RANK STABILITY OF ELLIPTIC CURVES IN CERTAIN NON-ABELIAN EXTENSIONS

SIDDHI PATHAK AND ANWESH RAY

ABSTRACT. Let $E_{/\mathbb{Q}}$ be an elliptic curve with rank $E(\mathbb{Q}) = 0$. Fix an odd prime p, a positive integer n and a finite abelian extension $K/\mathbb{Q}$ with rank $E(K) = 0$. In this paper, we show that there exist infinitely many extensions L/K such that $L/\mathbb{Q}$ is Galois with $\mathrm{Gal}(L/\mathbb{Q}) \simeq \mathrm{Gal}(K/\mathbb{Q}) \ltimes \mathbb{Z}/p^n\mathbb{Z}$, and rank $E(L) = 0$. This is an extension of earlier results on rank stability of elliptic curves in cyclic extensions of prime power order to a non-abelian setting. We also obtain an asymptotic lower bound for the number of such extensions, ordered by their absolute discriminant.

1. INTRODUCTION

1.1. **The setting and historical background.** An elliptic curve is a smooth, projective, algebraic curve of genus 1, equipped with a distinguished point at ∞. These curves play a central role in number theory, algebraic geometry, and cryptography. The *Mordell–Weil group* of an elliptic curve E, defined over a number field K, is the group of K-rational points $E(K)$, under a natural group law arising from the geometry of the curve. By the *Mordell–Weil theorem*, $E(K)$ is a finitely generated abelian group, and can be expressed as

$$E(K) \cong \mathbb{Z}^r \oplus T,$$

where:

- $r \geq 0$ is an integer known as the *Mordell–Weil rank* of E over K, which measures the number of independent K-rational points of infinite order,
- T is a finite abelian group, called the *torsion subgroup*, consisting of points with finite order.

The rank r is a deep arithmetic invariant of the elliptic curve and is the subject of intense study. The famous Birch and Swinnerton–Dyer conjecture provides a profound connection between the rank r and the behavior of the Hasse–Weil L-function $L(E_{/K}, s)$ of E at $s = 1$. Specifically, the conjecture asserts that rank $E(K)$ is equal to the order of vanishing of $L(E_{/K}, s)$ at $s = 1$.

The points on $E(\overline{K})$, where $\overline{K}$ is the algebraic closure of K, naturally come equipped with an action of the absolute Galois group $\mathrm{Gal}(\overline{K}/K)$. This interaction allows for the arithmetic structure of $E(\overline{K})$ to be analyzed through Galois theoretic methods. A key tool in this analysis is the theory of Selmer groups, which consist of global Galois cohomology classes satisfying local conditions at all places. Selmer groups also carry information about the mysterious Tate–Shafarevich group $\Sha(E/K)$, whose elements consist of homogenous spaces measuring the failure of certain local-global principles for rational points on E.

Understanding the behaviour of the rank of an elliptic curve over extensions of number fields is a classical problem in number theory. One aspect of this study is to recognize the variation in the rank of an elliptic curve over field extensions. In particular, given an elliptic curve $E_{/\mathbb{Q}}$, one is interested in knowing how often is rank $E(L) > $ rank $E(\mathbb{Q})$, as $L/\mathbb{Q}$ varies over a family of number fields with fixed degree, ordered by absolute discriminant. In this regard, David, Fearnley and Kisilevsky

[DFK04, DFK07] studied the phenomenon of rank jumps of elliptic curves in cyclic extensions of prime order. More specifically, given an elliptic curve $E_{/\mathbb{Q}}$ and a prime p, they considered all cyclic extensions $L/\mathbb{Q}$ with Galois group isomorphic to $\mathbb{Z}/p\mathbb{Z}$, and asked how often rank $E(L) >$ rank $E(\mathbb{Q})$. Using the relationship between modular symbols and special values of cyclic twists of the Hasse-Weil L-function of E, they made predictions based on random matrix theory. In particular, it is conjectured that if $p \geq 7$, then there are only finitely many $\mathbb{Z}/p\mathbb{Z}$-extensions in which the rank can increase. These assertions are far from being resolved.

Mazur and Rubin [MR10] study distribution questions for 2-primary Selmer groups in quadratic twist families of elliptic curves. Their methods have applications to showing that the rank remains stable for a large number of quadratic twists. Their results imply (under additional conditions) that the rank can also become arbitrarily large after base change by a quadratic extension. For any prime p, the growth and stability for p-Selmer groups of elliptic curves in p-cyclic extensions of a number field has been studied by Klagsbrun, Mazur and Rubin [KMR14]. Similar results have been obtained by Smith, see [Smi22, Smi23] for further details. Park [Par24] has studied analogous questions over function fields. The phenomenon of rank jumps has been investigated further in other families of number field extensions. See for instance Lemke-Oliver–Thorne [LOT21], Schnidman–Weiss [SW23], Beneish–Kundu–Ray [BKR24], Berg–Ryan–Young [BRY24]. Moreover, the study of such rank stability questions has close connection to Hilbert's tenth problem, which has been recently studied for certain families of field extensions by Garcia–Fritz and Pasten [GFP20] and Kundu–Lei–Sprung [KLS24].

One advancement in this direction follows from the study of diophantine stability by Mazur-Rubin [MRL18]. They establish that for a simple abelian variety $A_{/K}$ with $\mathrm{End}_{\overline{K}}(A) = \mathrm{End}_K(A)$, there is a set S of primes with positive density such that for all $\ell \in S$ and for all integers $n > 0$, there are infinitely many $(\mathbb{Z}/\ell^n\mathbb{Z})$-extensions L/K that have $A(L) = A(K)$. This phenomenon has been studied by Ray–Weston from a different perspective in [RW23], where it is shown that for any prime $\ell \geq 5$, and any number field K, the density of elliptic curves $E_{/\mathbb{Q}}$, that are diophantine stable over K at ℓ is 1.

Another question of interest in number theory is the study of Galois extensions of a fixed number field with a given Galois group. Conjectures concerning the number of such extensions, ordered by their absolute discriminant, were proposed by Malle [Mal02, Mal04]. These can be viewed as statistical generalizations of the inverse Galois problem for number fields. There has been considerable progress towards these predictions, especially when the Galois group is of a specific kind. For instance, Malle's conjecture has been proved for abelian groups by Mäki [Mäk85] and Wright [Wri89] and for certain nilpotent groups by Koymans and Pagano [KP23]. Although the inverse Galois problem for finite solvable groups over number fields was resolved by Shafarevich [Š54], Malle's conjecture for general solvable groups is still open.

In this paper, we merge the above two themes to address the problem of counting certain solvable extensions of $\mathbb{Q}$ that have the rank stability property. More specifically, given a finite abelian group B, an elliptic curve $E_{/\mathbb{Q}}$ with rank $E(\mathbb{Q}) = 0$, a rational prime ℓ and a positive integer $n > 0$, under mild hypothesis, we demonstrate the existence of infinitely many extensions $L/\mathbb{Q}$ with $\mathrm{Gal}(L/\mathbb{Q}) \simeq B \ltimes \mathbb{Z}/\ell^n\mathbb{Z}$ such that rank $E(L) =$ rank $E(K) =$ rank $E(\mathbb{Q}) = 0$. Additionally, we obtain a lower bound for the number of such metabelian extensions, ordered by their absolute discriminant. This can compared with the total number of $B \ltimes \mathbb{Z}/\ell^n\mathbb{Z}$ extensions of $\mathbb{Q}$ predicted by Malle's conjectures.

1.2. **Statement of the main result.** Let p be an odd prime number and n be a positive integer. Let T denote the cyclic group $\mathbb{Z}/p^n\mathbb{Z}$. Let B be an abelian group and

$$\chi_0 : B \to \mathrm{Aut}(T) \xrightarrow{\sim} (\mathbb{Z}/p^n\mathbb{Z})^\times$$

be a character. Let $\mathcal{G} := B \ltimes T$ with respect to χ_0. Here, the semi-direct product is defined by the relation $xhx^{-1} = \chi_0(x)h$ for all $x \in B$ and $h \in T$. Fix a Galois extension $K/\mathbb{Q}$ such that $\mathrm{Gal}(K/\mathbb{Q})$ is isomorphic to B.

A $(\mathcal{G}, K)$-extension $L/K/\mathbb{Q}$ is a Galois extension $L/\mathbb{Q}$ which contains K and there exists an isomorphism $\mathrm{Gal}(L/\mathbb{Q}) \xrightarrow{\sim} \mathcal{G}$ which induces an isomorphism of $\mathrm{Gal}(L/K)$ with T. Thus, identifying $\mathrm{Gal}(L/\mathbb{Q})$ with $\mathcal{G}$, we find that $L^T = K$. Throughout the paper, we denote the absolute discriminant of L as Δ_L.

Denote by $\mathrm{Sel}_p(E/L)$ the p-Selmer group of E over L. Then, there is a natural short exact sequence

$$0 \to E(L)/pE(L) \to \mathrm{Sel}_p(E/L) \to \text{Ш}(E/L)[p] \to 0.$$

Thus, if $\mathrm{Sel}_p(E/L) = 0$, then, in particular, the rank of $E(L)$ and the p-primary part of the Tate-Shafarevich group $\text{Ш}(E/L)$ are zero.

With the above notation, our main theorem is as follows.

Theorem 1.1. *Let $p \geq 5$ be a prime number, $K/\mathbb{Q}$ be an abelian number field and $E_{/\mathbb{Q}}$ be an elliptic curve. Assume that the following conditions are satisfied.*

(1) The p-Selmer group $\mathrm{Sel}_p(E/K)$ vanishes.
(2) The field K contains $\mathbb{Q}(\mu_{p^n})$. In particular, B has order divisible by $p^{n-1}(p-1)$.
(3) The character χ_0 is nontrivial modulo p.
(4) The intersection $K \cap \mathbb{Q}(E[p])$ is equal to $\mathbb{Q}(\mu_p)$.
(5) The Galois representation $\rho_{E,p} : \mathrm{G}_\mathbb{Q} \to \mathrm{GL}_2(\mathbb{F}_p)$ associated with the p-torsion of $E(\overline{\mathbb{Q}})$ is surjective.

Then there are infinitely many $(\mathcal{G}, K)$-extensions $L/K/\mathbb{Q}$ such that $\mathrm{Sel}_p(E/L) = 0$. In particular, the rank of $E(L)$ is zero. Moreover, if $N_{\mathcal{G},K}(E; x)$ denotes the total number of $(\mathcal{G}, K)$-extensions such that $\mathrm{Sel}_p(E/L) = 0$ and $|\Delta_L| \leq x$, then we have

$$N_{\mathcal{G},K}(E; x) \gg_{\mathcal{G},K} x^{\frac{1}{|B|(p^n-1)}} (\log x)^{(p^{n-1}(p-1)\alpha)-1},$$

where

$$\alpha := \left(\frac{p^2 - p - 1}{[K : \mathbb{Q}(\mu_p)](p-1)(p^2-1)} \right).$$

The above result is obtained as an immediate consequence of Theorem 4.8, proved in Section 4 and Theorem 5.2, proved in Section 5.

Given a positive real number $x > 0$, set $M_{\mathcal{G},K}(x)$ to denote the total number of $(\mathcal{G}, K)$-extensions $L/K/\mathbb{Q}$ such that $|\Delta_L| \leq x$. A variant of the *Malle-Bhargava principle* predicts that

$$M_{\mathcal{G},K}(x) \sim c\, x^{\frac{1}{|B|(p-1)p^{n-1}}} (\log x)^b, \tag{1.1}$$

where $c > 0$ and $b \in \mathbb{Z}$ are constants that depend on $\mathcal{G}$ and K. For further details, see [Alb21, p. 2519 and p.2530] and [Bha07]. Thus, the number $N_{\mathcal{G},K}(E; x)$ differs from the total number $M_{\mathcal{G},K}(x)$ up to a power of x to the order of $O\left(\frac{1}{|B|p^{n+1}}\right)$ and a factor of $\log x$.

An interesting class of examples to which Theorem 1.1 applies are when $K = \mathbb{Q}(\mu_{p^n})$ and $\chi_0(x) = x^k$, where k is not divisible by $(p-1)$. In this case, χ_0 is k-th power of the mod-p^n cyclotomic character. Then the conditions (2) and (3) of Theorem 1.1 are clearly satisfied. If the representation $\rho_{E,p}$ is surjective, then

$$\text{Gal}(\mathbb{Q}(E[p])/\mathbb{Q}(\mu_p)) \simeq \text{SL}_2(\mathbb{F}_p).$$

Since $p \geq 5$, the group $\text{PSL}_2(\mathbb{F}_p)$ is simple, $\text{SL}_2(\mathbb{F}_p)$ does not have any abelian quotients, with cardinality divisible by p. Hence, the condition (4) follows from (5) when $K = \mathbb{Q}(\mu_{p^n})$, and Theorem 1.1 is applicable. It is worth noting that the representation $\rho_{E,p}$ is surjective for most elliptic curves, when ordered according to height by a theorem of Duke [Duk97].

When $n = 1$, so $K = \mathbb{Q}(\mu_p)$, we obtain a stronger result (Theorem 3.9 from Section 3) which is also valid for $p = 3$ and easier to state. At the end of the Section 3, we provide an explicit example for which our hypotheses are satisfied.

1.3. **Method of proof.** We now describe the ideas that go into the proofs of Theorem 4.8 and Theorem 5.2. In Section 2, given a p^n cyclic extension L/K and an elliptic curve $E_{/K}$ such that $\text{Sel}_p(E/K) = 0$, we derive conditions for $\text{Sel}_p(E/L) = 0$. Proposition 2.9 asserts that if the following conditions hold, then, $\text{Sel}_p(E/L) = 0$.

(1) The Selmer group $\text{Sel}_p(E/K)$ is 0.
(2) All primes of K that lie above p and the primes of bad reduction for E are completely split in L.
(3) All primes v of K that ramify satisfy $\widetilde{E}(k_v)[p] = 0$. Here, $\widetilde{E}$ denotes the reduction of E at v and k_v is the residue field at v.

Suppose that E and K satisfy the conditions of Theorem 1.1. In Section 4, we parameterize $(\mathcal{G}, K)$-extensions satisfying certain local conditions by Selmer classes. These are global Galois 1-cohomology classes taking values in $\mathbb{Z}/p^n\mathbb{Z}(\chi)$ and satisfying various local conditions at a certain set of primes Y. We show that these extensions satisfy the hypotheses of Proposition 2.9 mentioned above. Finally, we count the number of such cohomology classes. In order to do this, we invoke a formula due to Wiles (cf. Theorem 3.7) that relates the size of the Selmer group to that of a certain dual Selmer group, along with local terms arising from the Selmer conditions. The set of primes Y will be chosen to contain a prescribed set of primes Z so that the dual Selmer group becomes independent of Y. These choices play a crucial role in obtaining the main results Theorem 4.8, that is, when $n \geq 1$. The density of these extensions ordered by discriminant is proved in Theorem 5.2, which relies on Theorem 4.8 and an application of Delange's Tauberian theorem. This result is proved in Section 5.

2. Growth of p-Selmer groups in p-extensions

Let p be an odd prime number and K be a number field. Given an elliptic curve $E_{/K}$, and an algebraic extension L/K, we denote by $E_{/L}$ the base changed curve over L and $E(L)$ its Mordell-Weil group. Fix an algebraic closure $\bar{L}$ of L and set G_L to denote the absolute Galois group $\text{Gal}(\bar{L}/L)$. Let Ω_L be the set of all non-archimedean places of L and for $v \in \Omega_L$, denote by L_v the completion of L at v. Choose an algebraic closure $\bar{L}_v$ and an embedding $\iota_v : \bar{L} \hookrightarrow \bar{L}_v$. Setting $\text{G}_{L_v} := \text{Gal}(\bar{L}_v/L_v)$, we find that this induces an embedding $\iota_v^* : \text{G}_{L_v} \hookrightarrow \text{G}_L$. For ease of notation, we shall use

$$H^i(L, \cdot) := H^i(\text{G}_L, \cdot),$$

$$H^i(L_v, \cdot) := H^i(\text{G}_{L_v}, \cdot)$$

for $i \geq 0$ and $v \in \Omega_L$. Given a global cohomology class f, denote by $\text{res}_v(f)$ the restriction of f to G_{L_v}.

For $n \geq 1$ denote by $E[p^n]$ the p^n-torsion subgroup of $E(\bar{K})$; set $E[p^\infty] := \bigcup_{n \geq 1} E[p^n]$. Let $\mathfrak{G}$ denote either G_L or G_{L_v} for some $v \in \Omega_L$. Consider the short exact sequence of $\mathfrak{G}$-modules

$$0 \to E[p^n] \to E \xrightarrow{\times p^n} E \to 0.$$

We obtain a long exact sequence in cohomology from which we derive the following exact sequence

$$0 \to E(\mathcal{L}) \otimes_{\mathbb{Z}} \mathbb{Z}/p^n\mathbb{Z} \xrightarrow{\kappa_{\mathcal{L},n}} H^1(\mathcal{L}, E[p^n]) \to H^1(\mathcal{L}, E)[p^n] \to 0,$$

where $\mathcal{L}$ denotes L or L_v. Passing to the direct limit, we obtain an important short exact sequence

$$0 \to E(\mathcal{L}) \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p \xrightarrow{\kappa_{\mathcal{L},\infty}} H^1(\mathcal{L}, E[p^\infty]) \to H^1(\mathcal{L}, E)[p^\infty] \to 0.$$

The Selmer group is then defined as

$$\mathrm{Sel}_{p^n}(E/L) := \ker\left(H^1(L, E[p^n]) \longrightarrow \prod_{v \in \Omega_L} H^1(L_v, E)[p^n] \right).$$

In other words, $\mathrm{Sel}_{p^n}(E/L)$ consists of classes $f \in H^1(L, E[p^n])$ such that for all $v \in \Omega_L$, we find that $\mathrm{res}_v(f) \in \mathrm{Image}(\kappa_{L_v,n})$. Let $\Sha(E/L)$ denote the Tate-Shafarevich group of $E_{/L}$. The Selmer group fits into a short exact sequence

$$0 \to E(L) \otimes \mathbb{Z}/p^n \to \mathrm{Sel}_{p^n}(E/L) \to \Sha(E/L)[p^n] \to 0. \tag{2.1}$$

Taking the direct limit over n, we have the following short exact sequence

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

Definition 2.1. *Let S be the finite set of primes v of K such that at least one of the following conditions is satisfied:*

- *v is ramified in L,*
- *E has bad reduction at v,*
- *v divides p.*

We write $S(L)$ to denote the primes of L that lie above S. Let L_S be the maximal extension of L that is contained in $\bar{L}$ in which all non-archimedean primes $v \notin S$ are unramified. Then, the Selmer group $\mathrm{Sel}_p(E/L)$ is given by

$$\mathrm{Sel}_p(E/L) := \ker\left(H^1(L_S/L, E[p]) \xrightarrow{\Phi_{S,L}} \bigoplus_{w \in S(L)} H^1(L_w, E)[p] \right), \tag{2.2}$$

where $\Phi_{S,L}$ is the direct sum of restriction maps for the primes $w \in S(L)$. For further details, see [Mil06, section 1, Corollary 6.6].

Given a finite abelian group M, denote by $M^\vee$ the Pontryagin dual of M. Recall the Cassels-Tate long exact sequence

$$0 \to \mathrm{Sel}_p(E/L) \to H^1(L_S/L, E[p]) \xrightarrow{\Phi_{S,L}} \bigoplus_{w \in S(L)} H^1(L_w, E)[p]$$

$$\to \mathrm{Sel}_p(E/L)^\vee \to H^2(L_S/L, E[p]) \to \ldots,$$

cf. [CS10, p.8].

Let G be a finite group of p-power order and M be a finite p-primary G-module. Set $M^G := \{m \in M \mid gm = m$ for all $g \in G\}$ and $M_G := M/\langle(g - 1)m$ for $g \in G$ and $m \in M\rangle$. We record a useful lemma below.

Lemma 2.2. *If $M^G = 0$ or $M_G = 0$, then $M = 0$.*

Proof. The stated result is [NSW08, Proposition 1.6.12]. □

Henceforth, we set L/K be a finite Galois extension and set $G := \mathrm{Gal}(L/K)$. Assume that G is a p-group, i.e., $|G|$ is a power of p. Let E be an elliptic curve over K. Given a prime v of K, let γ_v be the restriction map

$$\gamma_v : H^1(K_v, E)[p] \to \bigoplus_{w|v} H^1(L_w, E)[p] \tag{2.3}$$

where w ranges over all primes of L that lie above v.

Proposition 2.3. *With respect to notation above, assume that the Selmer group*

$$\mathrm{Sel}_p(E/K) = 0.$$

Let S be as in Definition 2.1. Then the following assertions hold.

  (i) We have that

$$\dim_{\mathbb{F}_p}\left(\mathrm{Sel}_p(E/L)^G\right) = \sum_{v \in S} \dim_{\mathbb{F}_p}\left(\ker \gamma_v\right).$$

  (ii) The p-Selmer group $\mathrm{Sel}_p(E/L) = 0$ if and only if γ_v is injective for all $v \in S$.

Proof. Since it is assumed that $\mathrm{Sel}_p(E/K) = 0$, the map $\Phi_{S,K}$ in (2.2) is surjective. From the exact sequence (2.1), we find that $E(K) \otimes \mathbb{Z}/p\mathbb{Z} = 0$. Consequently, $\mathrm{rank}\, E(K) = 0$ and $E(K)[p] = 0$. Consider the commutative diagram

$$
\begin{array}{ccccccc}
0 = \mathrm{Sel}_p(E/K) & \longrightarrow & H^1(K_S/K, E[p]) & \xrightarrow{\Phi_{S,K}} & \bigoplus_{v \in S} H^1(K_v, E)[p] & \longrightarrow & 0 \\
& & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} \\
0 & \longrightarrow & \mathrm{Sel}_p(E/L)^G & \longrightarrow & H^1(L_S/L, E[p])^G & \longrightarrow & \left(\bigoplus_{w \in S(L)} H^1(L_w, E)[p]\right)^G,
\end{array}
\tag{2.4}
$$

where $\gamma := \bigoplus_{v \in S} \gamma_v$. Since S contains the primes that are ramified in L, we can identify L_S with K_S. The map β is the inflation map from the inflation-restriction sequence. Because the right square in the diagram involving β and γ commutes, it follows that β restricts to a map α. From the above diagram, we obtain the long exact sequence

$$0 \to \ker \beta \to \ker \gamma \to \mathrm{Sel}_p(E/L)^G \to \mathrm{cok}\, \beta \to \mathrm{cok}\, \gamma.$$

The inflation restriction sequence now implies that

$$\ker \beta \simeq H^1(L/K, E(L)[p]);$$
$$\mathrm{cok}\, \beta \subseteq H^2(L/K, E(L)[p]).$$

As L/K is a p-extension and $E(L)[p]^G = E(K)[p] = 0$, it follows from Lemma 2.2 that $E(L)[p] = 0$. Therefore, $\ker \beta = \mathrm{cok}\, \beta = 0$, and we have an isomorphism

$$\mathrm{Sel}_p(E/L)^G \simeq \ker \gamma,$$

which proves assertion (i). The conclusion (ii) is now evident from Lemma 2.2. □

We have thus reduced our problem to understanding when the maps γ_v are injective for $v \in S$.

Remark 2.4. *It is clear that if v splits completely in L, then γ_v is injective.*

In our applications, we will only consider extensions L/K such that if $v \mid p$ or if v is a prime of bad reduction for E, then v splits completely in L. Moreover, we will assume henceforth that

$$G \simeq \mathbb{Z}/p^n\mathbb{Z} \qquad \text{for some } n \in \mathbb{Z}_{\geq 1}.$$

Thus, the remaining section focuses on studying $\ker \gamma_v$ when v is a prime of good reduction, $v \nmid p$ and v is not completely split in L. This is established in Proposition 2.8.

To this end, we first prove some intermediate results.

Lemma 2.5. *Let G be a finite p group and M be a G-module. Assume that M is uniquely divisible by p, i.e., the multiplication by p map is an automorphism of M. Then $H^i(G, M) = 0$ for all $i \geq 1$.*

Proof. Since M is uniquely divisible by p, it follows that multiplication by p on $H^i(G, M)$ is an automorphism. On the other hand, G is a finite p-group and hence every element of $H^i(G, M)$ is annihilated by a power of p. In greater detail, the restriction co-restriction homomorphism

$$H^i(G, M) \xrightarrow{\text{res}} H^i(\{1\}, M) \xrightarrow{\text{cor}} H^i(G, M)$$

is multiplication by $|G|$, and hence multiplication by $|G|$ is trivial on $H^i(G, M)$. Therefore, it follows that $H^i(G, M) = 0$ for all $i \geq 1$. $\qquad\square$

Let k be a finite field and G be a connected smooth algebraic group over k. Given a field extension $\mathfrak{l}/k$, let $G(\mathfrak{l})$ denote the $\mathfrak{l}$-rational points of G.

Theorem 2.6 (Lang). *The cohomology group $H^1(\mathrm{Gal}(\bar{k}/k), G(\bar{k}))$ vanishes.*

Proof. The statement above follows from [Lan56, Theorem 2]. $\qquad\square$

Corollary 2.7. *Let k be a finite field and G be a connected smooth algebraic group over k. Let $\mathfrak{l}/k$ be a finite extension, then,*
$$H^1(\mathrm{Gal}(\mathfrak{l}/k), G(\mathfrak{l})) = 0.$$

Proof. The inflation map is an injection
$$H^1(\mathrm{Gal}(\mathfrak{l}/k), G(\mathfrak{l})) \hookrightarrow H^1\left(\mathrm{Gal}(\bar{k}/k), G(\bar{k})\right)$$
and thus $H^1(\mathrm{Gal}(\mathfrak{l}/k), G(\mathfrak{l})) = 0$ by Theorem 2.6. $\qquad\square$

For a prime w of L such that $w \mid v$, let

$$W_v := \text{image} \left\{ H^1(L_w/K_v, E(L_w)) \xrightarrow{\text{inf}} H^1(K_v, E) \right\}.$$

From the inflation-restriction sequence, it is easy to see that

$$\ker \gamma_v \subseteq W_v[p]. \tag{2.5}$$

Since the inflation map is always injective, we simply identify W_v with $H^1(L_w/K_v, E(L_w))$.

Let k_w (resp. k_v) denote the residue field of L at w (resp. K at v). Let $\widetilde{E}$ denote the reduction of E at w and $E_0(L_w) \subseteq E(L_w)$ denote the subgroup of points with non-singular reduction. We note that if w is a prime of good reduction, then $E_0 = E$. We set $E_1(L_w)$ to denote the kernel of the reduction map

$$E_0(L_w) \to \widetilde{E}(k_w). \tag{2.6}$$

Setting $G_w := \mathrm{Gal}(L_w/K_v)$, we have an exact sequence of G_w-modules

$$0 \to E_1(L_w) \to E_0(L_w) \to \widetilde{E}(k_w) \to 0, \tag{2.7}$$

where $\widetilde{E}(k_w)$ is unramified.

Proposition 2.8. *Assume that $G \simeq \mathbb{Z}/p^n\mathbb{Z}$ for some $n \in \mathbb{Z}_{\geq 1}$ and that $v \nmid p$ is a prime at which E has good reduction. Let w be any prime of L that lies above v. Then the following assertions hold.*

(i) If v is totally ramified in L, then

$$\dim_{\mathbb{F}_p} (\ker \gamma_v) \leq \dim_{\mathbb{F}_p} \left(\widetilde{E}(k_v)[p] \right).$$

(ii) If v is unramified and inert in L, then γ_v is injective.

(iii) If v is ramified in L and $\widetilde{E}(k_v)[p] = 0$, then γ_v is injective.

Proof. We first consider the case when v is totally ramified in L, and identify G_w with G. As E has good reduction at w, we find that $E(L_w) = E_0(L_w)$. Since $v \nmid p$, the multiplication by p map acts as an isomorphism on $E_1(L_w)$ and thus, it follows from Lemma 2.5 that $H^i(G_w, E_1(L_w)) = 0$ for $i \geq 1$. Thus, from the long exact sequence in cohomology associated to (2.6), we get the following isomorphism induced by the reduction map

$$H^1(G_w, E(L_w)) \xrightarrow{\sim} H^1(G_w, \widetilde{E}(k_w)). \tag{2.8}$$

By equation (2.5), we deduce that

$$\dim_{\mathbb{F}_p}(\ker \gamma_v) \leq \dim_{\mathbb{F}_p} W_v[p].$$

Since L_w/K_v is totally ramified, $k_w = k_v$. Therefore, the action of G_w on $\widetilde{E}(k_w)$ is trivial and we find that

$$\begin{aligned}
\dim_{\mathbb{F}_p} W_v[p] &= \dim_{\mathbb{F}_p} \mathrm{Hom}(G_w, \widetilde{E}(k_w))[p] \\
&= \dim_{\mathbb{F}_p} \mathrm{Hom}(\mathbb{Z}/p^n\mathbb{Z}, \widetilde{E}(k_w)[p]) \\
&= \dim_{\mathbb{F}_p}\left(\widetilde{E}(k_v)[p]\right).
\end{aligned}$$

This proves part (i) of the Proposition.

Next, we consider the case when v is unramified and inert in L. Then we identify G_w with $\mathrm{Gal}(k_w/k_v)$ and from the isomorphism in equation (2.8), we have that

$$H^1(G_w, E(L_w)) \simeq H^1(k_w/k_v, \widetilde{E}(k_w)).$$

The vanishing of $H^1(k_w/k_v, \widetilde{E}(k_w))$ follows from Corollary 2.7, which is a consequence of Lang's theorem. This proves part (ii) of the Proposition.

In order to prove part (iii), it follows from Lemma 2.2 that $\widetilde{E}(k_w)[p] = 0$. Therefore $\widetilde{E}(k_w)$ is uniquely p-divisible and hence $H^1(G_w, \widetilde{E}(k_w))[p] = 0$. The isomorphism (2.8) does not require v to be totally ramified in L and we find that $H^1(G_w, E(L_w))[p] = 0$. Therefore, the kernel of γ_v is zero, concluding the proof of part (iii). We thank the referee for suggesting this argument to prove part (iii). □

Proposition 2.9. *With respect to above notation, assume that the following assertions hold.*

(i) *The Selmer group* $\mathrm{Sel}_p(E/K)$ *is equal to* 0.

(ii) *All primes of K that lie above p and the primes of bad reduction for E are completely split in L.*

(iii) *All primes v of K that ramify in L satisfy $\widetilde{E}(k_v)[p] = 0$.*

Then, $\mathrm{Sel}_p(E/L) = 0$.

Proof. Let S be as in Definition 2.1. Then it follows from Proposition 2.3 (ii) that $\mathrm{Sel}_p(E/L) = 0$ if and only if γ_v is injective for all $v \in S$. For $v \in S$, if v divides p or v is a prime of bad reduction of E, then v is assumed to be split completely in L, according to hypothesis (ii). By Remark 2.4, γ_v is injective. The only other primes $v \in S$ are those that ramify in L. According to our assumption (iii), $\widetilde{E}(k_v)[p] = 0$ for such primes. Then, it follows from Proposition 2.8 part (iii) that γ_v is injective. This concludes our proof. □

Recall that $E[p]$ is the p-torsion submodule of $E(\overline{\mathbb{Q}})$. Let $\rho_{E,p} : G_\mathbb{Q} \to \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ be the Galois representation on $E[p]$. Let $\mathbb{Q}(E[p])$ be the Galois extension of $\mathbb{Q}$ *cut out* by $\rho_{E,p}$. In other words, it is defined to be the field $\overline{\mathbb{Q}}^{\ker \rho_{E,p}}$. We note that the Galois group $\mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q})$ can be identified

with the image of $\rho_{E,p}$. Given a prime ℓ at which E has good reduction, set $G_\ell := \mathrm{Gal}(\overline{\mathbb{Q}}_\ell/\mathbb{Q}_\ell)$ and take $I_\ell \subset G_\ell$ to be the inertia subgroup, defined to be the kernel of the mod-ℓ reduction map

$$G_\ell \to G_{\mathbb{F}_\ell}.$$

Let $\sigma_\ell \in G_\ell / I_\ell$ be the Frobenius automorphism. Denote by $a_\ell(E)$ the trace of the Frobenius element at ℓ. This is well defined since ℓ is a prime of good reduction for E. Moreover, the following relations hold (modulo p)

$$\mathrm{trace}\,\rho_{E,p}(\sigma_\ell) = a_\ell(E) \text{ and } \det \rho_{E,p}(\sigma_\ell) = \ell. \tag{2.9}$$

We set $K(E[p])$ to denote the composite $K \cdot \mathbb{Q}(E[p])$. We introduce a new set of primes which will play a significant role in our results.

Definition 2.10. *Let E be an elliptic curve over $\mathbb{Q}$ and let $\mathfrak{T}_E$ be the set of prime numbers ℓ satisfying the following conditions*

    (a) $\ell \neq p$,
    (b) ℓ is a prime at which E has good reduction,
    (c) ℓ is completely split in $K(\mu_p)$,
    (d) $\mathrm{trace}\left(\rho_{E,p}(\sigma_\ell)\right) \neq 2$.

We note that all but finitely many primes ℓ satisfy the first two of the above conditions. Given $\ell \in \mathfrak{T}_E$, the condition (c) above implies that $\ell \equiv 1 \bmod p$. It follows from (2.9) that $\rho_{E,p}(\sigma_\ell) \in \mathrm{SL}_2(\mathbb{F}_p)$ and from Definition 2.10 (d) that $a_\ell(E) \not\equiv 2 \bmod p$. Since

$$a_\ell(E) = \ell + 1 - \#\widetilde{E}(\mathbb{F}_\ell) \qquad \text{and} \qquad \ell \equiv 1 \bmod p,$$

we have that $\widetilde{E}(\mathbb{F}_\ell)[p] = 0$ for $\ell \in \mathfrak{T}_E$. The result below gives the relationship between the set of primes $\mathfrak{T}_E$ and the primes v that satisfy the condition $\widetilde{E}(k_v)[p] = 0$ from part (iii) of Proposition 2.9.

Lemma 2.11. *Let ℓ be a prime in $\mathfrak{T}_E$. Then $\widetilde{E}(k_v)[p] = 0$ for any of the primes of K such that $v|\ell$.*

Proof. Since ℓ splits in K, we find that $\widetilde{E}(k_v) = \widetilde{E}(\mathbb{F}_\ell)$. That $\widetilde{E}(\mathbb{F}_\ell)[p] = 0$ follows from the discussion above. $\qquad\square$

Lemma 2.12. *Suppose that $\rho_{E,p}$ is surjective and that*

$$K(\mu_p) \cap \mathbb{Q}(E[p]) = \mathbb{Q}(\mu_p).$$

Then the natural density of $\mathfrak{T}_E$ is equal to

$$\mathfrak{d}(\mathfrak{T}_E) = \frac{p^2 - p - 1}{[K(\mu_p) : \mathbb{Q}(\mu_p)]\,(p^2 - 1)(p - 1)}.$$

Proof. Let $\theta : \mathrm{Gal}(K(E[p])/K) \to \rho_{E,p}(G_K)$ be the isomorphism, mapping σ to $\rho_{E,p}(\sigma)$. Let $\mathcal{S}$ be the subset of matrices A in $\rho_{E,p}(G_K)$ with $\det A = 1$ and $\mathrm{trace}\,A \neq 2$. Let ℓ be a prime of good reduction for E with $\ell \neq p$ that is unramified in K. Then ℓ is unramified in $K(E[p])$. Moreover, $\sigma_\ell \in \theta^{-1}(\mathcal{S})$ if and only if $\ell \in \mathfrak{T}_E$. Indeed, if $\sigma_\ell \in \theta^{-1}(\mathcal{S})$, then $\sigma_\ell \in \mathrm{Gal}(K(E[p])/K)$. In fact, $\sigma_\ell \in \mathrm{Gal}(K(E[p])/K(\mu_p))$ since $\det(\rho_{E,p}(\sigma_\ell)) = 1$. Therefore ℓ splits in $K(\mu_p)$, and $\mathrm{trace}(\rho_{E,p}(\sigma_\ell)) \neq 2$ by the definition of $\mathcal{S}$, establishing the forward implication. For the converse, if $\ell \in \mathfrak{T}_E$, then it can be argued similarly that $\sigma_\ell \in \theta^{-1}(\mathcal{S})$.
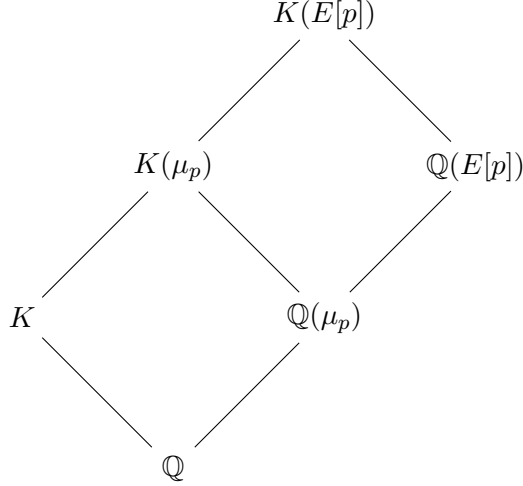
If $\#\mathcal{S} > 0$, then by the Chebotarev density theorem, the set of primes that satisfy the above conditions is infinite, with natural density $\left(\frac{\#\mathcal{S}}{[K(E[p]):\mathbb{Q}]}\right)$. We now count the number of matrices $A = \begin{pmatrix} a & b \\ c & 2-a \end{pmatrix} \in \mathrm{SL}_2(\mathbb{F}_p)$, that is, the number of triples $(a, b, c) \in \mathbb{F}_p^3$ such that $bc = a(2-a) - 1 = -a^2 + 2a - 1 = -(a-1)^2$. We consider two cases. Suppose $a = 1$. Then, either b or c is 0. Thus, the total number of triples when $a = 1$ is $2p - 1$. Next assume that $a \neq 1$. Then, b and c are both non-zero, and c is determined by a and b. Hence, the total number of triples for which $a \neq 1$ is equal to $(p-1)^2$. Hence, we have

$$\#\mathcal{S} = \#\,\mathrm{SL}_2(\mathbb{F}_p) - (p-1)^2 - (2p-1) = p(p^2-1) - (p-1)^2 - (2p-1)$$
$$= p^3 - p^2 - p.$$

Hence, we obtain that

$$\mathfrak{d}(\mathfrak{T}_E) = \frac{\#\mathcal{S}}{[K(E[p]):K]} = \frac{\#\mathcal{S}}{[K(\mu_p):\mathbb{Q}(\mu_p)][\mathbb{Q}(E[p]):\mathbb{Q}]} = \frac{\#\mathcal{S}}{[K(\mu_p):\mathbb{Q}(\mu_p)]\,\#\,\mathrm{GL}_2(\mathbb{F}_p)}$$
$$= \frac{p^3 - p^2 - p}{[K(\mu_p):\mathbb{Q}(\mu_p)]\,(p^2-1)(p^2-p)} = \frac{p^2 - p - 1}{[K(\mu_p):\mathbb{Q}(\mu_p)]\,(p^2-1)(p-1)}.$$

$\square$

3. Stability in extensions with Galois group $B \ltimes \mathbb{Z}/p\mathbb{Z}$

In this section, we fix p to be an odd prime number and K to be a Galois extension of $\mathbb{Q}$, with $B := \mathrm{Gal}(K/\mathbb{Q})$. Denote by ω the mod-p cyclotomic character. Given an $\mathbb{F}_p[\mathrm{G}_\mathbb{Q}]$-module M and an integer k, we set $M(k)$ to denote the k-fold Tate-twist $M \otimes_{\mathbb{F}_p} \mathbb{F}_p(\omega^k)$. Let E be an elliptic curve over $\mathbb{Q}$. Throughout this section, we make the following assumptions

- $\mathrm{Sel}_p(E/K) = 0$,
- B is a finite abelian group,
- $|B|$ is coprime to p,
- χ_0 is nontrivial mod p,
- K contains $\mathbb{Q}(\mu_p)$,
- $K \cap \mathbb{Q}(E[p]) = \mathbb{Q}(\mu_p)$.
- The Galois representation $\rho_{E,p} : \mathrm{G}_\mathbb{Q} \to \mathrm{GL}_2(\mathbb{F}_p)$ is surjective.

Let $\mathcal{G}$ be a finite group that is a semi-direct product $\mathcal{G} = B \ltimes T$, where $T \simeq \mathbb{Z}/p\mathbb{Z}$. The more general case when $T \simeq \mathbb{Z}/p^n\mathbb{Z}$ will be the subject of the next section. We consider $n = 1$ separately since in this case, the results are stronger and much easier to state.

We call $L/K/\mathbb{Q}$ a $(\mathcal{G}, K)$-extension if
- L is a Galois extension of $\mathbb{Q}$ which contains K,
- there is an isomorphism $\phi : \mathrm{Gal}(L/\mathbb{Q}) \xrightarrow{\sim} \mathcal{G}$ which restricts to an isomorphism $\mathrm{Gal}(L/K) \xrightarrow{\sim} T$.

We identify the Galois group $\mathrm{Gal}(L/\mathbb{Q})$ with $\mathcal{G}$ and find that $L^T = K$. We note that the condition $\mathrm{Sel}_p(E/K) = 0$ is equivalent to requiring that $\mathrm{rank}\, E(K) = 0$, $E(K)[p] = 0$ and $\mathrm{III}(E/K)[p] = 0$.

Let $\chi_0 : B \to \mathrm{Aut}(T) \xrightarrow{\sim} \mathbb{F}_p^\times$ be the character defined by

$$\chi_0(\sigma) := \sigma h \sigma^{-1}.$$

The group $\mathcal{G}$ is determined by χ_0 and we write $\mathcal{G} = B \ltimes_{\chi_0} T$ to emphasize this. We take $\chi : \mathrm{G}_\mathbb{Q} \to \mathbb{F}_p^\times$ to be the composite map

$$\mathrm{G}_\mathbb{Q} \twoheadrightarrow \mathrm{Gal}(K/\mathbb{Q}) \xrightarrow{\sim} B \xrightarrow{\chi_0} \mathbb{F}_p^\times,$$

where the first map above is the natural quotient map.

Let $\mathbb{F}_p(\chi)$ be the $\mathrm{G}_\mathbb{Q}$-module on which $\sigma \in \mathrm{G}_\mathbb{Q}$, the absolute Galois group, acts as follows: $\sigma \cdot x := \chi(\sigma)x$, where $\sigma \in \mathrm{G}_\mathbb{Q}$ and $x \in \mathbb{F}_p$. Let $Z^1(\mathrm{G}_\mathbb{Q}, \mathbb{F}_p(\chi))$ be the group of crossed homomorphisms, $f : \mathrm{G}_\mathbb{Q} \to \mathbb{F}_p(\chi)$. Given a finite set of primes Σ containing the primes at which χ is ramified, let $\mathbb{Q}_\Sigma$ be the maximal algebraic extension of $\mathbb{Q}$ in which the primes $\ell \notin \Sigma$ are unramified. Set $\mathrm{G}_\Sigma := \mathrm{Gal}(\mathbb{Q}_\Sigma/\mathbb{Q})$ and $Z^1(\mathbb{Q}_\Sigma/\mathbb{Q}, \mathbb{F}_p(\chi)) := Z^1(\mathrm{G}_\Sigma, \mathbb{F}_p(\chi))$. Let $f \in H^1(\mathbb{Q}_\Sigma/\mathbb{Q}, \mathbb{F}_p(\chi))$ and consider the restriction

$$g := f\big|_{\mathrm{Gal}(\mathbb{Q}_\Sigma/K)} : \mathrm{Gal}(\mathbb{Q}_\Sigma/K) \to \mathbb{F}_p.$$

Since the character χ is trivial when restricted to G_K, the restriction g is a homomorphism.

Definition 3.1. *Let K_f be the extension of K cut out by f, i.e., $K_f := (\mathbb{Q}_\Sigma)^{\ker g}$.*

The homomorphism g satisfies the relation

$$g(\sigma x \sigma^{-1}) = \chi(\sigma)g(x),$$

for $x \in \mathrm{Gal}(\mathbb{Q}_\Sigma/K)$ and $\sigma \in \mathrm{Gal}(\mathbb{Q}_\Sigma/\mathbb{Q})$. Thus, we find that $\ker(g)$ is a normal subgroup of $\mathrm{Gal}(\mathbb{Q}_\Sigma/\mathbb{Q})$, and hence, K_f is a Galois extension of K. Moreover, the Galois group $\mathrm{Gal}(K_f/\mathbb{Q})$ is isomorphic to $\mathcal{G}$ and the extension K_f is unramified at all primes $\ell \notin \Sigma$. Since B has order coprime to p,

$$H^i(B, \mathbb{F}_p(\chi)) = 0 \qquad \text{for} \qquad i > 0.$$

Hence, the restriction map,

$$\mathrm{res}_K : H^1(\mathbb{Q}_\Sigma/\mathbb{Q}, \mathbb{F}_p(\chi)) \to \mathrm{Hom}\big(\mathrm{Gal}(\mathbb{Q}_\Sigma/K), \mathbb{F}_p(\chi)\big)^B$$

is an isomorphism. Therefore, distinct cohomology classes f, f' give rise to distinct homomorphisms g, g'. Thus, we find that $K_f = K_{f'}$ if and only if $g = cg'$ for some scalar $c \in \mathbb{F}_p^\times$. This latter condition is equivalent to $f = cf'$.

Given a finite dimensional $\mathbb{F}_p$-vector space V, let $\mathbb{P}(V)$ denote the space of all $\mathbb{F}_p$-lines in V. In other words, $\mathbb{P}(V)$ is the set of all equivalence classes $\big(V \backslash \{0\}\big) / \sim$, where $v \sim v'$ if and only if there is a constant $c \in \mathbb{F}_p^\times$ such that $v = cv'$.

Proposition 3.2. *With respect to the notation above, there is a natural bijection*

$$\varphi_\Sigma : \mathbb{P}\left(H^1(\mathbb{Q}_\Sigma/\mathbb{Q}, \mathbb{F}_p(\chi))\right) \xrightarrow{\sim} \{L \mid L \text{ is a } (\mathcal{G}, K) \text{ extension of } \mathbb{Q}, \text{ unramified outside } \Sigma\},$$

defined by taking $\varphi_\Sigma(f) = K_f$.

Proof. From the inflation restriction sequence, we identify $\mathrm{Hom}\left(\mathrm{Gal}(\mathbb{Q}_\Sigma/K), \mathbb{F}_p(\chi)\right)^B$ with $H^1(\mathbb{Q}_\Sigma/\mathbb{Q}, \mathbb{F}_p(\chi))$. Given a $(\mathcal{G}, K)$-extension $L/K/\mathbb{Q}$, choose an isomorphism $\phi : \mathrm{Gal}(L/\mathbb{Q}) \xrightarrow{\sim} \mathcal{G}$ which restricts to an isomorphism

$$\phi_K : \mathrm{Gal}(L/K) \xrightarrow{\sim} T.$$

This in turn gives rise to a non-zero B-equivariant isomorphism

$$\psi : \mathrm{Hom}\left(\mathrm{Gal}(\mathbb{Q}_\Sigma/K), \mathbb{F}_p(\chi)\right)^B,$$

which is defined to be the natural composite

$$\mathrm{Gal}(\mathbb{Q}_\Sigma/K) \twoheadrightarrow \mathrm{Gal}(L/K) \xrightarrow{\phi_K} T \xrightarrow{\sim} \mathbb{F}_p(\chi).$$

Here, the action of B on $\mathrm{Hom}\left(\mathrm{Gal}(\mathbb{Q}_\Sigma/K), \mathbb{F}_p(\chi)\right)$ is as follows. Given $\sigma \in B = \mathrm{Gal}(K/\mathbb{Q})$ and $g \in \mathrm{Hom}\left(\mathrm{Gal}(\mathbb{Q}_\Sigma/K), \mathbb{F}_p(\chi)\right)$ let K_g be the field extension of K that is cut out by g. Pick a lift $\tilde{\sigma}$ of σ to $\mathrm{Gal}(K_f/\mathbb{Q})$. Then, set

$$(\sigma g)(x) := \chi(\sigma)g(\tilde{\sigma}^{-1}x\tilde{\sigma}).$$

This action is well defined, and independent of the choice of lift $\tilde{\sigma}$ since K_g is an abelian extension of K. Given two isomorphisms ϕ and ϕ', the associated maps ψ and ψ' are equivalent. The association $L \mapsto [\psi]$ is the inverse of φ_Σ. This proves the proposition. $\qquad\square$

Let $S_\mathbb{Q}$ be the set of all rational primes ℓ such that at least one of the following conditions hold:

- ℓ is ramified in K,
- ℓ is a prime at which E has bad reduction.

We note that p is ramified in K, and hence is contained in $S_\mathbb{Q}$. Let Σ be a finite set of rational primes that contains the set $S_\mathbb{Q}$. We set $Y := \Sigma \backslash S_\mathbb{Q}$, and assume that $Y \subset \mathfrak{T}_E$, where $\mathfrak{T}_E$ is as in Definition 2.10. We shall introduce splitting conditions for $(\mathcal{G}, K)$-extensions at the primes in $S_\mathbb{Q}$. For this purpose, we introduce the relevant Selmer groups.

Denote by G_Σ the Galois group $\mathrm{Gal}(\mathbb{Q}_\Sigma/\mathbb{Q})$. For ease of notation, we set

$$H^i(\mathbb{Q}_\Sigma/\mathbb{Q}, \cdot) := H^i(\mathrm{G}_\Sigma, \cdot),$$
$$H^i(\mathbb{Q}_\ell, \cdot) := H^i(\mathrm{Gal}(\overline{\mathbb{Q}}_\ell/\mathbb{Q}_\ell), \cdot).$$

Let M be a finite $\mathbb{F}_p[\mathrm{G}_\Sigma]$-module.

Definition 3.3. *A Selmer structure* supported on Σ *is a collection of subspaces*

$$\mathcal{L}_\ell \subseteq H^1(\mathbb{Q}_\ell, M)$$

for all $\ell \in \Sigma$. The Selmer group associated to the Selmer structure $\mathcal{L} = \{\mathcal{L}_\ell\}_{\ell \in \Sigma}$ is defined as follows

$$H^1_\mathcal{L}(\mathbb{Q}_\Sigma/\mathbb{Q}, M) := \left\{ f \in H^1(\mathbb{Q}_\Sigma/\mathbb{Q}, M) \mid \mathrm{res}_\ell(f) \in \mathcal{L}_\ell \text{ for all } \ell \in \Sigma \right\}.$$

We note that for an elliptic curve E over $\mathbb{Q}$ and a prime p, the p^n-Selmer group can be realized in this way for $M := E[p^n]$. In greater detail, let ℓ be a prime number and set $\mathcal{L}_\ell$ to denote the image of the mod-p local Kummer map

$$\kappa_{\mathbb{Q}_\ell, n} : E(\mathbb{Q}_\ell) \otimes \mathbb{Z}/p^n\mathbb{Z} \to H^1(\mathbb{Q}_\ell, E[p^n]).$$

Let Σ be the set of primes dividing Np where N is the conductor of E. Then we have that

$$\mathrm{Sel}_{p^n}(E/\mathbb{Q}) = H^1_\mathcal{L}(\mathbb{Q}_\Sigma/\mathbb{Q}, E[p^n]).$$

Given $f \in H^1_{\mathcal{L}}(\mathbb{Q}_\Sigma/\mathbb{Q}, \mathbb{F}_p(\chi))$ recall from Definition 3.1 that K_f is the extension of K cut out by f. A $(\mathcal{G}, K)$-extension $L/K/\mathbb{Q}$ is said to satisfy the Selmer condition $\mathcal{L}$ if $L = K_f$ for some $f \in H^1_{\mathcal{L}}(\mathbb{Q}_\Sigma/\mathbb{Q}, \mathbb{F}_p(\chi))$. When $\mathcal{L}_\ell = 0$ (resp. $\mathcal{L}_\ell = H^1(\mathbb{Q}_\ell, \mathbb{F}_p(\chi))$) we say that the condition at ℓ is *strict* (resp. *relaxed*). Throughout, we shall impose the strict condition above the primes $\ell \in S_\mathbb{Q}$ and the relaxed condition above the primes $\ell \in Y$. More precisely, we specify

$$\mathcal{L}_\ell := \begin{cases} 0 & \text{if } \ell \in S_\mathbb{Q}; \\ H^1(\mathbb{Q}_\ell, \mathbb{F}_p(\chi)) & \text{if } \ell \in Y. \end{cases} \tag{3.1}$$

We denote the associated Selmer group by

$$H^1_Y(\mathbb{Q}_\Sigma/\mathbb{Q}, \mathbb{F}_p(\chi)) := H^1_{\mathcal{L}}(\mathbb{Q}_\Sigma/\mathbb{Q}, \mathbb{F}_p(\chi)),$$

where $\mathcal{L}$ is as defined in (3.1). We fix this choice of $\mathcal{L}$ for the rest of this section.

Definition 3.4. *Let $\mathcal{W}_Y = \mathcal{W}_Y(E, K)$ be the set of $(\mathcal{G}, K)$-extensions which are unramified outside Σ and completely split at primes v of K above $S_\mathbb{Q}$.*

If $Y' \subseteq Y$, then, $\mathcal{W}_{Y'} \subseteq \mathcal{W}_Y$. The classes in $H^1_Y(\mathbb{Q}_\Sigma/\mathbb{Q}, \mathbb{F}_p(\chi))$ give rise to extensions in $\mathcal{W}_Y$.

Proposition 3.5. *With respect to notation above, suppose that $L \in \mathcal{W}_Y$. Assume that $\mathrm{Sel}_p(E/K) = 0$. Then $\mathrm{Sel}_p(E/L) = 0$.*

Proof. It suffices to show that the conditions of Proposition 2.9 are satisfied.
  (i) We have assumed that $\mathrm{Sel}_p(E/K) = 0$.
  (ii) Since $L \in \mathcal{W}_Y$, we find that all primes of K above $S_\mathbb{Q}$ are completely split in L. In particular, all primes of K that lie above p and the primes of bad reduction for $E_{/K}$ are completely split in L.
  (iii) The set of primes of K that ramify in L is a subset of the primes that lie above Y. Since Y is assumed to be a subset of $\mathfrak{T}_E$, it follows from Lemma 2.11 that $\widetilde{E}(k_v)[p] = 0$ for all primes of K that lie above Y.

It thus follows from Proposition 2.9 that $\mathrm{Sel}_p(E/L) = 0$. $\qquad\qquad\square$

We now recall the formula due to Wiles that allows one to compute the size of a Selmer group by relating it to the dual Selmer group. Let M be a finite $\mathbb{F}_p[\mathrm{G}_\Sigma]$-module and $\mathcal{L}$ be a Selmer structure on Σ. Let $M^\vee := \mathrm{Hom}_{\mathbb{F}_p}\left(M, \mathbb{F}_p(1)\right)$ be the Tate-dual of M. At each prime $\ell \in \Sigma$, let $\mathcal{L}_\ell^\vee$ be the orthogonal complement of $\mathcal{L}_\ell$ with respect to the nondegenerate local Tate pairing

$$H^1(\mathbb{Q}_\ell, M) \times H^1(\mathbb{Q}_\ell, M^\vee) \to H^2(\mathbb{Q}_\ell, \mathbb{F}_p(1)) \xrightarrow{\sim} \mathbb{F}_p.$$

Definition 3.6. *The* dual Selmer group *is defined as follows*

$$H^1_{\mathcal{L}^\vee}(\mathbb{Q}_\Sigma/\mathbb{Q}, M^\vee) := \left\{ g \in H^1(\mathbb{Q}_\Sigma/\mathbb{Q}, M^\vee) \mid \mathrm{res}_\ell(g) \in \mathcal{L}_\ell^\vee \text{ for all } \ell \in \Sigma \right\}.$$

For $M := \mathbb{F}_p(\chi)$, the Tate-dual is $M^\vee = \mathbb{F}_p(\omega\chi^{-1})$. For a choice of Y and the $S_\mathbb{Q}$-strict Selmer structure, the dual Selmer group in our context is given by

$$H^1_Y(\mathbb{Q}_\Sigma/\mathbb{Q}, \mathbb{F}_p(\omega\chi^{-1})) := \left\{ g \in H^1(\mathbb{Q}_\Sigma/\mathbb{Q}, \mathbb{F}_p(\omega\chi^{-1})) \mid \mathrm{res}_\ell(g) = 0 \text{ for all } \ell \in Y \right\}.$$

Theorem 3.7 (Wiles)**.** *Let M be a finite $\mathbb{F}_p[\mathrm{G}_\Sigma]$-module. The formula of Wiles asserts that*

$$\frac{\#H^1_{\mathcal{L}}(\mathbb{Q}_\Sigma/\mathbb{Q}, M)}{\#H^1_{\mathcal{L}^\vee}(\mathbb{Q}_\Sigma/\mathbb{Q}, M^\vee)} = \left(\frac{\#H^0(\mathbb{Q}, M)}{\#H^0(\mathbb{Q}, M^\vee)} \right) \times \prod_{\ell \in \Sigma} \left(\frac{\#\mathcal{L}_\ell}{\#H^0(\mathbb{Q}_\ell, M)} \right).$$

Proof. For a proof of the result, cf. [NSW08, Ch. 8]. $\qquad\qquad\square$

Proposition 3.8. *With respect to above notation, there is an explicit constant $C > 0$, that depends only on $S_{\mathbb{Q}}$ and K, such that*

$$\#\mathcal{W}_Y \geq \frac{p^{|Y|}}{C} - \frac{1}{(p-1)}.$$

Proof. It follows from the proof of Proposition 3.2 that the set $\mathcal{W}_Y$ is in bijection with $\mathbb{P}\left(H^1_Y(\mathbb{Q}_\Sigma/\mathbb{Q}, \mathbb{F}_p(\chi))\right)$ and hence,

$$\#\mathcal{W}_Y = \frac{\#H^1_Y(\mathbb{Q}_\Sigma/\mathbb{Q}, \mathbb{F}_p(\chi)) - 1}{p - 1}. \tag{3.2}$$

The formula of Wiles, as in Theorem 3.7, implies that

$$\#H^1_Y(\mathbb{Q}_\Sigma/\mathbb{Q}, \mathbb{F}_p(\chi)) = p \times \#H^1_Y(\mathbb{Q}_\Sigma/\mathbb{Q}, \mathbb{F}_p(\omega\chi^{-1})) \times C^{-1} \times \prod_{\ell \in Y} \left(\frac{\#H^1(\mathbb{Q}_\ell, \mathbb{F}_p(\chi))}{\#H^0(\mathbb{Q}_\ell, \mathbb{F}_p(\chi))}\right),$$

where

$$C := p \times \#H^0(\mathbb{Q}, \mathbb{F}_p(\omega\chi^{-1})) \times \prod_{\ell \in S_{\mathbb{Q}}} \#H^0(\mathbb{Q}_\ell, \mathbb{F}_p(\chi));$$

a quantity that depends only on $S_{\mathbb{Q}}$ and χ, and not on Y.

Note that each of the primes $\ell \in Y$ is in $\mathfrak{T}_E$ and hence splits in K. Therefore the character χ is trivial when restricted to $G_{\mathbb{Q}_\ell}$. Also, we note that since $\mathbb{Q}(\mu_p)$ is contained in K, the prime ℓ is 1 mod p. It follows from class field theory that $\#H^1(\mathbb{Q}_\ell, \mathbb{F}_p) = p^2$ and therefore,

$$\frac{\#H^1(\mathbb{Q}_\ell, \mathbb{F}_p(\chi))}{\#H^0(\mathbb{Q}_\ell, \mathbb{F}_p(\chi))} = \frac{p^2}{p} = p$$

for $\ell \in Y$. Therefore, substituting the above in (3.2), we have that

$$\#H^1_Y(\mathbb{Q}_\Sigma/\mathbb{Q}, \mathbb{F}_p(\chi)) \geq \frac{p^{|Y|+1}}{C}$$

and

$$\#\mathcal{W}_Y \geq \left(\frac{\frac{p^{|Y|+1}}{C} - 1}{p - 1}\right) \geq \frac{p^{|Y|}}{C} - \frac{1}{(p-1)}.$$

This completes the proof. □

Thus, we now have our main result of this section.

Theorem 3.9. *Let K be a Galois extension of $\mathbb{Q}$ and p be an odd prime number. Let E be an elliptic curve over $\mathbb{Q}$ and assume that the following conditions are satisfied*

(i) $\mathrm{Sel}_p(E/K) = 0$,
(ii) $B := \mathrm{Gal}(K/\mathbb{Q})$ is a finite abelian group,
(iii) $|B|$ is prime to p,
(iv) K contains $\mathbb{Q}(\mu_p)$,
(v) $K \cap \mathbb{Q}(E[p]) = \mathbb{Q}(\mu_p)$.
(vi) The Galois representation $\rho_{E,p} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_p)$ is surjective.

Let $\mathcal{G}$ be a finite group that is a semi-direct product $\mathcal{G} = B \ltimes T$, where $T \simeq \mathbb{Z}/p\mathbb{Z}$. Let $\mathfrak{T}_E$ be as in Definition 2.10, and for any finite set $Y \subset \mathfrak{T}_E$, let $\mathcal{W}_Y$ be as in Definition 3.4. Then

$$\#\mathcal{W}_Y \gg p^{|Y|},$$

for any finite set $Y \subset \mathfrak{T}_E$. Moreover, for any $L \in \mathcal{W}_Y$, the Selmer group $\mathrm{Sel}_p(E/L) = 0$. In particular, the rank of $E(L)$ is 0.

Note that $\mathfrak{T}_E$ is an infinite set of primes with density

$$\mathfrak{d}(\mathfrak{T}_E) = \frac{p^2 - p - 1}{[K : \mathbb{Q}(\mu_p)](p-1)(p^2-1)},$$

as proved in Lemma 2.12, with $\mathbb{Q}(\mu_p) \subseteq K$.

Proof of Theorem 3.9. Recall from Definition 2.10 that $\mathfrak{T}_E$ is set of prime numbers ℓ satisfying the following conditions

- $\ell \neq p$,
- ℓ is a prime at which E has good reduction,
- ℓ is completely split in $K(\mu_p)$,
- trace $\big(\rho_{E,p}(\sigma_\ell)\big) \neq 2$.

It follows from Proposition 3.8 that $\#\mathcal{W}_Y \gg p^{|Y|}$, and from Proposition 3.5 that $\mathrm{Sel}_p(E/L) = 0$ for $L \in \mathcal{W}_Y$. $\qquad\square$

An Example. We end this section with an example where the conditions of Theorem 3.9 are satisfied. We take $p = 3$ and since $K = \mathbb{Q}(\mu_3)$. The cyclotomic character $\omega : \mathrm{Gal}(K/\mathbb{Q}) \to (\mathbb{Z}/3\mathbb{Z})^\times$ is an isomorphism, and $\chi_0 : (\mathbb{Z}/3\mathbb{Z})^\times \to (\mathbb{Z}/3\mathbb{Z})^\times$ is the identity map. Then, χ is equal to ω. Consider the elliptic curve

$$E : y^2 + y = x^3 - x^2 - 7820x - 263580;$$

consider the following code on Sage

```
E=EllipticCurve("11a2")
K = QuadraticField(-3, 'z')
EK = E.base_extend(K)
EK.rank()
rho = E.galois_representation()
rho.image_type(3)
EK.torsion_order()
```

which shows that $E(K)[3] = 0$, rank $E(K) = 0$ and $\rho_{E,3}$ is surjective. It remains to show that $\text{Ш}(E/K)[3] = 0$ and then we shall deduce that $\mathrm{Sel}_3(E/K) = 0$.
Note that

$$\mathrm{Sel}_3(E/K) = \mathrm{Sel}_3(E/\mathbb{Q}) \oplus \mathrm{Sel}_3(E^{(-3)}/\mathbb{Q})$$

where $E^{(-3)}$ is the quadratic twist of E by -3. Thus, it suffices to show (via 3-descent) that $\mathrm{Sel}_3(E/\mathbb{Q}) = 0$ and $\mathrm{Sel}_3(E^{(-3)}/\mathbb{Q}) = 0$. For this, we use the following code on Magma

```
E := EllipticCurve("11a2");
ThreeSelmerGroup(E);
Et:=QuadraticTwist(E, -3);
ThreeSelmerGroup(Et);
```

which shows that $\mathrm{Sel}_3(E/\mathbb{Q})$ and $\mathrm{Sel}_3(E^{(-3)}/\mathbb{Q})$ are trivial.

4. Stability in extensions with Galois group $B \ltimes \mathbb{Z}/p^n\mathbb{Z}$

In this section, $p \geq 5$ is a prime number. We consider $K/\mathbb{Q}$ and $E_{/\mathbb{Q}}$ with $B := \mathrm{Gal}(K/\mathbb{Q})$. We let $\mathcal{G} = B \ltimes T$ where $T \simeq \mathbb{Z}/p^n\mathbb{Z}$ and $\chi_0 : B \to (\mathbb{Z}/p^n\mathbb{Z})^\times$ be the associated character. We take $\chi : \mathrm{G}_\mathbb{Q} \to (\mathbb{Z}/p^n\mathbb{Z})^\times$ the associated Galois character which factors as

$$\mathrm{G}_\mathbb{Q} \to \mathrm{Gal}(K/\mathbb{Q}) \xrightarrow{\sim} B \xrightarrow{\chi_0} (\mathbb{Z}/p^n\mathbb{Z})^\times.$$

Throughout, M will denote the Galois module $(\mathbb{Z}/p^n\mathbb{Z})(\chi)$. We set ϵ_n to denote the mod-p^n cyclotomic character and identify the Tate-dual of M with $(\mathbb{Z}/p^n\mathbb{Z})(\epsilon_n\chi^{-1})$.

Assume that the following conditions are satisfied

- $\mathrm{Sel}_p(E/K) = 0$,
- B is a finite abelian group,
- K contains $\mathbb{Q}(\mu_{p^n})$. In particular, the group B has order divisible by $p^{n-1}(p-1)$.
- The character χ_0 is nontrivial modulo p.
- The intersection $K \cap \mathbb{Q}(E[p])$ is equal to $\mathbb{Q}(\mu_p)$.
- The Galois representation $\rho_{E,p} : \mathrm{G}_\mathbb{Q} \to \mathrm{GL}_2(\mathbb{F}_p)$ is surjective.

Once more, let $S_\mathbb{Q}$ be the set of all rational primes ℓ such that at least one of the following conditions hold:

- ℓ is ramified in K,
- ℓ is a prime at which E has bad reduction.

For a finite set of primes Σ that contains $S_\mathbb{Q}$, set $Y := \Sigma \backslash S_\mathbb{Q}$. Let $\mathfrak{T}_E$ be as in Definition 2.10. Assume that $Y \subset \mathfrak{T}_E$.

Consider the inflation restriction sequence

$$0 \to H^1(B, M) \xrightarrow{\inf_K} H^1(\mathbb{Q}_\Sigma/\mathbb{Q}, M) \xrightarrow{\mathrm{res}_K} \mathrm{Hom}\left(\mathrm{Gal}(\mathbb{Q}_\Sigma/K), M\right)^B. \qquad (4.1)$$

We take $H^1_{\mathrm{surj}}(\mathbb{Q}_\Sigma/\mathbb{Q}, M)$ to be the subset of $H^1(\mathbb{Q}_\Sigma/\mathbb{Q}, M)$ consisting of classes for which $\mathrm{res}_K(f)$ surjects onto M. We note that when $n = 1$, the set $H^1_{\mathrm{surj}}(\mathbb{Q}_\Sigma/\mathbb{Q}, M)$ consists of non-zero classes. Given a cohomology class $f \in H^1_{\mathrm{surj}}(\mathbb{Q}_\Sigma/\mathbb{Q}, M)$, set $g := \mathrm{res}_K(f)$ and let $K_f := \overline{\mathbb{Q}}^{\ker g}$. It is easy to see that K_f is a $(\mathcal{G}, K)$-extension of $\mathbb{Q}$.

Define $f \sim f'$ if there exists $c \in (\mathbb{Z}/p^n\mathbb{Z})^\times$ such that $f - cf' \in \inf_K\left(H^1(B, M)\right)$, and let $\overline{H^1}_{\mathrm{surj}}(\mathbb{Q}_\Sigma/\mathbb{Q}, M) = H^1_{\mathrm{surj}}(\mathbb{Q}_\Sigma/\mathbb{Q}, M)/\sim$ denote the set of equivalence classes. If $f \sim f'$, then $K_f = K_{f'}$. It is also easy to see that

$$\#\overline{H^1}_{\mathrm{surj}}(\mathbb{Q}_\Sigma/\mathbb{Q}, M) = \frac{\#H^1_{\mathrm{surj}}(\mathbb{Q}_\Sigma/\mathbb{Q}, M)}{p^{n-1}(p-1)\ \#H^1(B, M)}.$$

Proposition 4.1. *With respect to notation above, there is a natural injection*

$$\overline{H^1}_{\mathrm{surj}}(\mathbb{Q}_\Sigma/\mathbb{Q}, M) \hookrightarrow \{L \mid L \text{ is a } (\mathcal{G}, K) \text{ extension of } \mathbb{Q}, \text{ unramified outside } \Sigma\},$$

defined by taking $\varphi_\Sigma(f) := K_f$.

Proof. From (4.1), identify $\overline{H^1}_{\mathrm{surj}}(\mathbb{Q}_\Sigma/\mathbb{Q}, M)$ with the equivalence classes of B-equivariant surjective homorphisms $g : \mathrm{Gal}(\mathbb{Q}_\Sigma/K) \to M$. Here, $g \sim g'$ if there exists $c \in (\mathbb{Z}/p^n\mathbb{Z})^\times$ such that $g = cg'$. These equivalence classes give rise to the set of $(\mathcal{G}, K)$-extensions that are unramified outside Σ, where the association in question is φ_Σ. $\qquad \square$

In this section, we write $Y = V \cup Z$, where V and Z are disjoint sets. The set Z is be fixed throughout and will be chosen later. The set V will vary over non-empty finite subsets of $\mathfrak{T}_E$ that are disjoint from Z.

Definition 4.2. *Let $\mathfrak{B}_V = \mathfrak{B}_V(E, K)$ denote the set of $(\mathcal{G}, K)$-extensions $L/K/\mathbb{Q}$ such that*

- *primes outside $\Sigma = S_\mathbb{Q} \cup V \cup Z$ are unramified in L*
- *primes of K above V are totally ramified in L*
- *primes of K above $S_\mathbb{Q}$ are completely split in L.*

As in the previous section, we wish to parameterize such extensions by Selmer classes. Given a prime $\ell \in Y$, since Y is a subset of $\mathfrak{T}_E$, ℓ splits in K. Since K contains $\mathbb{Q}(\mu_{p^n})$ by assumption, it follows that $\ell \equiv 1 \mod p^n$. As χ is trivial when restricted to G_K, the character χ is also trivial when restricted to $G_{\mathbb{Q}_\ell}$. By local class field theory, $H^1(\mathbb{Q}_\ell, M) = \mathrm{Hom}\left(G_{\mathbb{Q}_\ell}, M\right)$, and thus, $\#H^1(\mathbb{Q}_\ell, M) = p^{2n}$. For a prime $\ell \in V$, and a class $f \in H^1_Y(\mathbb{Q}_\Sigma/\mathbb{Q}, M)$, we say that f is totally ramified at ℓ if the restricted homomorphism $\mathrm{res}_\ell(f) : I_\ell \to M$ is surjective.

Let $\mathcal{L}$ be the Selmer structure supported on Σ that is strict at all primes of $S_{\mathbb{Q}}$ and relaxed at all primes of Y. More specifically

$$\mathcal{L}_\ell := \begin{cases} 0 & \text{if } \ell \in S_{\mathbb{Q}}; \\ H^1(\mathbb{Q}_\ell, M) & \text{if } \ell \in Y. \end{cases}$$

As in the previous section, we let $H^1_Y(\mathbb{Q}_\Sigma/\mathbb{Q}, M)$ and $H^1_Y(\mathbb{Q}_\Sigma/\mathbb{Q}, M^\vee)$ be the associated Selmer and dual Selmer groups respectively. We have

$$H^1_Y(\mathbb{Q}_\Sigma/\mathbb{Q}, M) = \{f \in H^1(\mathbb{Q}_\Sigma/\mathbb{Q}, M) \mid f \text{ is trivial at all primes } \ell \in S_{\mathbb{Q}}\};$$
$$H^1_Y(\mathbb{Q}_\Sigma/\mathbb{Q}, M^\vee) = \{\psi \in H^1(\mathbb{Q}_\Sigma/\mathbb{Q}, M^\vee) \mid \psi \text{ is trivial at all primes } \ell \in Y\}.$$

As a consequence of Wiles' formula (Theorem 3.7), we get

$$\frac{\#H^1_Y(\mathbb{Q}_\Sigma/\mathbb{Q}, M)}{\#H^1_Y(\mathbb{Q}_\Sigma/\mathbb{Q}, M^\vee)} = \left(\frac{\#H^0(\mathbb{Q}, M)}{\#H^0(\mathbb{Q}, M^\vee)}\right) \times \left(\prod_{\ell \in S_{\mathbb{Q}}} \frac{1}{\#H^0(\mathbb{Q}_\ell, M)}\right) \times \left(\prod_{\ell \in Y} \frac{\#H^1(\mathbb{Q}_\ell, M)}{\#H^0(\mathbb{Q}_\ell, M)}\right)$$
$$= \frac{p^{n|Y|}}{C},$$

where C is a constant that does not depend on Σ. We want to count the number of classes in $H^1_Y(\mathbb{Q}_\Sigma/\mathbb{Q}, M)$ that are totally ramified at the primes $\ell \in V$. In order to make this possible, we choose a set of primes $Z \subset \mathfrak{T}_E$, so that the dual Selmer group $H^1_Y(\mathbb{Q}_\Sigma/\mathbb{Q}, M^\vee) = 0$ for any choice of $V \subset \mathfrak{T}_E$.

Since $\mathbb{Q}(\mu_{p^n}) \subseteq K$, ϵ_n is trivial when restricted to G_K. The same is also true of χ, as is evident from its definition. Therefore, the action of G_K on $M^\vee$ is trivial. Consider the following inflation-restriction sequence.

$$0 \to H^1(B, M^\vee) \xrightarrow{\inf_K} H^1(\mathbb{Q}_\Sigma/\mathbb{Q}, M^\vee) \xrightarrow{\mathrm{res}_K} \mathrm{Hom}\left(\mathrm{Gal}(\mathbb{Q}_\Sigma/K), M^\vee\right)^B. \tag{4.2}$$

Let $0 \neq \psi \in H^1(\mathbb{Q}_\Sigma/\mathbb{Q}, M^\vee)$, and $\psi_K := \mathrm{res}_K(\psi)$ be the restriction of ψ to G_K. Define $K_\psi := \overline{K}^{\ker(\psi_K)}$ to be the extension of K that is cut out by ψ. Note that K_ψ/K is a Galois extension, with $\mathrm{Gal}(K_\psi/K) \simeq \mathrm{image}(\psi_K)$. Hence, $\mathrm{Gal}(K_\psi/K) \simeq \mathbb{Z}/p^m\mathbb{Z}$ for some $m \leq n$.

The proof of the following Lemma requires the assumption that $p \geq 5$. We use the fact that the group $\mathrm{PSL}_2(\mathbb{F}_p)$ is known to be simple when $p \geq 5$. Given a finite Galois extension $F/\mathbb{Q}$, by a Chebotarev class in $\mathrm{Gal}(F/\mathbb{Q})$ we mean a conjugacy class in $\mathrm{Gal}(F/\mathbb{Q})$.

Lemma 4.3. *Let $\psi \in H^1(\mathbb{Q}_\Sigma/\mathbb{Q}, M^\vee)$ be a class for which ψ_K is non-trivial. Let $\mathcal{C}_\psi$ be the set of all rational primes ℓ such that*

(a) ℓ splits in K,
(b) the trace of $\rho_{E,p}(\sigma_\ell)$ is not 2 mod p,
(c) any prime v of K that lies above ℓ does not split completely in K_ψ.

Then the collection of primes $\ell \in \mathcal{C}_\psi$ is infinite and defined by Chebotarev classes in the Galois group $\mathrm{Gal}(K_\psi(E[p])/\mathbb{Q})$.

Proof. Let ℓ be a rational prime, unramified in K. Denote by $\mathcal{C}_1 \subseteq \mathrm{Gal}(K/\mathbb{Q})$ the conjugacy class consisting of the identity element. The condition (a) is satisfied if and only if $\sigma_\ell \in \mathcal{C}_1$. Now, view $\mathcal{C}_1 \subseteq \mathrm{Gal}(K/\mathbb{Q}(\mu_p))$. Since $\rho_{E,p}$ is surjective, we identify $\mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q}(\mu_p))$ with $\mathrm{SL}_2(\mathbb{F}_p)$. Denote by $\mathcal{C}_2 \subseteq \mathrm{SL}_2(\mathbb{F}_p)$ the matrices with trace not equal to 2, that is condition (b). Recall that $K \cap \mathbb{Q}(E[p]) = \mathbb{Q}(\mu_p)$, and hence,

$$\mathrm{Gal}(K(E[p])/\mathbb{Q}(\mu_p)) \simeq \mathrm{Gal}(K/\mathbb{Q}(\mu_p)) \times \mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q}(\mu_p)).$$

Define $\mathcal{C}_3 := \mathcal{C}_1 \times \mathcal{C}_2$ and view it as a subset of $\mathrm{Gal}(K(E[p])/\mathbb{Q})$. Thus, both conditions (a) and (b) are satisfied if and only if ℓ is unramified in $K(E[p])$ and $\sigma_\ell \in \mathcal{C}_3$.
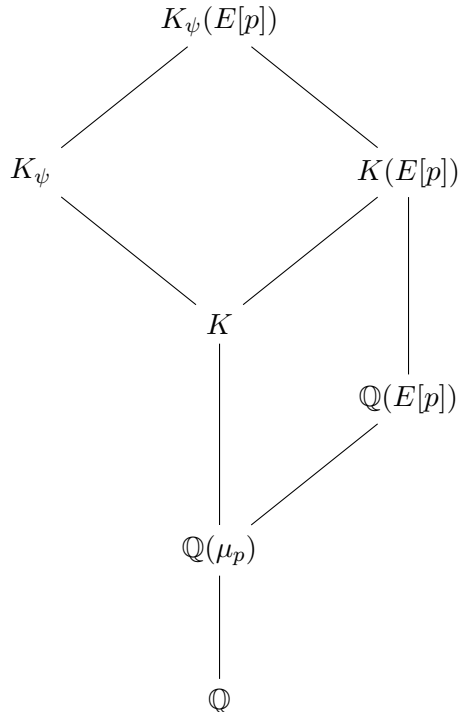
Note that $K_\psi \cap K(E[p]) = K$ as $p \geq 5$. In greater detail, K_ψ/K is a cyclic p-extension, whereas $\mathrm{Gal}(K(E[p])/K) \simeq \mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q}(\mu_p)) \simeq \mathrm{SL}_2(\mathbb{F}_p)$. As $\mathrm{PSL}_2(\mathbb{F}_p)$ is simple when $p \geq 5$, there are no sub-extensions $K \subsetneq K' \subsetneq K(E[p])$ with K'/K being cyclic, of order dividing p. Consequently, $K_\psi \cap K(E[p]) = K$, and

$$\mathrm{Gal}(K_\psi(E[p])/K) \simeq \mathrm{Gal}(K_\psi/K) \times \mathrm{Gal}(K(E[p]/K).$$

Since $\mathcal{C}_1$ is identity, $\mathcal{C}_3 \subseteq \mathrm{Gal}(K(E[p])/K)$. Let $\mathcal{C}_4 \subseteq \mathrm{Gal}(K_\psi/K)$ consist of the non-trivial elements, and define $\mathcal{C}_\psi := \mathcal{C}_3 \times \mathcal{C}_4$, viewed as a subset of $\mathrm{Gal}(K_\psi(E[p])/K) \subseteq \mathrm{Gal}(K_\psi(E[p])/\mathbb{Q})$. Thus, for a rational prime ℓ, unramified in K, the conditions (a), (b) and (c) are satisfied if and only if $\sigma_\ell \in \mathcal{C}_\psi$. □

We now apply the above lemma to show the following.

Proposition 4.4. *There exists a finite set of primes $Z \subset \mathfrak{T}_E$ such that*

$$H_Y^1(\mathbb{Q}_\Sigma/\mathbb{Q}, M^\vee) = \inf_K \left(H^1(B, M^\vee) \right)$$

whenever $Z \subseteq Y$.

Proof. We recall that

$$H^1_Y(\mathbb{Q}_\Sigma/\mathbb{Q}, M^\vee) = \{f \in H^1(\mathbb{Q}_\Sigma/\mathbb{Q}, M^\vee) \mid \mathrm{res}_\ell(f) = 0 \text{ for all } \ell \in Y\}.$$

Since all primes of Y split in K, it follows that $\inf_K \left(H^1(B, M^\vee)\right)$ is contained in the above dual Selmer group. Let ψ be a cohomology class in $H^1(\mathbb{Q}_\Sigma/\mathbb{Q}, M^\vee)$ that is not contained in the image of the inflation map. Then, $\psi_K \neq 0$ and and it follows from Lemma 4.3 that there is an infinite collection of primes ℓ in $\mathfrak{T}_E$ such that $\mathrm{res}_\ell(f) \neq 0$. We enumerate the classes $\psi \in H^1(\mathbb{Q}_\Sigma/\mathbb{Q}, M^\vee)$ such that ψ_K is non-trivial as $\psi_1, \psi_2, \cdots, \psi_m$. For each ψ_j, choose a prime $\ell_j \in \mathcal{C}_{\psi_j}$ and $Z := \{\ell_1, \ell_2, \cdots, \ell_m\}$. For this choice of Z, we have that $H^1_Y(\mathbb{Q}_\Sigma/\mathbb{Q}, M^\vee)$ is equal to $\inf_K \left(H^1(B, M^\vee)\right)$. $\square$

Lemma 4.5. *Let Y and Z be as in Proposition 4.4 and $\Sigma = V \cup Z \cup S_\mathbb{Q}$. Then, we have*

$$\#H^1_Y(\mathbb{Q}_\Sigma/\mathbb{Q}, M^\vee) = \#H^1_Z(\mathbb{Q}_{Z \cup S_\mathbb{Q}}/\mathbb{Q}, M^\vee). \tag{4.3}$$

Moreover,

$$\#H^1_Y(\mathbb{Q}_\Sigma/\mathbb{Q}, M) = \#H^1_Z(\mathbb{Q}_{Z \cup S_\mathbb{Q}}/\mathbb{Q}, M^\vee) \times p^{n|V|}.$$

Proof. Proposition 4.4 implies that

$$H^1_Y(\mathbb{Q}_\Sigma/\mathbb{Q}, M^\vee) = H^1_Z(\mathbb{Q}_{Z \cup S_\mathbb{Q}}/\mathbb{Q}, M^\vee) = \inf_K \left(H^1(B, M^\vee)\right),$$

and thus equation (4.3) is proved. It follows from Wiles' formula (Theorem 3.7) that

$$\frac{\#H^1_Y(\mathbb{Q}_\Sigma/\mathbb{Q}, M)}{\#H^1_Y(\mathbb{Q}_\Sigma/\mathbb{Q}, M^\vee)} = \left(\frac{\#H^0(\mathbb{Q}, M)}{\#H^0(\mathbb{Q}, M^\vee)}\right) \times \left(\prod_{\ell \in S_\mathbb{Q}} \frac{1}{\#H^0(\mathbb{Q}_\ell, M)}\right) \times \left(\prod_{\ell \in Y} \frac{\#H^1(\mathbb{Q}_\ell, M)}{\#H^0(\mathbb{Q}_\ell, M)}\right);$$

$$\frac{\#H^1_Z(\mathbb{Q}_{S_\mathbb{Q} \cup Z}/\mathbb{Q}, M)}{\#H^1_Z(\mathbb{Q}_{S_\mathbb{Q} \cup Z}/\mathbb{Q}, M^\vee)} = \left(\frac{\#H^0(\mathbb{Q}, M)}{\#H^0(\mathbb{Q}, M^\vee)}\right) \times \left(\prod_{\ell \in S_\mathbb{Q}} \frac{1}{\#H^0(\mathbb{Q}_\ell, M)}\right) \times \left(\prod_{\ell \in Z} \frac{\#H^1(\mathbb{Q}_\ell, M)}{\#H^0(\mathbb{Q}_\ell, M)}\right).$$

From equation (4.3), we find that

$$\#H^1_Y(\mathbb{Q}_\Sigma/\mathbb{Q}, M) = \#H^1_Z(\mathbb{Q}_{S_\mathbb{Q} \cup Z}/\mathbb{Q}, M) \times \left(\prod_{\ell \in V} \frac{\#H^1(\mathbb{Q}_\ell, M)}{\#H^0(\mathbb{Q}_\ell, M)}\right);$$

$$= \#H^1_Z(\mathbb{Q}_{S_\mathbb{Q} \cup Z}/\mathbb{Q}, M) \times p^{n|V|}.$$

$\square$

Let $\ell \in \mathfrak{T}_E$. Since ℓ splits completely in K, which contains $\mathbb{Q}(\mu_{p^n})$, the Galois action of $\mathrm{G}_{\mathbb{Q}_\ell}$ on M is trivial. Let $H^1_{\mathrm{nr}}(\mathbb{Q}_\ell, M)$ be the image of the inflation map

$$\inf_\ell : H^1(\mathrm{G}_{\mathbb{Q}_\ell}/\mathrm{I}_\ell, M) \to H^1(\mathbb{Q}_\ell, M).$$

Since the Galois action on M is trivial, $H^1_{\mathrm{nr}}(\mathbb{Q}_\ell, M)$ is identified with the subgroup of unramified homomorphisms in $\mathrm{Hom}(\mathrm{G}_{\mathbb{Q}_\ell}, \mathbb{Z}/p^n\mathbb{Z})$, and thus,

$$\#H^1_{\mathrm{nr}}(\mathbb{Q}_\ell, M) = p^n. \tag{4.4}$$

Proposition 4.6. *Let Z be as in Proposition 4.4. Then, with respect previous notation, we have the following short exact sequence*

$$0 \to H^1_Z(\mathbb{Q}_{S_\mathbb{Q} \cup Z}/\mathbb{Q}, M) \xrightarrow{\alpha_Z} H^1_Y(\mathbb{Q}_\Sigma/\mathbb{Q}, M) \xrightarrow{\pi_V} \bigoplus_{\ell \in V} \frac{H^1(\mathbb{Q}_\ell, M)}{H^1_{\mathrm{nr}}(\mathbb{Q}_\ell, M)} \to 0.$$

Here α_Z is the inflation map and π_V is induced by the direct sum of restriction maps for the primes in V.

Proof. The inflation map

$$\alpha_Z : H_Z^1(\mathbb{Q}_{S_\mathbb{Q} \cup Z}/\mathbb{Q}, M) \to H_Y^1(\mathbb{Q}_\Sigma/\mathbb{Q}, M)$$

is injective and the sequence

$$0 \to H_Z^1(\mathbb{Q}_{S_\mathbb{Q} \cup Z}/\mathbb{Q}, M) \to H_Y^1(\mathbb{Q}_\Sigma/\mathbb{Q}, M) \to \bigoplus_{\ell \in V} \frac{H^1(\mathbb{Q}_\ell, M)}{H_{\mathrm{nr}}^1(\mathbb{Q}_\ell, M)}$$

is exact. In order to prove that the above is a short exact sequence, we must observe that

$$\# \left(H_Z^1(\mathbb{Q}_{S_\mathbb{Q} \cup Z}/\mathbb{Q}, M) \right) \prod_{\ell \in V} \# \left(\frac{H^1(\mathbb{Q}_\ell, M)}{H_{\mathrm{nr}}^1(\mathbb{Q}_\ell, M)} \right) = \# \left(H_Y^1(\mathbb{Q}_\Sigma/\mathbb{Q}, M) \right).$$

Recall that for $\ell \in \mathfrak{T}_E$, we have

$$\# H^1(\mathbb{Q}_\ell, M) = \# \mathrm{Hom} \left(\mathrm{G}_{\mathbb{Q}_\ell}, \mathbb{Z}/p^n\mathbb{Z} \right) = p^{2n};$$
$$\# H_{\mathrm{nr}}^1(\mathbb{Q}_\ell, M) = \# \mathrm{Hom} \left(\mathrm{G}_{\mathbb{Q}_\ell} / \mathrm{I}_\ell, \mathbb{Z}/p^n\mathbb{Z} \right) = p^n.$$

The conclusion now follows from the above equation and the assertion of Lemma 4.5. □

Let $\mathfrak{B}_V$ be as in Definition 4.2 and $\mathfrak{A}_V$ be the subset of $\bigoplus_{\ell \in V} \frac{H^1(\mathbb{Q}_\ell, M)}{H_{\mathrm{nr}}^1(\mathbb{Q}_\ell, M)}$ consisting of tuples $(z_\ell + H_{\mathrm{nr}}^1(\mathbb{Q}_\ell, M))_{\ell \in V}$ where the class $z_{\ell | \mathrm{I}_\ell} : \mathrm{I}_\ell \to M$ is a surjective homomorphism for all $\ell \in V$. Then, it is easy to see that

$$\# \mathfrak{A}_V = \left((p-1)p^{n-1} \right)^{|V|}. \tag{4.5}$$

Let $H_{Y,V-\mathrm{ram}}^1(\mathbb{Q}_\Sigma/\mathbb{Q}, M)$ be set of all cohomology classes $f \in H_Y^1(\mathbb{Q}_\Sigma/\mathbb{Q}, M)$ such that $\pi_V(f) \in \mathfrak{A}_V$. These are the classes $f \in H_Y^1(\mathbb{Q}_\Sigma/\mathbb{Q}, M)$ that are totally ramified at all primes in V. Note that this is only a subset of $H_Y^1(\mathbb{Q}_\Sigma/\mathbb{Q}, M)$, and not a subgroup. However, if $f \in H_Y^1(\mathbb{Q}_\Sigma/\mathbb{Q}, M)$ and $h \in \inf_K \left(H^1(B, M) \right)$, then

$$f \in H_{Y,V-\mathrm{ram}}^1(\mathbb{Q}_\Sigma/\mathbb{Q}, M) \Leftrightarrow f + h \in H_{Y,V-\mathrm{ram}}^1(\mathbb{Q}_\Sigma/\mathbb{Q}, M).$$

Therefore, we may define an equivalence relation on $H_{Y,V-\mathrm{ram}}^1(\mathbb{Q}_\Sigma/\mathbb{Q}, M)$ by $f \sim g$ if $f - cg \in \inf_K \left(H^1(B, M) \right)$ for some $c \in (\mathbb{Z}/p^n\mathbb{Z})^\times$, and set

$$\overline{H^1}_{Y,V-\mathrm{ram}}(\mathbb{Q}_\Sigma/\mathbb{Q}, M) := H_{Y,V-\mathrm{ram}}^1(\mathbb{Q}_\Sigma/\mathbb{Q}, M)/\sim$$

to be the set of equivalence classes.

Proposition 4.7. *With respect to the notation above, the following assertions hold.*

(i) $\# \overline{H^1}_{Y,V-\mathrm{ram}}(\mathbb{Q}_\Sigma/\mathbb{Q}, M) = \left(\frac{\# H_Z^1(\mathbb{Q}_{S_\mathbb{Q} \cup Z}/\mathbb{Q}, M)}{\# H^1(B, M)} \right) \times \left((p-1)p^{n-1} \right)^{|V|-1}.$

(ii) *The injection from Proposition 4.1 restricts to a natural injection*

$$\phi_V : \overline{H^1}_{Y,V-\mathrm{ram}}(\mathbb{Q}_\Sigma/\mathbb{Q}, M) \hookrightarrow \mathfrak{B}_V,$$

defined by $\phi_V(f) := K_f$. This map is well defined and independent of the equivalence class of f.

(iii) *The size of $\mathfrak{B}_V$ is given by*

$$\# \mathfrak{B}_V \geq C \left((p-1)p^{n-1} \right)^{|V|},$$

where $C := \left(\frac{\# H_Z^1(\mathbb{Q}_{S_\mathbb{Q} \cup Z}/\mathbb{Q}, M)}{(p-1)p^{n-1}\# H^1(B, M)} \right)$ is a positive constant that does not depend on V.

Proof. From the definition above, it is clear that

$$\#\overline{H^1}_{Y,V-\mathrm{ram}}(\mathbb{Q}_\Sigma/\mathbb{Q}, M) = \frac{\#H^1_{Y,V-\mathrm{ram}}(\mathbb{Q}_\Sigma/\mathbb{Q}, M)}{(p-1)p^{n-1}\#\inf_K\left(H^1(B, M)\right)}.$$

Therefore, to compute $\#H^1_{Y,V-\mathrm{ram}}(\mathbb{Q}_\Sigma/\mathbb{Q}, M)$, recall the short exact sequence

$$0 \to H^1_Z(\mathbb{Q}_{S_\mathbb{Q}\cup Z}/\mathbb{Q}, M) \to H^1_Y(\mathbb{Q}_\Sigma/\mathbb{Q}, M) \xrightarrow{\pi_V} \bigoplus_{\ell \in V} \frac{H^1(\mathbb{Q}_\ell, M)}{H^1_{\mathrm{nr}}(\mathbb{Q}_\ell, M)} \to 0$$

from Proposition 4.6. We identify

$$H^1_{Y,V-\mathrm{ram}}(\mathbb{Q}_\Sigma/\mathbb{Q}, M) = \pi_V^{-1}\left(\mathfrak{A}_V\right).$$

Note that if $f \in H^1_{Y,V-\mathrm{ram}}(\mathbb{Q}_\Sigma/\mathbb{Q}, M)$ and $h \in H^1_Z(\mathbb{Q}_{S_\mathbb{Q}\cup Z}/\mathbb{Q}, M)$, then, $f+h \in H^1_{Y,V-\mathrm{ram}}(\mathbb{Q}_\Sigma/\mathbb{Q}, M)$. Hence, we have

$$\frac{\#H^1_{Y,V-\mathrm{ram}}(\mathbb{Q}_\Sigma/\mathbb{Q}, M)}{\#H^1_Z(\mathbb{Q}_{S_\mathbb{Q}\cup Z}/\mathbb{Q}, M)} = \#\mathfrak{A}_V.$$

By equation (4.5), we deduce that

$$\#\overline{H^1}_{Y,V-\mathrm{ram}}(\mathbb{Q}_\Sigma/\mathbb{Q}, M) = \left(\frac{\#H^1_Z(\mathbb{Q}_{S_\mathbb{Q}\cup Z}/\mathbb{Q}, M)}{\#H^1(B, M)}\right) \times \left((p-1)p^{n-1}\right)^{|V|}.$$

This proves part(i).

For part (ii), consider the map

$$\tilde{\phi}_V : H^1_{Y,V-\mathrm{ram}}(\mathbb{Q}_\Sigma/\mathbb{Q}, M) \to \mathfrak{B}_V$$

defined by $\tilde{\phi}_V(f) := K_f$. We see that $K_f = K_{f'}$ if and only if $f - cf'$ lies in the image of $\inf_K$ for some $c \in (\mathbb{Z}/p^n\mathbb{Z})^\times$. Therefore, $\tilde{\phi}_V$ descends to an injection ϕ_V.

Part (iii) is an immediate consequence of parts (i) and (ii). $\qquad\square$

We are now in a position to conclude the proof of our main result.

Theorem 4.8. *Let $p \geq 5$ be a prime number, $K/\mathbb{Q}$ be an abelian number field and $E_{/\mathbb{Q}}$ be an elliptic curve. Setting $B := \mathrm{Gal}(K/\mathbb{Q})$ and $T \simeq \mathbb{Z}/p^n\mathbb{Z}$, let $\mathcal{G} = B \ltimes T$. Assume that the conditions of Theorem 1.1 are satisfied. Let $S_\mathbb{Q}$ denote the set of all rational primes ℓ such that*

- *ℓ is ramified in K,*
- *ℓ is a prime at which E has bad reduction,*

and let S be the set of primes of K that lie above $S_\mathbb{Q}$. Let $\mathfrak{T}_E$ be as in Definition 2.10. Fix a choice of a finite set of primes $Z \subset \mathfrak{T}_E$, determined by Lemma 4.4. Let V be any finite set of primes contained in $\mathfrak{T}_E$ that is disjoint from $S_\mathbb{Q} \cup Z$. Let $\mathfrak{B}_V$ be as in Definition 4.2. Then the following assertions hold:

(a) *$\#\mathfrak{B}_V \geq C\left((p-1)p^{n-1}\right)^{|V|}$, for a positive constant C,*

(b) *for any $(\mathcal{G}, K)$-extension $L/K/\mathbb{Q}$ contained in $\mathfrak{B}_V$, $\mathrm{Sel}_p(E/L) = 0$. In particular, the rank of $E(L)$ is 0.*

Proof. The first assertion is proven in part (iii) of Proposition 4.7. For the second part, it suffices to show that the $(\mathcal{G}, K)$ extension L satisfies the conditions of Proposition 2.9. The only primes of K that ramify in L are those that lie above $Y = V \cup Z$. These primes are in $\mathfrak{T}_E$, and so by Lemma 2.11, for all primes v of K that lie above them, we have that $\widetilde{E}(k_v)[p] = 0$. This concludes the proof. $\qquad\square$

5. **A density result**

Let E be an elliptic curve over $\mathbb{Q}$, and $K/\mathbb{Q}$ be a Galois number field extension satisfying the conditions of Theorem 1.1. We now obtain a lower bound for the number of $(\mathcal{G}, K)$-extensions $L/K/\mathbb{Q}$ for which $\mathrm{Sel}_p(E/L) = 0$, ordered by absolute discriminant. Let $N_{\mathcal{G},K}(E; x)$ denote the total number of $(\mathcal{G}, K)$-extensions $L/K/\mathbb{Q}$ such that $\mathrm{Sel}_p(E/L) = 0$ and $|\Delta_L| \leq x$. We obtain an asymptotic lower bound for $N_{\mathcal{G},K}(E; x)$. Let $\mathfrak{T}_E$ be the set of primes as in Definition 2.10.

Lemma 5.1. *Let V be a finite set of primes in $\mathfrak{T}_E$ and let L be a $(\mathcal{G}, K)$-extension in $\mathfrak{B}_V$. Then*

$$|\Delta_L| = \left(\prod_{\ell \in V} \ell\right)^{|B|(p^n-1)}.$$

Proof. By definition, each prime $\ell \in \mathfrak{T}_E$ is completely split in K. Since L belongs to $\mathfrak{B}_V$, each of the primes $v \mid \ell$ of K is totally ramified in L. Note that all primes that are ramified in L are tamely ramified. Recall that

$$\Delta_L = \mathrm{Norm}_{L/\mathbb{Q}}\left(\mathfrak{D}_{L/\mathbb{Q}}\right)$$

where $\mathfrak{D}_{L/\mathbb{Q}}$ is the different ideal of $L/\mathbb{Q}$. It follows from well known properties of the different in a tamely ramified extension that

$$|\Delta_L| = \left(\prod_{\ell \in V} \ell\right)^{|B|(p^n-1)},$$

cf. [Ser79, Proposition 13]. $\square$

Theorem 5.2. *Let E be an elliptic curve over $\mathbb{Q}$, and $K/\mathbb{Q}$ be a Galois number field extension satisfying the conditions of Theorem 1.1. With respect to earlier notation, we have*

$$N_{\mathcal{G},K}(E; x) \gg x^{\frac{1}{|B|(p^n-1)}} (\log x)^{\left(p^{n-1}(p-1)\alpha\right)-1},$$

where

$$\alpha := \left(\frac{p^2 - p - 1}{[K : \mathbb{Q}(\mu_p)](p-1)(p^2-1)}\right).$$

Proof. The argument of proof similar to [Ser75, Theorem 2.4, p.5 line -3 to p.6 line -10.]. We provide a sketch here for completeness. Setting $y := x^{\frac{1}{|B|(p^n-1)}}$, denote by $M(y)$ the collection of all finite subsets V of $\mathfrak{T}_E$ such that

$$\prod_{\ell \in V} \ell \leq y.$$

From Theorem 4.8 and Lemma 5.1, we have

$$N_{\mathcal{G},K}(E; x) \geq \sum_{V \in M(y)} \#\mathfrak{B}_V. \tag{5.1}$$

Thus, from Theorem 4.8 part (a) and (5.1) we get

$$N_{\mathcal{G},K}(E; x) \geq C \sum_{V \in M(y)} r^{|V|}, \tag{5.2}$$

where $r := p^{n-1}(p-1)$. Consider the function

$$F(s) := \sum_{\substack{V \subset \mathfrak{T}_E \\ V \text{ finite}}} \frac{r^{|V|}}{\prod_{\ell \in V} \ell^s} = \prod_{\ell \in \mathfrak{T}_E} \left(1 + \frac{r}{\ell^s}\right).$$

Thus, we see that

$$\log F(s) = r \sum_{\ell \in \mathfrak{T}_E} \frac{1}{\ell^s} + \theta_1(s),$$

where $\theta_1(s)$ is holomorphic in $\mathrm{Re}(s) \geq 1$; and as a consequence,

$$\log F(s) = r\alpha \, \log\left(\frac{1}{s-1}\right) + \theta_2(s),$$

where $\alpha = \mathfrak{d}(\mathfrak{T}_E)$, which is computed in Lemma 2.12, and $\theta_2(s)$ is holomorphic in $\mathrm{Re}(s) \geq 1$. Thus, we deduce that

$$F(s) = (s-1)^{-r\alpha} \, h(s),$$

where $h(s)$ is a non-zero holomorphic function in $\mathrm{Re}(s) \geq 1$. By Delange's Tauberian theorem (cf. [Ten15, Theorem 7.28]), we deduce that

$$N_{\mathcal{G},K}(E; x) \gg y \, (\log y)^{r\alpha - 1} \gg x^{\frac{1}{|B|(p^n-1)}} (\log x)^{\left(p^{n-1}(p-1)\alpha\right) - 1}.$$

This proves the result. $\qquad\qquad\square$

ACKNOWLEDGMENTS

REFERENCES

[Alb21] Brandon Alberts. Statistics of the first Galois cohomology group: a refinement of Malle's conjecture. *Algebra Number Theory*, 15(10):2513–2569, 2021.

[Bha07] Manjul Bhargava. Mass formulae for extensions of local fields, and conjectures on the density of number field discriminants. *Int. Math. Res. Not. IMRN*, (17):Art. ID rnm052, 20, 2007.

[BKR24] Lea Beneish, Debanjana Kundu, and Anwesh Ray. Rank jumps and growth of Shafarevich-Tate groups for elliptic curves in $\mathbb{Z}/p\mathbb{Z}$-extensions. *J. Aust. Math. Soc.*, 116(1):1–38, 2024.

[BRY24] Jennifer Berg, Nathan C. Ryan, and Matthew P. Young. Vanishing of quartic and sextic twists of L-functions. *Res. Number Theory*, 10(1):Paper No. 20, 25, 2024.

[CS10] J. Coates and R. Sujatha. *Galois cohomology of elliptic curves.* Published by Narosa Publishing House, New Delhi; for the Tata Institute of Fundamental Research, Mumbai, second edition, 2010.

[DFK04] Chantal David, Jack Fearnley, and Hershy Kisilevsky. On the vanishing of twisted L-functions of elliptic curves. *Experiment. Math.*, 13(2):185–198, 2004.

[DFK07] Chantal David, Jack Fearnley, and Hershy Kisilevsky. Vanishing of L-functions of elliptic curves over number fields. In *Ranks of elliptic curves and random matrix theory*, volume 341 of *London Math. Soc. Lecture Note Ser.*, pages 247–259. Cambridge Univ. Press, Cambridge, 2007.

[Duk97] William Duke. Elliptic curves with no exceptional primes. *Comptes rendus de l'Académie des sciences. Série 1, Mathématique*, 325(8):813–818, 1997.

[GFP20] Natalia Garcia-Fritz and Hector Pasten. Towards Hilbert's tenth problem for rings of integers through Iwasawa theory and Heegner points. *Math. Ann.*, 377(3-4):989–1013, 2020.

[KLS24] Debanjana Kundu, Antonio Lei, and Florian Sprung. Studying hilbert's 10th problem via explicit elliptic curves. *Mathematische Annalen*, pages 1–31, 2024.

[KMR14] Zev Klagsbrun, Barry Mazur, and Karl Rubin. A Markov model for Selmer ranks in families of twists. *Compos. Math.*, 150(7):1077–1106, 2014.

[KP23] Peter Koymans and Carlo Pagano. On malle's conjecture for nilpotent groups. *Transactions of the American Mathematical Society, Series B*, 10(11):310–354, 2023.

[Lan56] Serge Lang. Algebraic groups over finite fields. *Amer. J. Math.*, 78:555–563, 1956.

[LOT21] Robert J. Lemke Oliver and Frank Thorne. Rank growth of elliptic curves in non-abelian extensions. *Int. Math. Res. Not. IMRN*, 2021(24):18411–18441, 2021.

[Mäk85] Sirpa Mäki. *On the density of abelian number fields*, volume 54. Suomalainen tiedeakatemia, 1985.

[Mal02] Gunter Malle. On the distribution of Galois groups. *J. Number Theory*, 92(2):315–329, 2002.

[Mal04] Gunter Malle. On the distribution of Galois groups. II. *Experiment. Math.*, 13(2):129–135, 2004.

[Mil06] J. S. Milne. *Arithmetic duality theorems.* BookSurge, LLC, Charleston, SC, second edition, 2006.

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

[MRL18] Barry Mazur, Karl Rubin, and Michael Larsen. Diophantine stability. *American Journal of Mathematics*, 140(3):571–616, 2018.

[NSW08] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg. *Cohomology of number fields*, volume 323 of *Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, second edition, 2008.

[Par24] Sun Woo Park. On the prime selmer ranks of cyclic prime twist families of elliptic curves over global function fields, 2024.

[RW23] Anwesh Ray and Tom Weston. Diophantine stability for elliptic curves on average. *arXiv preprint arXiv:2304.09742*, 2023.

[Ser75] Jean-Pierre Serre. Divisibilité de certaines fonctions arithmétiques. In *Séminaire Delange-Pisot-Poitou (16e année: 1974/75), Théorie des nombres, Fasc. 1*, pages Exp. No. 20, 28. Secrétariat Math., Paris, 1975.

[Ser79] Jean-Pierre Serre. *Local fields*, volume 67 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Berlin, 1979. Translated from the French by Marvin Jay Greenberg.

[Smi22] Alexander Smith. The distribution of ℓ^∞-selmer groups in degree ℓ twist families i. *arXiv preprint arXiv:2207.05674*, 2022.

[Smi23] Alexander Smith. The distribution of ℓ^∞-selmer groups in degree ℓ twist families ii, 2023.

[SW23] Ari Shnidman and Ariel Weiss. Rank growth of elliptic curves over n-th root extensions. *Trans. Amer. Math. Soc. Ser. B*, 10:482–506, 2023.

[Ten15] Gérald Tenenbaum. *Introduction to analytic and probabilistic number theory*, volume 163 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, third edition, 2015. Translated from the 2008 French edition by Patrick D. F. Ion.

[Š54] I. R. Šafarevič. Construction of fields of algebraic numbers with given solvable Galois group. *Izv. Akad. Nauk SSSR Ser. Mat.*, 18:525–578, 1954.

[Wri89] David J Wright. Distribution of discriminants of abelian extensions. *Proceedings of the London Mathematical Society*, 3(1):17–50, 1989.

(Pathak) Chennai Mathematical Institute, H1, SIPCOT IT Park, Kelambakkam, Siruseri, Tamil Nadu 603103, India

Email address: siddhi@cmi.ac.in

(Ray) Chennai Mathematical Institute, H1, SIPCOT IT Park, Kelambakkam, Siruseri, Tamil Nadu 603103, India

Email address: anwesh@cmi.ac.in