elliptic curve, let $\Sigma$ be a finite set of primes of $\mathbb{Z}$ and let $\mathbb{Q}_\Sigma^{ab}$ be the maximal abelian extension of $\mathbb{Q}$ unramified outside $\Sigma$. Then $E(\mathbb{Q}_\Sigma^{ab})$ is finitely generated.*

See also [15] for B. Mazur's similar results of finite generation of the Mordell-Weil group in $\mathbb{Z}_p$-extensions of number fields. For recent progress and results of infinite generation in the non-abelian setting, see [1], [26] and [14].

In the rest of this article, $S$ will denote an infinite set of primes of $\mathbb{Z}$, while $\Sigma$ is reserved for finite sets of primes. The symbol $\mathbb{Q}_S^{ab}$ (resp. $\overline{\mathbb{Q}}_S$) stands for the maximal abelian extension (resp. maximal extension) of $\mathbb{Q}$ unramified outside $S$ and contained in $\overline{\mathbb{Q}}$. For a prime $p \geq 2$, we will write $\mu_p \subset \overline{\mathbb{Q}}$ for the group of all $p$th roots of unity and we define $\mathbb{Q}_S^{(p)}$ as the compositum of all extensions of $\mathbb{Q}$ of the form $\mathbb{Q}(\mu_p, \sqrt[p]{d})$, for some $d \in \mathbb{Q}^\times$, and unramified outside $S$. We note $\mathbb{Q}_S^{(p)}/\mathbb{Q}$ is Galois for all $p$ but non-abelian for $p > 2$. If $(\sigma) = (\sigma_1, \ldots, \sigma_n) \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})^n$ and $F \subset \overline{\mathbb{Q}}$ is a field then the symbol $F^{(\sigma)}$ stands for the intersection of all fixed fields $F^{\langle \sigma_i \rangle}$, for $i = 1, \ldots, n$, where $\langle \sigma_i \rangle$ is the subgroup generated by $\sigma_i$. As we discussed above, the torsion subgroup of $E(\mathbb{Q}_S^{(p)})$ is finite, for all primes $p$, thus the torsion of $E((\mathbb{Q}_S^{(p)})^{(\sigma)})$ is also finite for all $(\sigma) \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})^n$. Our first theorem is:

**Theorem 1.3.** *Let $E/\mathbb{Q}$ be an elliptic curve and let $S$ be an infinite set of primes.*

(1) *Suppose that $\mathrm{rank}_{\mathbb{Z}}(E(\mathbb{Q}))$ is odd. If the parity conjecture holds for all quadratic twists of $E$ then the rank of $E((\mathbb{Q}_S^{(2)})^{(\sigma)})$ is infinite, for all $n \geq 0$ and all $(\sigma) \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})^n$. Hence $\mathrm{rank}_{\mathbb{Z}}(E((\mathbb{Q}_S^{ab})^{(\sigma)}))$ is infinite as well.*

(2) *Suppose $E/\mathbb{Q}$ does not have wild ramification at 2 and 3. There are infinitely many primes $p > 2$ such that if the parity conjecture holds for $E$ over extensions of degree $p$ and we set $S' = S \cup \{p\}$ then the rank of $E((\mathbb{Q}_{S'}^{(p)})^{(\sigma)})$ is infinite, for all $n \geq 0$ and all $(\sigma) \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})^n$.*

*In particular, if the hypotheses of (1) or (2) are satisfied, then the rank of $E(\overline{\mathbb{Q}}_S^{(\sigma)})$ is infinite.*

The previous statements are a combination of Theorem 5.3 and Corollary 6.4 below. In most cases, there is a choice of prime $p$ of (2) with $p \in S$. We offer a concrete example in the last section of the article.

If $A$ is an abelian variety defined over a number field $F$ and $p$ is a prime then $\mathrm{Sel}_{p^\infty}(A/F)$ is the usual Selmer group sitting in an exact sequence:

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

where $Ш(A/F)[p^\infty]$ denotes the torsion elements of $p$-power order in the Tate-Shafarevich group of $A/F$. The Tate-Shafarevich conjecture (i.e. the group $Ш(A/F)$ is finite) implies that the rank of $A(F)$ and the corank of $\mathrm{Sel}_{p^\infty}(A/F)$ coincide. As a consequence of parity for Selmer groups (recently shown by J. Nekovář and B-D. Kim, see Theorem 5.2 below) and the methods used to prove Theorem 1.3 we obtain:

**Theorem 1.4.** *Let $E/\mathbb{Q}$ be an elliptic curve and let $S$ be an infinite set of primes. Suppose that the root number of $E/\mathbb{Q}$ is $W(E/\mathbb{Q}) = -1$ and let $p > 2$ be a prime of good reduction for $E/\mathbb{Q}$. Then the $\mathbb{Z}_p$-corank of $\mathrm{Sel}_{p^\infty}(E/F)$ is unbounded over number fields $F$ contained in $((\mathbb{Q}_S^{(2)})^{(\sigma)})$, for all $n \geq 0$ and all $(\sigma) \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})^n$. In particular, if the $p$-primary part of $\text{Ш}(E^d/\mathbb{Q})$ is finite, for all square-free $d \in \mathbb{Q}^\times$, then the rank of $E((\mathbb{Q}_S^{(2)})^{(\sigma)})$ is infinite.*

See Section 5.1 for a proof. If $K$ is a quadratic extension of $\mathbb{Q}$, the symbol $K_S^{p\text{-dihe}}$ stands for the maximal abelian $p$-elementary extension of $K$ unramified outside $S$ and dihedral over $\mathbb{Q}$:

**Theorem 1.5.** *Let $(A/\mathbb{Q}, \phi)$ be a polarized abelian variety, let $n \geq 0$ and let $(\sigma) \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})^n$ be fixed. Suppose there is a quadratic extension $K/\mathbb{Q}$, fixed by $(\sigma)$, such that $\mathrm{corank}_{\mathbb{Z}_p} \mathrm{Sel}_{p^\infty}(A/K)$ is odd, for some prime $p > 2$ which splits in $K$ and such that $\gcd(p, \deg(\phi)) = 1$. Let $S$ be an infinite set of rational primes which does not include any of the primes of bad reduction for $A/\mathbb{Q}$, and such that $S$ contains infinitely many primes either inert in $K$ and congruent to $-1 \mod p$, or split in $K$ and congruent to $1 \mod p$ . Then the corank of $\mathrm{Sel}_{p^\infty}(A/F)$ is unbounded over finite extensions $F/K$ contained in the field $(K_S^{p\text{-dihe}})^{(\sigma)}$.*

Theorems 1.3, 1.4 and 1.5 may be regarded as a partial complement to Theorem 1.2 and also as a strengthened version of the following conjecture of M. Larsen:

**Conjecture 1.6** (Larsen, [13])**.** *Let $A/\mathbb{Q}$ be an abelian variety. Then $A(\overline{\mathbb{Q}}^{(\sigma)})$ is of infinite rank for all $n \geq 0$ and all $(\sigma) \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})^n$.*

G. Frey and M. Jarden have shown (see [5]) that there is a subset $H$ of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ of Haar measure 1 such that $A(\overline{\mathbb{Q}}^{(\sigma)})$ is of infinite rank for all $(\sigma) \in H^n$, thus Larsen's conjecture claims that $H$ is equal in fact to all of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. B-H. Im and Larsen have shown that the conjecture holds true for $n = 1$ (see [8]). As a consequence of Theorems 1.3 (resp. Thm. 1.5), if we assume the parity conjecture (resp. if the $p$-primary parts of the Tate-Shafarevich groups $\text{Ш}(A/F)$ are finite), then Larsen's conjecture holds true for a wide class of elliptic curves and all $n \geq 0$. In view of Theorem 1.3, it seems very plausible that the following is also true:

**Conjecture 1.7.** *Let $S$ be an infinite set of primes and let $A/\mathbb{Q}$ be an abelian variety. Then $\mathrm{rank}_{\mathbb{Z}}(A((\mathbb{Q}_S^{ab})^{(\sigma)}))$ is infinite, for all $n \geq 0$ and all $(\sigma) \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})^n$.*

A few remarks are in order:

**Remark 1.8.** The proof of Theorem 1.3 relies heavily on recent deep results of Mazur and K. Rubin (see [16]). Part (1) of Theorem 1.3 (see Thm. 5.3) is shown by extending a method used in [9], and the proof should generalize to abelian varieties in the obvious way (and thus providing more evidence towards Conjecture 1.7). Moreover, if $E(\mathbb{Q})$ is of even rank then one can find infinitely many twists $E^d/\mathbb{Q}$ of odd rank and apply Theorem 1.3 (or similarly apply Theorem 1.5) to show that there is infinitely many open subgroups $H$ of index 2 in $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ such that for all $n \geq 0$ and all $(\sigma) \in H^n$ the rank of $E((\mathbb{Q}_S^{(2)})^{(\sigma)})$ is infinite.

**Remark 1.9.** The proof of part (2) of Thm. 1.3 (see Cor. 6.4) relies on recent results of V. Dokchitser in [3]. The condition on the wild ramification does not seem essential but rather a simplification, for the local root numbers in characteristic 2 and 3 are much harder to calculate in the presence of wild ramification (see [4] for results on the calculation of such root numbers).

**Remark 1.10.** From now on, for a field $F$, let $G_F = \mathrm{Gal}(\overline{F}/F)$. It is worth remarking that the class of fields $\mathcal{S} = \{(\mathbb{Q}_S^{(p)})^{(\sigma)} : S \text{ infinite},\ n \geq 0,\ (\sigma) \in G_{\mathbb{Q}}^n\}$ is much larger than the class of fields $\mathcal{F} = \{(\mathbb{Q}^{(p)})^{(\sigma')} : m \geq 0,\ (\sigma') \in G_{\mathbb{Q}}^m\}$. The inclusion $\mathcal{F} \subset \mathcal{S}$ is clear, by setting $S$ to be the set of all rational primes. To show that the inclusion is not an equality, we show choices (for any $m \geq 0$) of $S$, $\sigma'$ such that $(\mathbb{Q}^{(p)})^{(\sigma')}$ is not contained in $(\mathbb{Q}_S^{(p)})^{(\sigma)}$, for any choice of $\sigma$. Let $S$ be an infinite set of primes with a complement, i.e. there is $q$ prime and $q \notin S$. Pick $(\sigma')$ fixing $\alpha = \sqrt[p]{dq}$ for some $d \in \mathbb{Z}$ such that $dq$ is $p$-power free, then $\mathbb{Q}(\alpha) \subset (\mathbb{Q}^{(p)})^{(\sigma')}$ but $\mathbb{Q}(\alpha)/\mathbb{Q}$ is ramified at $q \notin S$ and so $\mathbb{Q}(\alpha) \not\subseteq (\mathbb{Q}_S^{(p)})^{(\sigma)}$ for any choice of $(\sigma)$.

**Remark 1.11.** After finishing this work, it has been brought to my attention that, in an independent project ([19]), S. Petersen has shown that if $A/\mathbb{Q}$ is an abelian variety and $W(A(\mathbb{Q})) = -1$ then the rank of $A((\mathbb{Q}^{(2)})^{(\sigma)})$ is infinite, assuming that the parity conjecture holds. The key difference with Theorem 1.3 above is that our method allows controlled ramification outside any fixed infinite set of primes $S$, and provides results for $\mathbb{Q}_S^{(p)}$ for $p > 2$.

## 2. A Further Remark on "Large" Fields

In this section we explain how Theorem 1.3 may also be interpreted as further evidence towards a conjecture which claims that $\mathbb{Q}^{ab}$ is a large field, in the sense of F. Pop (see [20]), and perhaps as evidence that $(\mathbb{Q}_S^{ab})^{(\sigma)}$ is large too, for any infinite set of primes $S$, and any $n \geq 0$, $\sigma \in G_{\mathbb{Q}}^n$. A field $F$ is large if any smooth curve $C/F$ with one $F$-rational point has necessarily infinitely many $F$-rational points. The connection with our problem is the following proposition (due to A. Tamagawa):

**Proposition 2.1** ([12], Prop. 1)**.** *Let $F$ be a large field (in the sense of Pop) of characteristic zero and let $E/F$ be an elliptic curve. Then* $\mathrm{rank}_{\mathbb{Z}}(E(F))$ *is infinite.*

As a consequence of Theorem 1.2 and Tamagawa's proposition, the field $\mathbb{Q}_\Sigma^{ab}$ is not large, for any finite set of primes $\Sigma$. On the contrary, Theorem 1.3 (or Conjecture 1.7 if it holds) may be seen as evidence that $(\mathbb{Q}_S^{ab})^{(\sigma)}$ is large, for any $S$ and $(\sigma)$ as before.

## 3. Strategy

In this section we establish the strategy for the proof of the main theorem. Namely, Theorem 3.3 below will show that if an abelian variety $A/\mathbb{Q}$ satisfies a certain property $(T^n_{S,p})$ then the rank of $A((\mathbb{Q}_S^{(p)})^{(\sigma)})$ is infinite for all $(\sigma) \in G^n_{\mathbb{Q}}$.

**Lemma 3.1.** *Let $n \geq 0, t \geq 1$ be integers, let $p \geq 2$ be a prime and let $a_1, \dots, a_t$ be elements in a number field $K$. Let*

$$L = K(\mu_p, \sqrt[p]{a_1}, \dots, \sqrt[p]{a_t})$$

*be a number field with $[L : K] = (p-1) \cdot p^t$, and let $\sigma = (\sigma_1, \dots, \sigma_n)$ be an $n$-tuple in $G^n_K$. If $t \geq n+1$ then there is at least one extension $K'/K$ of degree $p$ with $K \subset K' \subset L \cap \overline{K}^{(\sigma)}$ with $K' = K(\sqrt[p]{c})$, $c \neq 1$ and*

$$c = \prod_{j=1}^{t} (a_j)^{e_j}, \quad e_j = 0, 1, \dots, p-1. \tag{1}$$

*Proof.* The case $n = 0$ is trivial. Let $n \geq 1$ be an integer, let $p \geq 2$ be prime and let $L/K$ and $(\sigma) \in G^n_K$ be as in the statement of the lemma. As an immediate consequence of the hypotheses, $L/K$ is Galois and $L/K(\mu_p)$ is $p$-elementary abelian. In particular, the order of each $\gamma \in G = \mathrm{Gal}(L/K)$ divides $(p-1)p$ and the order of a subgroup $\langle \gamma_1, \dots, \gamma_m \rangle \leq G$ divides the number $(p-1)p^m$. In particular, let $\gamma_i$ be the restriction of $\sigma_i$ to $L$ and let $H$ be the subgroup generated by $\gamma_i$, for $i = 1, \dots, n$. Thus $p^{t-n}$ divides $|G|/|H|$ and, since $t \geq n+1$, $p$ divides $|G|/|H|$. Let $L^H$ be the fixed field of $L$ by $H$. Then $p$ divides the degree of the abelian extension $L^H(\mu_p)/K(\mu_p)$. Let $F/K(\mu_p)$ be a subextension of degree $p$ contained in $L^H(\mu_p)/K(\mu_p)$. Then $F = K(\mu_p, \sqrt[p]{c})$ for some $c$ as in Eq. (1), because a simple counting argument, and Kummer theory, shows that all degree $p$ extensions of $K(\mu_p)$ inside $L$ are of this form. Hence $K' = K(\sqrt[p]{c}) \subseteq L^H(\mu_p)$ and so there is a $p$th root of unity $\zeta$ such that $K'' = K(\zeta \sqrt[p]{c}) \subseteq L^H$, and since $\zeta \sqrt[p]{c}$ is another $p$th root of $c$ we may call it $\sqrt[p]{c}$. Thus $K' = K(\sqrt[p]{c})/K$ is fixed by $(\sigma)$. □ □

**Definition 3.2.** *Let $S$ be an infinite set of primes of $\mathbb{Z}$. Let $n$ be a non-negative integer and let $p \geq 2$ be a prime. We say that an abelian variety $A/\mathbb{Q}$ satisfies property $(T^n_{S,p})$ if for all $i \geq 1$ there exist $D_i = (d_{i,1}, \dots, d_{i,n+1}) \in (\mathbb{Q}^\times)^{n+1}$ such that:*

1. *Put $L_0 = \mathbb{Q}(\mu_p)$ and define $L_i = L_{i-1}(\{\sqrt[p]{d_{i,j}} : j = 1, \dots, n+1\})$ for all $i \geq 1$. Then $[L_i : L_{i-1}] = p^{n+1}$;*
2. *For all $i, j \geq 1$, the numbers $d_{i,j}$ are only divisible by primes in $S$. Consequently, the fields $L_i$ of (1) are unramified outside $S \cup \{p\}$;*
3. *For all $i \geq 1$ and $d \in \mathbb{Q}^\times$ of the form*

$$d = \prod_{j=1}^{n+1} (d_{i,j})^{e_j} \quad \text{with } e_j = 0, \dots, p-1$$

*the rank of $A(\mathbb{Q}(\sqrt[p]{d}))$ is strictly greater than that of $A(\mathbb{Q})$.*

As before, if $S$ is a set of primes of $\mathbb{Z}$, the symbol $\mathbb{Q}_S^{ab}$ is the maximal abelian extension unramified outside $S$ and $\mathbb{Q}_S^{(p)}$ is the compositum of all extensions of $\mathbb{Q}$ unramified outside $S$ and of the form $\mathbb{Q}(\mu_p, \sqrt[p]{d})$, for some $d \in \mathbb{Q}^\times$.

**Theorem 3.3.** *Let $n \geq 0$ be a fixed integer, let $S \cup \{p\}$ be an infinite set of primes of $\mathbb{Z}$ and let $A/\mathbb{Q}$ be an abelian variety satisfying the property $(T^n_{S,p})$. Further, assume that $A$ has no abelian subvariety with complex multiplication defined over $\mathbb{Q}(\mu_p)$. Then for each $(\sigma) = (\sigma_1, \ldots, \sigma_n) \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})^n$, the rank of $A((\mathbb{Q}_S^{(p)})^{(\sigma)})$ is infinite.*

*Proof.* Let $n \geq 0$, $p$ and $S$ be as in the statement and suppose $A/\mathbb{Q}$ satisfies property $(T^n_{S,p})$. Let $D_i$, $i \geq 1$, be the elements of $(\mathbb{Q}^\times)^{n+1}$ satisfying (1), (2) and (3) as in Definition 3.2. Fix an element $(\sigma) \in G^n_{\mathbb{Q}}$. We will inductively construct extensions $K_m/K$ of degree $p$ for all $m \geq 1$, unramified outside $S$, fixed by $(\sigma)$, and points $P_m \in A$ strictly defined over $K_m$ (and not just over $\mathbb{Q}$) as follows.

Let $L_i$, $i \geq 0$, be defined as in (1) of Defn. 3.2. Then $L_1/\mathbb{Q}$ is an extension of degree $(p-1)p^{n+1}$, unramified outside $S$. By Lemma 3.1, there exists a extension $K_1/\mathbb{Q}$ of degree $p$, contained in $L_1$ (and therefore unramified outside $S$), such that $K_1 \subset (\mathbb{Q}_S^{(p)})^{(\sigma)}$. Moreover $K_1 = \mathbb{Q}(\sqrt[p]{d})$ for some $d \in \mathbb{Q}^\times$

$$d = \prod_{j=1}^{n+1} (d_{1,j})^{e_j} \quad \text{with } e_j = 0, \ldots, p-1$$

and, by (3) of Def. 3.2, $A(K_1)$ is of rank greater than the rank of $A(\mathbb{Q})$. Hence $A(K_1)$ contains a point of infinite order $P_1$, strictly defined over $K_1$.

We complete the proof by induction on $m$. Suppose that for $i = 1, \ldots, m$, we have chosen extensions $K_i/\mathbb{Q}$ of degree $p$ unramified outside $S$, with $K_i \subset L_i$ and independent points $P_i \in A(K_i)$ of infinite order, strictly defined over $K_i$. Since $L_{m+1}/L_m$ is an extension of degree $p^{n+1}$, we also have $\mathbb{Q}(\{\sqrt[p]{d_{m+1,j}} : j = 1, \ldots, n+1\})/\mathbb{Q}$ is of degree $p^{n+1}$. By Lemma 3.1, there exists an extension $K_{t+1}/\mathbb{Q}$ of degree $p$, contained in $L_{m+1}$ (and therefore unramified outside $S$), and $K_{m+1} \subset (\mathbb{Q}_S^{(p)})^{(\sigma)}$. As before, $K_{m+1} = \mathbb{Q}(\sqrt[p]{d})$ for some $d \in \mathbb{Q}^\times$

$$d = \prod_{j=1}^{n+1} (d_{m+1,j})^{e_j} \quad \text{with } e_j = 0, \ldots, p-1$$

and, by (3) of Def. 3.2, $A(K_{m+1})$ contains a point of infinite order $P_{m+1}$, strictly defined over $K_{m+1}$. Notice that in fact $K_{m+1}$ is not contained in $L_m$ and therefore $K_{m+1} \neq K_i$ for all $i = 1, \ldots, m$. Hence $P_{m+1}$ is necessarily independent from the group generated by $P_1, \ldots, P_m$. By assumption, $A$ has no abelian subvarieties with complex multiplication defined over $\mathbb{Q}(\mu_p)$, thus by

Zarhin's theorem ([30], [27]), the torsion subgroup of $A(\mathbb{Q}_S^{(p)}) \subset A(\mathbb{Q}(\mu_p)^{ab})$ is finite. Hence, one can extract out of $\{P_i\}_{i=1}^{\infty}$ an infinite sequence of points of $A$ defined over $(\mathbb{Q}_S^{(p)})^{(\sigma)}$ which are independent modulo torsion. This concludes the proof of the theorem. □ □

## 4. Background on Twists and Root Numbers

In this section we provide a number of well-known results on twists of elliptic curves, which will be used in subsequent proofs. If $d \in \mathbb{Q}^{\times}$ is a square-free rational number, the symbol $E^d$ stands for the quadratic twist of the elliptic curve $E/\mathbb{Q}$ by $d$. Let $N_E$ be the conductor of $E$ and let $W(E/\mathbb{Q})$ be the global root number (or $W(E)$ if the field of definition is clear from the context), i.e., the sign in the functional equation for $L(E/\mathbb{Q}, s)$. We will write $W(E, d)$ for $W(E^d)$.

**Lemma 4.1** ([22]; cf. [3], Corollary 2)**.** *Suppose $E$ is an elliptic curve over $\mathbb{Q}$, let $N_E$ be the conductor of $E/\mathbb{Q}$ and let $d \in \mathbb{Z}$ be a fundamental discriminant (i.e. either $d \equiv 1 \mod 4$ or $d = 4d'$ with $d' \equiv 2, 3 \mod 4$, and $d, d'$ square-free).*

(1) *If $\gcd(N_E, d) = 1$ then $W(E, d) = \left(\frac{d}{-N_E}\right) \cdot W(E)$ where $\left(\frac{\cdot}{\cdot}\right)$ is the Kronecker symbol.*
(2) *If $d, d'$ are fundamental discriminants, relatively prime to $N_E$ and to each other, then $W(E, dd') = W(E, d) \cdot W(E, d') \cdot W(E)$.*

**Lemma 4.2** ([29], X.§5)**.** *Let $d \in \mathbb{Q}^{\times}$ be a square free integer, $K = \mathbb{Q}(\sqrt{d})$, let $E/\mathbb{Q}$ be an elliptic curve and let $p > 2$ be a prime of good reduction. Then:*

$$\begin{aligned} \operatorname{rank}_{\mathbb{Z}}(E(K)) &= \operatorname{rank}_{\mathbb{Z}}(E(\mathbb{Q})) + \operatorname{rank}_{\mathbb{Z}}(E^d(\mathbb{Q})) \\ \operatorname{corank}_{\mathbb{Z}_p} \operatorname{Sel}_{p^\infty}(E/K) &= \operatorname{corank}_{\mathbb{Z}_p} \operatorname{Sel}_{p^\infty}(E/\mathbb{Q}) + \operatorname{corank}_{\mathbb{Z}_p} \operatorname{Sel}_{p^\infty}(E^d/\mathbb{Q}). \end{aligned}$$

*Proof.* There exists an isomorphism $\psi : E^d \to E$ defined over $K$ and a homomorphism $\mathrm{Tr} : E(K) \to E(\mathbb{Q})$ induced by the trace from $K$ down to $\mathbb{Q}$. The image of the trace map contains $2E(\mathbb{Q})$ and its kernel is precisely $\psi(E^d(\mathbb{Q}))$. A similar argument, replacing $E(\mathbb{Q})$ by $\operatorname{Sel}_{p^\infty}(E/\mathbb{Q})$, shows the equality of coranks. □ □

## 5. The Compositum of All Quadratic Extensions

Here we study some cases of elliptic curves over $\mathbb{Q}_S^{(2)} \subset \mathbb{Q}_S^{ab}$, subject to the parity conjecture, and we provide a proof of part (1) of Theorem 1.3.

**Conjecture 5.1** (Parity Conjecture)**.** *Let $K$ be a number field, let $E/K$ be an elliptic curve and let $W(E/K)$ be the root number of $E/K$. Then $W(E/K) = (-1)^{\operatorname{rank}_{\mathbb{Z}}(E(K))}$.*

J. Nekovář and B-D. Kim have shown the parity conjecture for Selmer groups over $\mathbb{Q}$:

**Theorem 5.2** ([18], [11]). *Let $E/\mathbb{Q}$ be an elliptic curve and let $p > 2$ be a prime of good reduction for $E$. Then*

$$\operatorname{corank}_{\mathbb{Z}_p} \operatorname{Sel}_{p^\infty}(E/\mathbb{Q}) \equiv \operatorname{ord}_{s=1} L(E/\mathbb{Q}, s) \mod 2.$$

*Equivalently, $W(E/\mathbb{Q}) = (-1)^{\operatorname{corank}_{\mathbb{Z}_p} \operatorname{Sel}_{p^\infty}(E/\mathbb{Q})}$.*

**Theorem 5.3.** *Let $E/\mathbb{Q}$ be an elliptic curve with $\operatorname{rank}_{\mathbb{Z}}(E(\mathbb{Q}))$ odd and let $S$ be an infinite set of primes. If the parity conjecture holds for all quadratic twists of $E$ then the rank of $E((\mathbb{Q}_S^{(2)})^{(\sigma)})$ is infinite, for all $n \geq 0$ and all $(\sigma) \in \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})^n$.*

*Proof.* By Theorem 3.3, it suffices to show that $E/\mathbb{Q}$ satisfies property $(T^n_{S,2})$ for all $n \geq 0$. First, we show the existence of a set $\mathcal{D}$ formed by infinitely many fundamental discriminants $d_i \in \mathbb{Z}$ one for each $i \geq 1$, divisible only by primes in $S$ and such that:

(1) $d_i$ and $d_j$ are relatively prime, for $i \neq j$;
(2) $\left(\frac{d_i}{-N_E}\right) = 1$, and so $W(E, d_i) = -1$, for all $i \geq 1$.

We construct $\mathcal{D}$ by induction. Suppose that $d_1, d_2, \ldots, d_m$ have been chosen satisfying (1) and (2) above, for some $m \geq 0$. Let $S = \{p_1, p_2, \ldots\}$, with $0 < p_i < p_{i+1}$ and let $p_{i_1}, p_{i_2}$ be the two smallest primes in $S$ relatively prime to $2N_E \prod_{i=1}^m d_i$. For a prime $p > 2$ we will write:

$$d(p) = \begin{cases} p & , \text{ if } p \equiv 1 \mod 4; \\ -p & , \text{ if } -p \equiv 1 \mod 4. \end{cases}$$

If one of $d(p_{i_s})$, for $s = 1$ or $2$, is such that $\left(\frac{d(p_{i_s})}{-N_E}\right) = 1$ then define $d_{m+1} = d(p_{i_s})$, otherwise we set $d_{m+1} = d(p_{i_1})d(p_{i_2})$ so that, in both cases we have $\left(\frac{d_{m+1}}{-N_E}\right) = 1$, by the properties of the Kronecker symbol (note that $d_{m+1} \equiv 1 \mod 4$ and so $d_{m+1}$ is a fundamental discriminant).

Let us fix $n \geq 0$ and define $D_i = (d_{(n+1)(i-1)+1}, \ldots, d_{(n+1)i}) \in (\mathbb{Q}^\times)^{n+1}$ for all $i \geq 1$. We claim that these $D_i$ satisfy properties (1), (2) and (3) of Definition 3.2. For each $i \geq 1$, the fields $L_i$ are defined by

$$L_i = \mathbb{Q}(\{\sqrt{d_j} : 1 \leq j \leq (n+1) \cdot i\})$$

and since all the $d_i$'s are pairwise relatively prime by construction, none of the numbers in $C_i$:

$$C_i = \{d = \prod_{j=1}^{(n+1)i} (d_j)^{e_j} : e_j = 0, 1\}$$

can be a square of $\mathbb{Q}$. Thus $[L_i : \mathbb{Q}] = 2^{(n+1)i}$ and $[L_i : L_{i-1}] = 2^{n+1}$. Moreover, the $d_i's$ are only divisible by primes of $S$, thus $L_i/\mathbb{Q}$ is unramified outside $S$ (notice that since all $d_i \equiv 1 \mod 4$ the prime 2 does not ramify). This shows (1) and (2).

Finally, in order to show (3), let $d \in C_i$ with $d = d_{i_1} \cdots d_{i_k}$ for some distinct indices $i_1 < \ldots < i_k$. Since $E(\mathbb{Q})$ has odd rank, if the Parity Conjecture holds for $E/\mathbb{Q}$ then $W(E) = -1$, and if $d \in \mathbb{Z}$ is a fundamental discriminant (say $d \equiv 1 \mod 4$) relatively prime to $N_E$ then, by Lemma 4.1 the root number of $E^d/\mathbb{Q}$ is $W(E,d) = -\left(\frac{d}{-N_E}\right)$. Then

$$W(E,d) = -\left(\frac{d}{-N_E}\right) = -\left(\frac{d_{i_1}}{-N_E}\right)\cdots\left(\frac{d_{i_k}}{-N_E}\right) = -1.$$

If the Parity Conjecture holds for $E^d/\mathbb{Q}$, then $E^d/\mathbb{Q}$ is of positive rank and, by Lemma 4.2, $\mathrm{rank}_{\mathbb{Z}}(E(\sqrt{d})) > \mathrm{rank}_{\mathbb{Z}}(E(\mathbb{Q}))$. This shows (3) and the proof of the theorem is complete. □ □

5.1. **Proof of Theorem 1.4.** Let $E/\mathbb{Q}$ be an elliptic curve with $W(E) = -1$, let $S$ be an infinite set of rational primes, let $p > 2$ be a prime of good reduction for $E$ and let $(\sigma) \in G_Q^n$ be fixed. The proof of Theorem 5.3, combined with Lemma 3.1, show that there are infinitely many distinct quadratic fields $K_i = \mathbb{Q}(\sqrt{d_i})$, one for each $i \geq 1$, fixed by $(\sigma)$, and such that $W(E, d_i) = -1$. Moreover, by Theorem 5.2, the $\mathbb{Z}_p$-corank of $\mathrm{Sel}_{p^\infty}(E^{d_i}/\mathbb{Q})$ is odd for such $d_i$ and, by Lemma 4.2:

$$\mathrm{corank}_{\mathbb{Z}_p} \mathrm{Sel}_{p^\infty}(E/K_i) > \mathrm{corank}_{\mathbb{Z}_p} \mathrm{Sel}_{p^\infty}(E/\mathbb{Q}).$$

Let $P_i$, for $i \geq 1$, be a point of infinite order in $\mathrm{Sel}_{p^\infty}(E/K_i)$ not present in $\mathrm{Sel}_{p^\infty}(E/\mathbb{Q})$. Thus, for $i \neq j$, the points $P_i$ and $P_j$ are independent in $\mathrm{Sel}_{p^\infty}(E/K_iK_j)$ because they are defined over distinct fields. Hence, the $\mathbb{Z}_p$-corank of $\mathrm{Sel}_{p^\infty}(E/F_n) \geq n+1$, for $F_n = K_1 \cdots K_n$. □

## 6. Rank over $\mathbb{Q}_S^{(p)}$, for $p > 2$

This section completes the proof of Theorem 1.3 by providing a proof of part (2). First we mention that a result of T. Dokchitser ([2], Thm. 1) shows that $\mathrm{rank}_{\mathbb{Z}}(E(\mathbb{Q}^{(3)}))$ is infinite, without using the parity conjecture. However, his method does not seem to yield infinite rank over subfields of the form $(\mathbb{Q}^{(3)})^{(\sigma)}$. Instead, we summarize the results we need from V. Dokchitser's work [3] to show infinite rank over $(\mathbb{Q}_S^{(p)})^{(\sigma)}$, subject to the parity conjecture.

If $p \neq l$ are primes, we say that $E/K$ has wild ramification at $p$ if the $l$-adic Tate module is wildly ramified at $p$. If $E$ is defined over $\mathbb{Q}$ then only $p = 2$ or 3 may be wildly ramified and this happens when $p^3$ divides the conductor $N_E$ of $E/\mathbb{Q}$.

**Theorem 6.1** ([3], Thm. 6)**.** *Let $E/\mathbb{Q}$ be an elliptic curve and let $p > 2$ be prime. Assume that $E$ has good reduction at $p$ and does not have wild ramification at 2 and 3. Let $m > 1$ be a $p$-power free integer, which is not divisible by any prime where $E$ has additive reduction. Then the sign in the* *functional equation for $E$ over $\mathbb{Q}(\sqrt[p]{m})$ is given by*

$$W(E(\mathbb{Q}(\sqrt[p]{m}))) = W(E(\mathbb{Q}))\cdot(-1)^{\left(\frac{p-1}{2}+t\right)}$$

*where $t$ is the number of primes of multiplicative reduction of $E$, which do not divide $m$, and which are non-squares modulo $p$.*

Dokchitser's theorem has the following immediate consequence:

**Corollary 6.2** (cf. [3], Cor. 7)**.** *Let $E$ be an elliptic curve over $\mathbb{Q}$ without wild ramification at 2 and 3. Let $p > 2$ be prime, suppose that $E$ has good reduction at $p$, and let $t$ the number of primes of multiplicative reduction of $E$ which are non-squares modulo $p$. If $(\frac{p-1}{2}+t)$ is odd then $W(E(\mathbb{Q}(\sqrt[p]{m}))) \neq W(E(\mathbb{Q}))$ for all $p$-power free integers $m$ relatively prime to the primes of additive reduction of $E$.*

Finally, we are ready to show:

**Theorem 6.3.** *Let $E/\mathbb{Q}$, $p > 2$, $t \geq 0$ be as in the statement of Corollary 6.2, with $(\frac{p-1}{2}+t)$ odd, and let $S$ be an infinite set of primes, with $p \in S$. If the parity conjecture holds for $E$ over any extension $K/\mathbb{Q}$ of degree $p$, and $E$ does not have complex multiplication by $\mathbb{Q}(\sqrt{-p})$ then $\operatorname{rank}_{\mathbb{Z}}(E((\mathbb{Q}_S^{(p)})^{(\sigma)}))$ is infinite, for all $n \geq 0$ and all $(\sigma) \in \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})^n$.*

*Proof.* Notice that if $E$ has complex multiplication over $\mathbb{Q}(\mu_p)$ it must be over an imaginary quadratic number field $\mathbb{Q}(\sqrt{-p})$ contained in $\mathbb{Q}(\mu_p)$ (this could only happen for $p \equiv 3 \mod 4$). But, by assumption, $E$ does not have CM by such field. By Theorem 3.3, it suffices to show that $E/\mathbb{Q}$ satisfies property $(T_{S,p}^n)$ for all $n \geq 0$. First, let $\mathcal{D} = \{d_1, d_2, \ldots\}$ be the set of all primes in $S$ which do not divide $2pN_E$. Then:

(1) If $d_i, d_j \in \mathcal{D}$ then $d_i$ and $d_j$ are relatively prime, for $i \neq j$;
(2) $W(E(\mathbb{Q}(\sqrt[p]{d_i}))) \neq W(E(\mathbb{Q}))$ for all $i \geq 1$, by Corollary 6.2.

Let us fix $n \geq 0$, let $t = n+1$ and define $D_i = (d_{t(i-1)+1}, \ldots, d_{t\cdot i}) \in (\mathbb{Q}^\times)^t$ for all $i \geq 1$. We claim that these $D_i$ satisfy properties (1), (2) and (3) of Definition 3.2. For each $i \geq 1$, the fields $L_i$ are defined by

$$L_i = \mathbb{Q}(\mu_p, \{\sqrt[p]{d_j} : 1 \leq j \leq t\cdot i\})$$

and since all the $d_i$'s are pairwise relatively prime by construction, none of the numbers in $C_i$:

$$C_i = \{d = \prod_{j=1}^{t\cdot i}(d_j)^{e_j} : e_j = 0, 1, \ldots, p-1\}$$

can be a $p$th power of $\mathbb{Q}$. Thus $[L_i : \mathbb{Q}] = (p-1)p^{t\cdot i}$ and $[L_i : L_{i-1}] = p^t$. Moreover, the $d_i's$ are only divisible by primes of $S$, thus $L_i/\mathbb{Q}$ is unramified outside $S$ (notice that $p$ is definitely ramified). This shows (1) and (2).

Finally, if $d \in C_i$ then $d$ is not a $p$th power of $\mathbb{Q}$ and it is relatively prime to $N_E$. Thus, by Corollary 6.2, $W(E(\mathbb{Q}(\sqrt[p]{d}))) \neq W(E(\mathbb{Q}))$. If the parity conjecture holds for $\mathbb{Q}(\sqrt[p]{d})/\mathbb{Q}$ then $\mathrm{rank}_{\mathbb{Z}}(E(\mathbb{Q}(\sqrt[p]{d}))) > \mathrm{rank}_{\mathbb{Z}}(E(\mathbb{Q}))$ and (3) holds, which completes the proof of the theorem. □ □

**Corollary 6.4.** *Let $E/\mathbb{Q}$ be an elliptic curve without wild ramification at 2 and 3, and let $S$ be an infinite set of primes. There are infinitely many primes $p > 2$ such that if the Parity Conjecture holds for extensions of degree $p$ and we set $S' = S \cup \{p\}$ then the rank of $E((\mathbb{Q}_{S'}^{(p)})^{(\sigma)})$ is infinite, for all $n \geq 0$ and all $(\sigma) \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})^n$. In particular, $\mathrm{rank}_{\mathbb{Z}}(E(\overline{\mathbb{Q}}^{(\sigma)}))$ is infinite.*

*Further, if there is $q \in S$ such that $(\frac{q-1}{2} + t)$ is odd, then one can pick $p = q \in S$, where $t$ is the number of primes of multiplicative reduction for $E$ which are non-squares modulo $q$, and so $S = S'$.*

*Proof.* Let $q_1, \dots, q_s$ be the primes of multiplicative reduction dividing $N_E$, the conductor of $E/\mathbb{Q}$. If $E$ has CM by $\mathbb{Q}(\sqrt{-\ell})$, we will pick primes $p \neq \ell$. One only needs to find $p$ such that $(\frac{p-1}{2} + t)$ is odd, where $t$ is the number of primes $q_1, \dots, q_s$ which are non-squares modulo $p$. Ideally, try to choose $p \in S$ such that $(\frac{p-1}{2} + t)$ is odd. If this quantity is even for all $p \in S$ then use Dirichlet's theorem on primes in arithmetic progressions to choose $p \equiv 3 \mod 4$ if there are no primes of $E$ of multiplicative reduction or if the only prime of multiplicative reduction is 2; and $p \equiv 1 \mod 4\prod_{i=2}^{s} q_i$, with $p$ congruent to a non-square modulo $q_1 \neq 2$, otherwise, so that $t = 1$ and $(p-1)/2$ is even. □ □

## 7. Large Selmer Rank in Dihedral Extensions

In this section we will make use of the following deep theorem of K. Rubin and B. Mazur in order to prove Theorem 1.5.

**Theorem 7.1** ([16], Thm. B)**.** *Let $p > 2$ be prime. Suppose $K/k$ is a quadratic extension of number fields, $F/K$ is a finite abelian extension, $[F : K]$ is a power of $p$, and $F/k$ is dihedral (i.e. a lift of the involution of $K/k$ operates by conjugation on $\mathrm{Gal}(F/K)$ as inversion $\sigma \mapsto \sigma^{-1}$). Let $A/k$ be a polarized abelian variety defined over $k$ with a polarization of degree prime to $p$, such that $F/K$ is unramified at all primes where $A$ has bad reduction, and all primes above $p$ split in $K/k$. If $\mathrm{corank}_{\mathbb{Z}_p} \mathrm{Sel}_{p^\infty}(A/K)$ is odd, then $\mathrm{corank}_{\mathbb{Z}_p} \mathrm{Sel}_{p^\infty}(A/F) \geq [F : K]$.*

In order to prove Theorem 1.5 we need to show that the maximal dihedral $p$-extension of a quadratic field $K$, with constrained ramification and fixed by $(\sigma)$, is infinite. We start by proving the analogue of Lemma 3.1 that we will need here.

**Lemma 7.2.** *Let $k$ be a number field, let $n \geq 0$ be an integer and $(\sigma) \in G_k^n$ be fixed, let $t \geq 1$ be an integer, let $p \geq 2$ be a prime, let $K/k$ be an extension of number fields, fixed by $(\sigma)$, i.e. $K^{(\sigma)} = K$. Let $L_1, \dots, L_t$ be abelian extensions of $K$ of degree $p$, let $L$ be the compositum $L_1 L_2 \cdots L_t$ and suppose $[L : K] = p^t$. If $t > n$ then there is at least one extension $K'/K$ of degree $p$ with $K \subset K' \subset L \cap \overline{K}^{(\sigma)}$.*

*Proof.* Let $n \geq 0$ be an integer, let $p \geq 2$ be prime and let $L/K$ be as in the statement of the lemma. By construction, $L/K$ is Galois, $G = \mathrm{Gal}(L/K) \cong (\mathbb{Z}/p\mathbb{Z})^t$ and the order of $G$ is $p^t$. Moreover, it is clear that the order of any element of $G$ divides $p$, and similarly, if $H$ is the subgroup generated by elements $\gamma_1, \ldots, \gamma_n \in G$, then the order of $H$ divides $p^n$.

Let $(\sigma) = (\sigma_1, \ldots, \sigma_n) \in G_k^n$ be fixed, with the property that $K^{(\sigma)} = K$. Thus we will regard $(\sigma)$ as an element of $\mathrm{Gal}(\overline{k}/K)^n$ instead. Let $\gamma_i$ be the restriction of $\sigma_i$ to $L$ for $i = 1, \ldots, n$. The subgroup $H = \langle \gamma_1, \ldots, \gamma_n \rangle$ is a normal in $G$ (because $G$ is abelian). Thus, $L^{(\sigma)} = L^H$ and the degree $[L^H : K] = |G|/|H| = p^t/|H|$. Since the order of $H$ divides $p^n$, and by assumption $t > n$, then $p^{t-n}$ divides $[L^H : K]$, and in particular $p$ divides $[L^H : K]$. Moreover, $L^H/K$ is Galois and abelian, and $\mathrm{Gal}(L^H/K) \cong (\mathbb{Z}/p\mathbb{Z})^s$ for some $s > 0$. Hence, there is an abelian extension $K'/K$ of degree $p$, with $K \subset K' \subset L^H = L^{(\sigma)} = L \cap \overline{K}^{(\sigma)}$, as desired. □ □

We will also need the following theorem, due to I. R. Shafarevich, to understand the maximal abelian $p$-elementary extension of a field $K$, unramified outside a finite set of primes $\Sigma$, which we will denote by $K_\Sigma^{p\text{-elem}}$. In the statement of Shafarevich's theorem we will use the following notation. For an arbitrary field $L$, the symbol $\delta_p(L)$ is 1 or 0 as $L$ contains or does not contain the $p$th roots of unity. If $F/K$ is a $p$-elementary abelian extension, then $G = \mathrm{Gal}(F/K)$ is isomorphic to the direct sum of $d = d(G)$ copies of $\mathbb{Z}/p\mathbb{Z}$. Given a number field $K$, $r_1$ is the number of real embeddings and $r_2$ is half of the number of complex embeddings of $K$. Finally, the group Б$_\Sigma$ is defined as the quotient $V_\Sigma/K^{*p}$ where

$$V_\Sigma = \{\alpha \in K^* | (\alpha) = \mathfrak{A}^p,\ \alpha \in K_\wp^p \text{ for all } \wp \in \Sigma\}.$$

Here $K_\wp$ is the completion of $K$ at $\wp$. The group Б$_\Sigma$ is finite and, in fact, one can show that there is an upper bound independent of $\Sigma$:

$$\dim_{\mathbb{F}_p} Б_\Sigma \leq \dim_{\mathbb{F}_p} \mathrm{Cl}(K)/\mathrm{Cl}(K)^p + \delta_p(K)$$

where $\mathrm{Cl}(K)$ is the ideal class group of $K$ (see [7], p. 113, for more details).

**Theorem 7.3** ([7], Thm. 5.2, p. 118)**.** *Let $K$ be a number field, let $\Sigma$ be a finite set of places of $K$ and let $p$ be a fixed rational prime. The dimension of the Galois group of $K_\Sigma^{p\text{-elem}}/K$, regarded as a $\mathbb{F}_p$-vector space, is given by:*

$$(2) \quad \sum_{\wp \in \Sigma,\ \wp | p} [K_\wp : \mathbb{Q}_p] - \delta_p(K) - r_1 - r_2 + 1 + \sum_{\nu \in \Sigma} \delta_p(K_\nu) + \dim_{\mathbb{F}_p} Б_\Sigma.$$

**Corollary 7.4.** *Let $p > 2$ be a prime, let $K$ be a quadratic extension of $\mathbb{Q}$ and let $S$ be an infinite set of primes of $\mathbb{Z}$. Let $K_S^{p\text{-dihe}}$ be the maximal $p$-elementary abelian extension of $K$, unramified outside the primes of $K$ lying above primes in $S$, and dihedral over $\mathbb{Q}$ (as in the statement of Theorem 7.1). If the set $S$ contains infinitely many primes $q$ which either:*

(a) *$q$ remains inert in $K$ and $q \equiv -1 \mod p$, or*
(b) *$q$ splits in $K$ and $q \equiv 1 \mod p$,*

*then the extension $K_S^{p\text{-dihe}}/K$ is infinite.*

*Proof.* Let $p$, $K$ and $S$ be as in the statement of the theorem and let $S'$ be the set of all places of $K$ lying above primes in $S$. Clearly, there is an inclusion $K_S^{p\text{-dihe}} \subset K_{S'}^{p\text{-elem}}$ and by Theorem 7.3, the extension $K_{S'}^{p\text{-elem}}/K$ is infinite if and only if the series $\sum_{\nu\in S'} \delta_p(K_\nu)$ diverges. Let $q$ be a prime and let $\nu$ be a prime ideal of $K$ above $q$ (so that the norm $N\nu = q$ or $q^2$). Thus $N\nu \equiv 1 \mod p$ if and only if $\delta_p(K_\nu) = 1$, i.e. the completion $K_\nu$ contains the $p$th roots of unity. In particular, if $q$ satisfies either (a) or (b) as in the statement, then $\delta_p(K_\nu) = 1$. If $q$ splits then there are two different prime ideals $\nu$ and $\nu'$ such that $\delta_p(K_\nu) = \delta_p(K_{\nu'}) = 1$.

Suppose first that $S$ contains infinitely many primes $q$ satisfying (a). For all $N > 1$, by Theorem 7.3, we can find a finite set of primes $\Sigma \subset S$ such that every $q \in \Sigma$ is inert in $K$ (so by a slight abuse of notation we will consider $\Sigma$ as a set of primes of $K$) with $q \equiv -1 \mod p$, and such that the dimension of the Galois group $G$ of $K_\Sigma^{p\text{-elem}}/K$ is $d(G) > N$. The fact that the set of primes $\Sigma$ is fixed by the involution of $K/\mathbb{Q}$ and the maximality of $K_\Sigma^{p\text{-elem}}$ imply that the field $K_\Sigma^{p\text{-elem}}$ is actually Galois over $\mathbb{Q}$. Moreover, fix a $d(G)$-dimensional basis of $G$ and let $\tau \in \mathrm{GL}(d(G), \mathbb{F}_p)$ be the matrix giving the action of the involution of $K/\mathbb{Q}$ on $\mathrm{Gal}(K_\Sigma^{p\text{-elem}}/K)$. The square of the matrix $\tau$ is the identity, hence $\tau$ is diagonalizable and the eigenvalues of $\tau$ are $\pm 1$. Let $G^+$ and $G^-$ be the eigenspaces corresponding to the eigenvalues $\pm 1$ respectively and let $L$ be the fixed field by $G^-$ of $K_\Sigma^{p\text{-elem}}$. Then the extension $L/\mathbb{Q}$ is in fact Galois and abelian (because the involution acts trivially on $\mathrm{Gal}(L/K)$). If $L/K$ was non-trivial then there would be an extension of $\mathbb{Q}$ of degree $p$ unramified outside $\Sigma$, but this is clearly impossible because all primes of $\Sigma$ are congruent to $-1 \mod p$. Thus $L/K$ must be trivial and $G^- = G$, i.e. the only eigenvalue of $\tau$ is $-1$ and $\tau$ is simply $(-1)\,\mathrm{Id}$. Hence $K_\Sigma^{p\text{-elem}}/K$ is in fact dihedral and $d(G) > N$. Since $N$ was arbitrary, the desired conclusion follows.

Finally, suppose that $S$ contains infinitely many primes $q$ which split in $K$ and are congruent to $1 \mod p$. Let $q$ be one such prime and let $\nu$ and $\nu'$ be the prime ideals of $K$ lying above $q$. Let $\mathcal{O}_K$ be the ring of integers of $K$ and let $\mathrm{Cl}(K)$, $\mathrm{Cl}(K, \nu)$ be respectively the ideal class group of $K$ and the ray class group of $K$ of conductor $\nu$. Then the following is an exact sequence:

$$\mathcal{O}_K^\times \longrightarrow (\mathcal{O}_K/\nu)^\times \longrightarrow \mathrm{Cl}(K, \nu) \longrightarrow \mathrm{Cl}(K) \longrightarrow 1$$

and there is a similar sequence for $\nu'$. If $K$ is a real quadratic field, let $u$ be the fundamental unit in $\mathcal{O}_K$ and let $U$ be the set of rational primes dividing the norm $N(u^p - 1)$ (if $K$ is quadratic imaginary then set $U = \emptyset$). Thus, if $q \notin U \cup \{2, 3\}$ and $q \equiv 1 \mod p$ then there exist abelian extensions $F_\nu/K$ and $F_{\nu'}/K$ of degree $p$, respectively unramified outside $\nu$ and $\nu'$. Neither extension is Galois over $\mathbb{Q}$ but the compositum $F_\nu F_{\nu'}/K$ is Galois. Further, the involution of $K/\mathbb{Q}$ permutes $F_\nu$ and $F_{\nu'}$ and therefore the action of the involution on $\mathrm{Gal}(F_\nu F_{\nu'}/K)$ must be given by a matrix with two distinct eigenvalues $+1$ and $-1$. In particular, there are exactly two Galois extensions of degree $p$ of $K$ inside $F_\nu F_{\nu'}$, namely (i) the compositum of $K$ with the first layer of the $q$th cyclotomic extension of $\mathbb{Q}$ and (ii) an extension $F/K$ which is dihedral over $\mathbb{Q}$ and unramified outside $\nu, \nu'$. Since the set $U \cup \{2,3\}$ is finite and by assumption $S$ contains infinitely many primes $q$ as in (b), we conclude that the extension $K_S^{p\text{-dihe}}/K$ must be infinite. □ □

7.1. **Proof of Theorem 1.5.** Let $E/\mathbb{Q}$ be an elliptic curve and let $n$, $(\sigma)$, $K$ and $p > 2$ be as in the statement of the theorem. Let $S$ be an infinite set of rational primes which does not include any of the primes of bad reduction for $E/\mathbb{Q}$, and such that $S$ contains infinitely many primes $q$ inert in $K$ and $q \equiv -1 \mod p$, or split in $K$ and $q \equiv 1 \mod p$.

By Corollary 7.4 the extension $K_S^{p\text{-dihe}}/K$ is infinite and by Lemma 7.2, the extension $(K_S^{p\text{-dihe}})^{(\sigma)}/K$ is infinite as well. Let $N > 1$ be fixed and let $F/K$ be a subextension of $(K_S^{p\text{-dihe}})^{(\sigma)}/K$ with $[F:K] = p^N$. By Theorem 7.1, $\operatorname{corank}_{\mathbb{Z}_p} \operatorname{Sel}_{p^\infty}(E/F) > [F:K] = p^N$. Since $N$ is arbitrary, the theorem follows.

## 8. An Example

Let $E/\mathbb{Q}$ be the curve $37A1$, in J. Cremona's notation, given by $y^2 + y = x^3 - x$. The group of $\mathbb{Q}$-rational points of $E$ is isomorphic to $\mathbb{Z}$, generated by the point $(0,0)$, and its conductor is $N_E = 37$. Thus, $E/\mathbb{Q}$ has a unique bad prime and the reduction is (non-split) multiplicative. Also, whether we assume the parity conjecture or by direct calculation, the root number is $W(E/\mathbb{Q}) = -1$. Let $Q$ be the set of all odd primes $q \neq 37$ such that $q \equiv 3 \mod 4$ and $(\frac{q}{37}) = 1$, or $q \equiv 1 \mod 4$ and $(\frac{q}{37}) = -1$. The first few primes in $Q$ are $3, 5, 7, 11, 13, 17, 29, 47, \ldots$

Hence, $E/\mathbb{Q}$ satisfies the hypotheses of (1) and (2) in Theorem 1.3. Therefore if we assume the parity conjecture (for $E$ over number fields) and if $n \geq 0$, $S$ is an arbitrary infinite set of primes of $\mathbb{Z}$ and $(\sigma) \in G_{\mathbb{Q}}^n$ then

$$E\left((\mathbb{Q}_S^{(2)})^{(\sigma)}\right), \quad E\left((\mathbb{Q}_{S'}^{(q)})^{(\sigma)}\right)$$

are of infinite rank (and finite torsion) for all $q \in Q$, where $S' = S \cup \{q\}$.

Further, let $d \neq 0$ be a fundamental discriminant such that the Kronecker symbol $(\frac{d}{-37}) = -1$ and choose an odd prime $p \neq 37$ such that $p$ splits in $K = \mathbb{Q}(\sqrt{d})$. Then, by Lemma 4.1, the root number of $E^d/\mathbb{Q}$ is $W(E,d) = 1$ and by Theorem 5.2 the $\mathbb{Z}_p$-corank of $\operatorname{Sel}_{p^\infty}(E/\mathbb{Q})$ is odd and the $\mathbb{Z}_p$-corank of $\operatorname{Sel}_{p^\infty}(E^d/\mathbb{Q})$ is even. By Lemma 4.2, the corank of $\operatorname{Sel}_{p^\infty}(E/K)$ is odd. Let $S$ be any infinite set satisfying the hypotheses of Theorem 1.5, and let $(\sigma) \in G_{\mathbb{Q}}^n$ be an element fixing $K$. Then the $\mathbb{Z}_p$-corank of $\operatorname{Sel}_{p^\infty}(E/F)$ is unbounded over finite extensions $F/K$ contained in $(K_S^{p\text{-dihe}})^{(\sigma)}/K$. If $Ш(E/F)[p^\infty]$ is finite for all of these fields then the rank of

$$E\left((K_S^{p\text{-dihe}})^{(\sigma)}\right)$$

is infinite.

**Acknowledgements.** I would like to thank Ravi Ramakrishna and David Rohrlich for many interesting conversations, comments, suggestions and for providing me with some of the references that are cited in this article. I would also like to thank Karl Rubin for some useful comments and for pointing out the possibility of using [16] to prove Theorem 1.5.

## References

[1] Coates, J., Fukaya, T., Kato, K., Sujatha, R., Venjakob, O., The $GL_2$ main conjecture for elliptic curves without complex multiplication, Publ. Math. IHES 101 (2005).

[2] Dokchitser, T.: Ranks of elliptic curves in cubic extensions, Acta Arith. 126, pp. 357-360, (2007).

[3] Dokchitser, V.: Root numbers of non-abelian twists of elliptic curves (appendix by T. Fisher), Proc. London Math. Soc. (3) 91, pp. 300-324, (2005).

[4] Dokchitser, T., Dokchitser, V.: Root numbers of elliptic curves in residue characteristic 2, preprint, arXiv:math.NT/0612054.

[5] Frey, G., Jarden, M.: Approximation theory and the rank of abelian varieties over large algebraic fields, Proc. London Math. Soc. 28, pp. 112-128, (1974).

[6] Greenberg, R.: On the Birch and Swinnerton-Dyer conjecture, Invent. Math. 72, no. 2, pp. 241-265, (1983).

[7] Haberland, K.: Galois Cohomology of Algebraic Number Fields, VEB Deutscher Verlag der Wissenschaften, Berlin, (1978).

[8] Im, B-H., Larsen, M.: Abelian varieties over cyclic fields, Amer. J. Math. to appear, arXiv: math.NT/0605444.

[9] Im, B-H., Lozano-Robledo, Á.: On products of quadratic twists and ranks of elliptic curves over large fields, to appear.

[10] Kato, K.: $p$-adic Hodge theory and values of zeta functions of modular curves, Cohomologies $p$-adiques et applications arithmĕtiques. III. Astĕrisque No. 295, ix, pp. 117-290, (2004).

[11] Kim, B-D.: The parity conjecture for elliptic curves at supersingular reduction primes, Compositio Math. 143, pp. 47-72, (2007).

[12] Kobayashi, E.: A remark on the Mordell-Weil rank of elliptic curves over the maximal abelian extension of the rational number field, Tokyo J. Math. Vol. 29, no. 2, (2006).

[13] Larsen, M.: Rank of elliptic curves over almost algebraically closed fields, Bull. London Math. Soc. 35, pp. 817-820, (2003).

[14] Matsuura, R.: Root numbers of elliptic curves, Ph. D. Thesis (Boston University), in preparation.

[15] Mazur, B.: Rational points of abelian varieties with values in towers of number fields, Invent. Math. 18, pp. 183-266, (1972).

[16] Mazur, B., Rubin, K.: Finding large selmer rank via an arithmetic theory of local constants, to appear in Annals of Mathematics.

[17] Merel, L.: Bornes pour la torsion des courbes elliptiques sur les corps de nombres, Invent. Math. 124, no. 1-3, pp. 437-449, (1996).

[18] Nekovář, J.: On the parity of ranks of Selmer groups II, C. R. Acad. Sci. Paris Sér. I Math. 332, pp. 99-104, (2001).

[19] Petersen, S.: Root numbers and the rank of abelian varieties over large fields, preprint (dated July 26, 2006).

[20] Pop, F.: Embedding problems over large fields, Ann. of Math. (2) 144, no. 1, pp. 1-34, (1996).

[21] Ribet, K.: Torsion points of abelian varieties in cyclotomic extensions, Enseign. Math. 27, pp. 315-319, (1981).

[22] Rohrlich, D. E.: Variation of the root number in families of elliptic curves, Compositio Math., tome 87, no. 2, pp. 119-151, (1993).

[23] Rohrlich, D. E.: On L-functions of elliptic curves and cyclotomic towers, Invent. Math. 75, pp. 404-423, (1984).

[24] Rohrlich, D. E.: On L-functions of elliptic curves and anticyclotomic towers, Invent. Math. 75, no. 3, pp. 383-408, (1984).

[25] Rohrlich, D. E.: L-functions and division towers, Math. Ann. 281, pp. 611-632, (1988).

[26] Rohrlich, D. E.: Root numbers of semistable elliptic curves in division towers, Math. Res. Lett. 13, no. 3, pp. 359-376, (2006).

[27] Ruppert, W. M.: Torsion points of abelian varieties over abelian extensions, to appear.

[28] Silverman, J. H.: Integer points on curves of genus 1, J. London Math. Soc. (2), 28, pp. 1-7, (1983).

[29] Silverman, J. H.: The Arithmetic of Elliptic Curves, Springer, New York, (1986)

[30] Zarhin, Y. G.: Endomorphisms and torsion of abelian varieties, Duke Math. J. 54, no. 1, pp. 131-145 (1983).

*E-mail address*: `alozano@math.cornell.edu`