ON THE AVERAGE OF P-SELMER RANK IN QUADRATIC TWIST FAMILIES OF ELLIPTIC CURVES OVER FUNCTION FIELD

by

Niudun Wang

A dissertation submitted in partial fulfillment of
the requirements for the degree of

Doctor of Philosophy

(Mathematics)

at the

UNIVERSITY OF WISCONSIN–MADISON

2021

Date of final oral examination: 11/22/2021

The disertation is approved by the following members of the Final Oral Committee:

Jordan Ellenberg, Professor, Mathematics

Daniel Erman, Associate Professor, Mathematics

Shaoming Guo, Assistant Professor, Mathematics

Ananth Shankar, Assistant Professor, Mathematics

ABSTRACT

This thesis focuses on studying the rank of Selmer groups in quadratic twist families of elliptic curves over function field. Some of the results are closely related to Poonen-Rains heuristics that hypothesizes the average of Selmer ranks of elliptic curves in general.

We show in the first part that if the quadratic twist family of a given elliptic curve over $\mathbb{F}_q[t]$ with no $\mathbb{F}_q(t)$-rational p-torsion points has an element whose Neron model has a multiplication reduction away from ∞, then the average p-Selmer rank is $p+1$ in large q-limit for almost all primes p.

In the second part, we show that in the quadratic twist family of an elliptic curve over $\mathbb{F}_q[t]$ with a single point of order two that does not have a cyclic 4-isogeny defined over its two-division field, at least half of the quadratic twists have arbitrarily large 2-Selmer rank.

Acknowledgements

I would like to thank my advisor Jordan Ellenberg. Thank you for making math so fun and approachable, for always being patient with my questions, and for giving me the vision of what modern math is like which I have been curious about since I was little. Most importantly, you taught me math is everywhere and we don't have to be a mathematician to appreciate its beauty.

I would like to thank Sun Woo Park for the collaboration we had over a great chunk of this thesis, for the great time we spent together talking math and beyond. There is no way I could have pressed forward consistently without being inspired by your diligence. It is no exaggeration that I learned most math while working with you and it has been a privilege. I sincerely wish you the best in your career as you are returning to Madison next year from military service.

To Edwin, Qiao, Yeyu, and Wanlin, thank you for making my time so much more fun throughout the years. You have always been not only great friends, but also great examples. I would not have been the person I am today without your aspiration and support during hard times. If I have seen further it is by standing on the shoulders of giants.

And thank you to everyone else in Madison including Michel, Soumya, Solly, Brandon, Yu, Shuqi and many others. Those moments we had together will shine forever in memory.

Chapter 1

Poonen-Rains Heuristic

1.1 Introduction to Galois Cohomology

Let G be a topological group and M a G-module that G continuously acts on. We can define:

$$H^0(G, M) = M^G = \{m \in M : m^\sigma = m \text{ for all } \sigma \in G\}$$

A crossed homomorphism is a continuous homomorphism $f : G \longrightarrow M$ that satisfies

$$f(\sigma\tau) = f(\sigma) + f(\tau)^\tau$$

for all $\sigma, \tau \in G$.

We say that a continuous homomorphism $f : G \longrightarrow M$ is a principal crossed homomorphism if there exists some fixed $m \in M$ such that

$$f(\sigma) = m^\sigma - m$$

for all $\sigma \in G$.

We can define:

$$H^1(G, M) = \frac{\{\text{crossed homomorphisms}\}}{\{\text{principal crossed homomorphisms}\}}$$

Given such definitions, for any exact sequence of G-modules

$$0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow M_3 \longrightarrow 0,$$

it naturally induces a canonical exact sequence of cohomology groups:

$$0 \longrightarrow H^0(G, M_1) \longrightarrow H^0(G, M_2) \longrightarrow H^0(G, M_3) \longrightarrow H^1(G, M_1) \longrightarrow H^1(G, M_2) \longrightarrow H^1(G, M_3)$$

Let E be an elliptic curve defined over a global field k. For the rest of this chapter, we will fix $G = G_k = \mathrm{Gal}(\bar{k}/k)$ and $M = E(\bar{k})$.

One can show that the isogeny $[n] : E(\bar{k}) \longrightarrow E(\bar{k})$ is surjective and this gives arise an exact sequence:

$$0 \longrightarrow E(\bar{k})[n] \longrightarrow E(\bar{k}) \longrightarrow E(\bar{k}) \longrightarrow 0$$

where $E(\bar{k})[n]$ is the kernel of $[n] : E \longrightarrow E$.

Now we can take Galois Cohomology which in turn yields the long exact sequence:

$$0 \longrightarrow E(k)[n] \longrightarrow E(K) \longrightarrow E(K) \longrightarrow H^1(k, E(\bar{k})[n]) \longrightarrow H^1(k, E(\bar{k})) \longrightarrow H^1(k, E(\bar{k}))$$

where we follow the convention to denote $H^n(G_k, M)$ by $H^n(k, M)$.

From this long exact sequence in Galois cohomology one can deduce the long exact sequence:

$$0 \longrightarrow E(k)/nE(k) \longrightarrow H^1(k, E(\bar{k})[n]) \longrightarrow H^1(k, E(\bar{k}))[n] \longrightarrow 0$$

Unfortunately, $H^1(k, E(\bar{k})[n])$ does not have to be finite in general. Our goal is to replace $H^1(k, E(\bar{k})[n])$ with a group that we can show is finite and contains the image of $E(k)/nE(k)$. To this end, we will introduce Selmer groups in the next section.

1.2 Selmer groups

For a place v of k, consider E to be an elliptic curve defined over the local field K_v. We fix an extension of v to $\bar{k}$ which serves to fix an embedding $\bar{k} \subset \bar{k}_v$ and a decomposition group $G_v \subset G_{\bar{k}/k}$.

Since G_v acts on $E(\bar{k}_v)$, we have the following exact sequence:

$$0 \longrightarrow E(k_v)/nE(k_v) \longrightarrow H^1(G_v, E(\bar{k}_v)[n]) \longrightarrow H^1(G_v, E(\bar{k}_v))[n] \longrightarrow 0$$

If we compare it to the same exact sequence that we get in the previous section, we can find that the natural inclusions $G_v \subset G_{\bar{k}/k}$ and $E(\bar{k}) \subset E(\bar{k}_v)$ induces a commutative

diagram between them:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E(k)/nE(k) & \longrightarrow & H^1(k, E(\bar{k})[n]) & \longrightarrow & H^1(k, E(\bar{k}))[n] & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & E(k_v)/nE(k_v) & \longrightarrow & H^1(k_v, E(\bar{k}_v)[n]) & \longrightarrow & H^1(k_v, E(\bar{k}_v))[n] & \longrightarrow & 0 \end{array}$$

One can generalize this to all the places and get the following commutative diagram:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E(k)/nE(k) & \longrightarrow & H^1(k, E(\bar{k})[n]) & \longrightarrow & H^1(k, E(\bar{k}))[n] & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \prod\limits_{v \in M_k} E(k_v)/nE(k_v) & \longrightarrow & \prod\limits_{v \in M_k} H^1(k_v, E(\bar{k}_v)[n]) & \longrightarrow & \prod\limits_{v \in M_k} H^1(k_v, E(\bar{k}_v))[n] & \longrightarrow & 0 \end{array}$$

Our goal is to compute the image of $E(k)/nE(k)$ in the cohomology group $H^1(k, E(\bar{k})[n])$, or equivalently, to compute the kernel of the map

$$H^1(k, E(\bar{k})[n]) \longrightarrow H^1(k, E(\bar{k}))[n].$$

This problem amounts to determining whether certain homogeneous spaces possess a k-rational point which is not an easy question to answer in general. Inspired by this, to determine each local kernel

$$\ker(H^1(k_v, E(\bar{k}_v)[n]) \longrightarrow H^1(k_v, E(\bar{k}_v))[n])$$

is relatively straightforward to compute as the question is equivalent to whether a curve has a point over the complete local field k_v. There is a systematic way to check this through a finite amount of computation by Hensel's lemma. This insight leads us to define Selmer groups as follows:

Definition 1.1. *The n-Selmer group of E/K is the subgroup of $H^1(k, E(\bar{k})[n])$ defined by*

$$\begin{aligned} Sel_n(E/k) &= \{c \in H^1(k, E(\bar{k})[n]) : \forall v, c_v \text{ comes from } E(k_v)\} \\ &= ker(H^1(k, E(\bar{k})[n]) \longrightarrow \prod_v H^1(k_v, E(\bar{k}_v))). \end{aligned}$$

Similarly we define the Shafarevich-Tate group of E/k to be

$$Ш(E/k) = ker(H^1(k, E(\bar{k})) \longrightarrow \prod_v H^1(k_v, E(\bar{k}_v))).$$

Notice here the definition does not depend on our choice of extension of v to $\bar{k}$ as whether an element is in such kernel only has to do with whether the associated homogeneous space possesses k_v points. v itself has determined the embedding of k into k_v, so $\mathrm{Sel}_n(E/k)$ and $Ш(E/k)$ depend only on E and k.

Remark 1.2. *Ш gives a geometric way to measure the failure of local-global principle. We can view it as the group of homogeneous spaces for E/k that possess a k_v-rational point at all places v.*

Remark 1.3. *It is conjectured that Ш is finite and there is conjectured to be a precise relationship between the rank of $E(k)$ and the order of Ш.*

One can effectively compute Selmer groups given explicit elliptic curves. In fact we have the following theorem:

Theorem 1.4. [Sil91, Section VIII, Theorem 4.2] *There is an exact sequence*

$$0 \longrightarrow E(k)/nE(k) \longrightarrow Sel_n(E/k) \longrightarrow Ш(E/k)[n] \longrightarrow 0$$

and the Selmer group $Sel_n(E/k)$ is finite.

This directly shows that $E(k)/nE(k)$ is finite for any integer n which is the weak Mordell-Weil theorem. We will see in the next section what the distribution of Selmer groups is expected to be in the family of elliptic curves.

1.3 Poonen-Rains Heuristic

We have defined two maps in section 1.2, which are

$$\alpha : \prod_v E(k_v)/nE(k_v) \longrightarrow \prod_v H^1(k_v, E(\bar{k}_v)[n])$$

and

$$\beta : H^1(k, E(\bar{k})[n]) \longrightarrow \prod_v H^1(k_v, E(\bar{k}_v)[n]).$$

Recall that Selmer group is defined to be $\mathrm{Sel}_n(E) := \beta^{-1}(\mathrm{im}\ \alpha) \subset H^1(k, E(\bar{k})[n])$.

There is a natural way that one can define a map of sets (we choose $k = \mathbb{Q}$ in this section for example):

$$q_v : H^1(\mathbb{Q}_v, E) \longrightarrow H^2(\mathbb{Q}_v, \mathcal{G}_m) \longrightarrow \mathbb{Q}/\mathbb{Z}.$$

One can show that q_v is a quadratic form such that $q_v(x+y) - q_v(x) - q_v(y)$ is bi-addictive [JGZ74, page 415-419]. In addition to that, we have $q_v|W_v = 0$ where W_v is defined to be the image of $E(\mathbb{Q}_v)/nE(\mathbb{Q}_v) \longrightarrow H^1(\mathbb{Q}_v, E[n])$.

Notice for $\theta = (\theta_v)_v \in \prod_v H^1(\mathbb{Q}_v, E[n])$, we have $\theta_v \in W_v$ for all but finitely many places v and hence $q_v(\theta_v) = 0$. This allows us to generalize the quadratic form to $\prod_v H^1(\mathbb{Q}_v, E[n]) \longrightarrow \mathbb{Q}/\mathbb{Z}$ by defining:

$$Q(\theta) := \Sigma_v q_v(\theta_v).$$

One can make the following observation in regards to Selmer groups:

Theorem 1.5. [PR12, Theorem 4.14(a)] *Each of im α and im β is a maximal isotropic subgroup of $\prod_v H^1(\mathbb{Q}_v, E[n])$ with respect to Q.*

We have $\beta(\mathrm{Sel}_n E) = (\mathrm{im}\ \alpha) \cap (\mathrm{im}\ \beta)$ and one can also show that in the case where n is a prime number, β is injective. This implies that when n is a prime which is the case that we will study throughout this thesis, $\mathrm{Sel}_n(E)$ is isomorphic to an intersection of maximal isotropic subgroups of $\prod_v H^1(\mathbb{Q}_v, E[n])$.

This leads to the heuristic to model Selmer groups by choosing random maximal isotropic subspaces in an infinite-dimensional quadratic space conversely and intersecting them to obtain a space whose distribution is the same as Selmer groups. We will not elaborate the detailed construction here.

The average size of n-Selmer groups has the following conjecture:

Conjecture 1.6. [PR12, Conjecture 1.1] *The average size of n-Selmer groups in the family of elliptic curves ordered by height is given by the sum of the divisors of n.*

We will address some special cases that center around this conjecture in the next section.

1.4 Outline of this thesis

The new work for this thesis begins with a setting similar to the Poonen-Rains heuristic where we consider the quadratic twist family of a given elliptic curve defined over function field. We show in Chapter 2 that the large q-limit of Selmer groups in such family agrees with prior expectation. This is a joint work with Sun Woo Park.

In Chapter 3, we switch gear to show that although this heuristic is expected to hold for the entire family of elliptic curves, it is not necessarily true unconditionally for all quadratic twist families. In particular, we prove that for an elliptic curve with certain properties, the distribution of Selmer rank in its quadratic twist family conform to normal distribution. This is an evidence that the size of Selmer group for an arbitrary elliptic curve is still quite random and yet to be universally predicted.

Chapter 2

The case of large q-limit

2.1 Introduction

Let $\mathbb{F}_q$ be a finite field with $\mathrm{Char}(\mathbb{F}_q)$ relatively prime to 2 and 3. Let $C = \mathbb{P}^1/\mathbb{F}_q$ and $K = \mathbb{F}_q(C) = \mathbb{F}_q(t)$. Say $E : y^2 = x^3 + A(t)x + B(t)$ is a non-isotrivial elliptic curve defined over $\mathbb{F}_q[t]$. Define the canonical (naive) height of the elliptic curve as follows, where E' is any elliptic curve isomorphic to E of the form $y^2 = x^3 + C(t)x + D(t)$.

$$h(E) := \inf_{E' \cong E} (\max\{3 \deg C, 2 \deg D\})$$

Let E_f be the quadratic twist of E by square-free polynomial $f(t) \in \mathbb{F}_q[t]$.

$$E_f : f(t)y^2 = x^3 + A(t)X + B(t)$$

Let $M(n, q)$ be the set of square-free polynomials over $\mathbb{F}_q$ such that $h(E_f) \leq n$.

Poonen-Rains heuristic shows that the average p-Selmer rank of elliptic curves over a global field k is p+1(see [PR12].). It is natural to ask whether the same heuristic is reasonable for the family of quadratic twists of a fixed elliptic curve. We denote by $\mathbb{E}_{n,p}$ the average p-Selmer rank over those in the family of quadratic twists with canonical height at most n, namely:

$$\mathbb{E}_{n,p} = \frac{\sum_{f \in M(n,q)} |\mathrm{Sel}_p E_f|}{|M(n, q)|}$$

In this paper, we show that under certain assumption on the quadratic twist family of the fixed elliptic curve E, the average size of p-Selmer groups is $p + 1$ in large q limit. In particular, we can assume for some large enough q such that the discriminant Δ_E of E splits

in $\mathbb{F}_q[t]$, there exists a quadratic twist E_0 of E with minimal height among the quadratic twist family.

Theorem 2.1. *Let E be an elliptic curve defined over $K = \mathbb{F}_q(C) = \mathbb{F}_q(t)$ such that E has no $\mathbb{F}_q(t)$-rational p-torsion points, and there exists at least one quadratic twist of E whose Néron model admits a multiplicative reduction away from ∞. Let E_0 be the quadratic twist of E with minimal height among the family of quadratic twists of E. Then for all primes $p \geq 15$, and coprime to q and all local Tamagawa factors of E_0, we have the following equation.*

$$\lim_{n\to\infty}\lim_{q\to\infty}\mathbb{E}_{n,p} = \lim_{n\to\infty}\lim_{q\to\infty}\frac{\sum_{f\in M(n,q)}|\mathrm{Sel}_p E_f|}{|M(n,q)|} = p+1$$

Remark 2.2. *The main theorem shows that for all but finitely many primes p, the average p-Selmer rank in the large q-limit over the family of quadratic twists of E is $p+1$.*

Remark 2.3. *Let $f \in M(n,q)$ be any square free polynomial of degree n over $\mathbb{F}_q$. The condition that $p \geq 15$ guarantees that E_f has no $\mathbb{F}_q(t)$-rational p-torsion points, see Theorem 5.1 of* [CP80] *for further details. Furthermore, the Galois group $\mathrm{Gal}(K(E_f[p])/K)$ contains the special linear group $SL_2(\mathbb{F}_p)$, which is stated in* [CH05, Theorem 1.1] *and Theorem 3.6 of this paper.*

Remark 2.4. *While writing the paper, we learned the contemporaneous results from Aaron Landesman on a similar problem. Given a universal family of elliptic curves over $\mathbb{F}_q[t]$ with q coprime to $6n$, the geometric average size of n-Selmer group of the universal family is equal to sum of divisors of n as $q \to \infty$. We refer to* [Lan21] *for more details. The large q-limit of the probability distribution of n-Selmer groups over the universal family of elliptic curves can also be found in* [FLR20].

In subsequent sections, we will calculate $\lim_{n\to\infty}\lim_{q\to\infty}\mathbb{E}_{n,k,p}$ as follows. Fix an elliptic curve E over $\mathbb{F}_q[t]$. Let $F_{d,E}$ be the set of square-free polynomials f of degree d over $\bar{\mathbb{F}}_q$ such that f is coprime to Δ_E, the discriminant of E. Chris Hall's construction of étale $\mathbb{F}_l$-lisse sheaf over $F_{d,E}$ gives the average size of $\mathrm{Sel}_p(E_f)$ for a subfamily of quadratic twists of E. We then order the family of quadratic twists of E by the canonical height $h(E_f)$ which enables us to calculate the average size of $\mathrm{Sel}_p(E_f)$ in large q-limit.

2.2 Monodromy Group

In this section, we briefly discuss the main machinery used to prove Theorem 1.1. This section follows closely to chapter 2 and 3 of [Ell14]. Throughout this paper, we denote by $X_{\bar{\mathbb{F}}_q}$ the base change $X \times_{\mathbb{F}_q} \bar{\mathbb{F}}_q$ where X is a scheme over $\mathbb{F}_q$.

We start with a brief exposition on the moduli space of a family of quadratic twists of E by polynomials $g \in \mathbb{F}_q[t]$ of degree n such that $(g, \Delta_E) = 1$. A polynomial $g(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n$ of degree n corresponds to a point in the affine space $\mathbb{A}^{n+1}$ with coordinates $(a_0, a_1, a_2, \ldots, a_n)$. Note that the square-free polynomials are parameterized by the set of points on $\mathbb{A}^{n+1}$ where $\mathrm{Disc}(g)$ does not vanish, while $(g, \Delta_E) = 1$ amounts to $(a_0, a_1, a_2, \ldots, a_n)$ not on the zero locus given by the resultant of g and Δ_E. Thus those square free polynomials $g \in \mathbb{F}_q[t]$ with $(g, \Delta_E) = 1$ are parameterized by an open subscheme of $\mathbb{A}^{n+1}$, denoted by F_n. It is reasonable to expect that it suffices to compute the average p-Selmer rank on the elliptic curves parameterized by the open subscheme F_n. We will explain in later sections how we can bound the average p-Selmer rank on those quadratic twists parametrized by the complement of F_n.

Suppose there exists an étale cover $X \to F_n$ such that the number of $\mathbb{F}_q$-points on the geometric fiber of X at $f \in F_n(\mathbb{F}_q)$ equals to the size of $\mathrm{Sel}_p E_f$. Then we have the following equation.

$$|X(\mathbb{F}_q)| = \sum_{f \in F_n(\mathbb{F}_q)} |\mathrm{Sel}_p E_f|$$

On the other hand, the Grothendieck-Lefschetz trace formula gives an explicit equation of the number of $\mathbb{F}_q$-points on $X_{\bar{\mathbb{F}}_q}$([Mil13].)

$$|X(\mathbb{F}_q)| = \sum_i (-1)^i \mathrm{Tr}\ \mathrm{Frob}_q \mid \mathrm{H}^i_{\acute{e}t;c}(X_{\bar{\mathbb{F}}_q}, \mathbb{Q}_l)|$$

F_n is an open subscheme of $\mathbb{A}^{n+1}$ implies that $|F_n(\mathbb{F}_q)| = q^{n+1} - \mathrm{O}(q^n)$. The leading term of $F_n(\mathbb{F}_q)$ is q^{n+1}. Hence, computing the average size of Sel_p in large q-limit amounts to computing the following equation.

$$\lim_{q\to\infty} \frac{\sum_{f\in F_n(\mathbb{F}_q)} |\mathrm{Sel}_p E_f|}{|F_n(\mathbb{F}_q)|} = \lim_{q\to\infty} q^{-(n+1)} |X(\mathbb{F}_q)|$$

The Weil bounds imply that the eigenvalues of the Frobenius action Frob_q on $\mathrm{H}^i_{\acute{e}t;c}(X_{\bar{\mathbb{F}}_q};\mathbb{Q}_l)$ have absolute value bounded by $q^{n+1-\frac{i}{2}}$. Thus for a fixed n, if q becomes sufficiently large, any cohomology term other than $\mathrm{H}^0_{\acute{e}t;c}(X_{\bar{\mathbb{F}}_q};\mathbb{Q}_l)$ vanishes. Note that $\mathrm{H}^0_{\acute{e}t;c}(X_{\bar{\mathbb{F}}_q};\mathbb{Q}_l)$ is the $\mathbb{Q}_l$ vector space spanned by the irreducible components of $X_{\bar{\mathbb{F}}_q}$. Hence, the following observation holds.

$$\lim_{q\to\infty} q^{-(n+1)} |X(\mathbb{F}_q)| = \#\text{ of geometric irreducible components of } X \text{ rational over } \mathbb{F}_q \quad (2.2.1)$$

Let $f \in F_n$ be a fixed basepoint. we have the following short exact sequence.

$$1 \longrightarrow \pi_1((F_n)_{\bar{\mathbb{F}}_q}, f) \longrightarrow \pi_1(F_n, f) \longrightarrow \mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q) \longrightarrow 1$$

For any $f \in F_n$, the geometric fiber of X at f is an $\mathbb{F}_p$-vector space X_f. Observe that $\pi_1(F_n, f)$ acts linearly on X_f. Hence we can define the monodromy group of the cover $X \to F_n$ as the image of $\pi_1(F_n, f)$ in $\mathrm{GL}(X_f)$ and the geometric monodromy group as the image of $\pi_1((F_n)_{\bar{\mathbb{F}}_q}, f)$. Denote by Γ the monodromy group, and denote by Γ_0 the geometric monodromy group. This gives us another short exact sequence, where $[q]$ corresponds to the class in Γ/Γ_0 corresponding to the image of the Frobenius $\mathrm{Frob}_q \in \mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$, and $[q]^{\mathbb{Z}}$ corresponds to a subgroup of Γ/Γ_0 generated by $[q]$.

$$1 \longrightarrow \Gamma_0 \longrightarrow \Gamma \longrightarrow [q]^{\mathbb{Z}} \longrightarrow 1$$

We state and prove the following observations, which gives a geometric interpretation of equation (2.1).

Lemma 2.5. *The geometric irreducible components of X are in bijection with the orbits of the geometric monodromy group on X_f.*

Proof. Note that $X_{\bar{\mathbb{F}}_q}$ is étale over $(F_n)_{\bar{\mathbb{F}}_q}$ because X is étale over F_n. Hence, $\pi_1((F_n)_{\bar{\mathbb{F}}_q})$ acts on $X_{\bar{\mathbb{F}}_q}$. The group action preserves each irreducible component of $X_{\bar{\mathbb{F}}_q}$ since each component is étale over $(F_n)_{\bar{\mathbb{F}}_q}$, hence preserved by the functoriality of π_1. Therefore, under the action of $\pi_1((F_n)_{\bar{\mathbb{F}}_q})$, each orbit of the geometric monodromy group on X_f would lie inside one irreducible component of $X_{\bar{\mathbb{F}}_q}$. On the other hand, $\pi_1(X_{\bar{\mathbb{F}}_q})$ acts transitively on the geometric fibers of f within an irreducible geometric component, which yields the bijection. □

Lemma 2.6. *The action of the Frobenius on the geometric components is given by the action of* $[q]$ *on the orbits of* Γ_0.

This comes directly from the bijection between the geometric irreducible components of X and the orbits of Γ_0. Therefore, in order to compute the number of geometrically irreducible components of X, it suffices to understand the geometric monodromy group Γ_0 and compute the number of Γ_0-orbits on X_f which are fixed by $[q]$. Therefore, equation (2.1) can be rewritten as follows.

$$\lim_{q\to\infty} q^{-(n+1)}|X(\mathbb{F}_q)| = \#\text{ of orbits of } \Gamma_0 \text{ fixed by } [q] \tag{2.2.2}$$

2.3 Construction of Moduli Space

2.3.1 Cohomology Groups of Néron Models

In this subsection, we prove several claims which will help us with constructing the desired moduli space discussed in remark 2.3.

Let q be a power of prime $q = q_0^k$ such that q_0 is not divisible by 2 and 3. Fix an algebraic closure $\mathbb{F}_q \to \bar{\mathbb{F}}_q$. Let $C/\mathbb{F}_q = \mathbb{P}^1/\mathbb{F}_q$, and let $K = \mathbb{F}_q(C) = \mathbb{F}_q(t)$ be its function field. Fix an elliptic curve E over K, and let E_f be the quadratic twist of the elliptic curve by $f \in \mathrm{Conf}^n(\mathbb{F}_q)$. Let $\mathcal{E} \to C$ be the Néron model for the elliptic curve E. For any prime p that is invertible in K, the multiplication by p map on $E_f(K)$ extends uniquely to an isogeny $\times p : \mathcal{E} \to \mathcal{E}$. Define $\mathcal{E}_p$ to be the kernel of $\times p$.

We state a result from [Ces16], which states that the first cohomology group of $\mathcal{E}_p$ and Sel_p are isomorphic under certain arithmetic conditions. First, we state the following lemma from [Ces16, Appendix B].

Lemma 2.7. *Let S be a connected Noetherian normal scheme of dimension ≤ 1. Let $\bar{K}$ be the function field of S, and for every point $s \in S$, let $k(s)$ be the residue field of s. Let $A \to \mathrm{Spec}\bar{K}$ and $B \to \mathrm{Spec}\bar{K}$ be abelian varieties, and let $\mathcal{A} \to S$ and $\mathcal{B} \to S$ be their Néron models. Suppose $\phi : A \to B$ is a $\bar{K}$-isogeny of abelian varieties. Denote by $\tilde{\phi} : \mathcal{A} \to \mathcal{B}$ the map induced on Néron models over S. If $\mathcal{A}$ has semiabelian reduction at all the nongeneric $s \in S$ with $\mathrm{Char}(k(s))|\deg\phi$, then $\tilde{\phi} : \mathcal{A} \to \mathcal{B}$ is flat.*

Proof. See [Ces16, Lemma B.4]. □

In particular, the lemma above shows that the map $\times p : \mathcal{E} \to \mathcal{E}$ is flat if q is coprime to p. Using this implication, we can state the following application from [Ces16, Proposition 5.4].

Theorem 2.8. *Let $\phi : A \to B$ be a morphism of abelian varieties. Let $\mathcal{A}$ and $\mathcal{B}$ be their Néron models. Denote by $A[\phi]$ the kernel of $\phi : A \to B$, and denote by $\mathcal{A}[\phi]$ the kernel of $\phi : \mathcal{A} \to \mathcal{B}$. Let $\mathrm{Sel}_\phi A$ be the ϕ-Selmer group of A. Suppose the morphism $\phi : \mathcal{A} \to \mathcal{B}$ is flat. If $\deg\phi$ is coprime to any local Tamagawa factors of A and B, and 2 does not divide $\deg\phi$, then the following equation holds inside $\mathrm{H}^1_{\mathrm{fppf}}(K, A[\phi])$.*

$$\mathrm{H}^1_{\mathrm{fppf}}(S, \mathcal{A}[\phi]) = \mathrm{Sel}_\phi A$$

Proof. See [Ces16, Propostion 5.4]. □

More specifically, the theorem above implies that when p is coprime to 2, q, and the local Tamagawa factors of E, then there exists an isomorphism between $\mathrm{H}^1_{\mathrm{fppf}}(C, \mathcal{E}_p)$ and $\mathrm{Sel}_p E$.

In fact, under certain conditions on E, we can extend the results of Theorem 3.2 to the family of quadratic twists of E. Let E_f be the quadratic twist of the elliptic curve by square-free polynomials $f \in \mathbb{F}_q[t]$. Denote by $\mathcal{E}_f \to C$ the Néron model for the elliptic curve E_f. Let $\mathcal{E}_{f,p}$ be the kernel of multiplication by p map over $\mathcal{E}_f$.

Corollary 2.9. *Let $E/K : y^2 = x^3+Ax+B$ be an elliptic curve, and let Δ_E be the discriminant of E. Suppose that no prime factors π of Δ_E satisfy the condition that $\pi^2|A$ and $\pi^3|B$. Let p be a prime such that p is coprime to $2, 3, q_0$ and all the local Tamagawa factors of E. Then the following isomorphism holds for any square-free polynomial $f \in \mathbb{F}_q[t]$.*

$$\mathrm{H}^1_{\mathrm{fppf}}(C, \mathcal{E}_{f,p}) = \mathrm{Sel}_p E_f$$

Proof. For an explicit calculation of local Tamagawa factors using Tate's algorithm, see [Sil91, Chapater 4, Section 9]. Say $f = (\pi_1 \dots \pi_s)g$, where $J = \{\pi_1 \dots \pi_s\}$ are prime factors of Δ_E and $(g, \Delta_E) = 1$, We first note that the conditions on E imply that the discriminant of the twist E_f is equal to $f^6\Delta_E$. Tate's algorithm shows E_f has additive reduction on all primes π dividing g. Therefore, all local Tamagawa factors arising from such π's are at most 4.

On the other hand, the additive reductions $\pi_i \in J$ of E will stay as additive reductions of E_f, while the multiplicative reductions $\pi_j \in J$ will all become additive reductions of E_f. For all the other primes $\rho|\Delta_E$ but not in J, $v_\rho(\Delta_E)$ and $v_\rho(\Delta_{E_f})$ are the same. Therefore, for any $\rho|\Delta_E$, no matter weather ρ divides f or not, we will have the local Tamagawa factor of E_f at ρ either equals to the local Tamagawa factor of E or equals to 1,2,3. Then we can apply theorem 3.2. to E_f.

□

Remark 2.10. *For such an elliptic curve E in the above Corollary, we can actually conclude that if the Néron model of E itself has no multiplicative reduction away from ∞, there is no quadratic twists of E whose Néron model admits a multiplicative reduction away from ∞. This follows exactly from the fact that additive reductions $\pi_i \in J$ of E will stay as additive reductions of E_f.*

The theorem hence implies that for all but finitely many primes p, the following isomorphism holds.

$$\mathrm{H}^1_{\mathrm{fppf}}(C, \mathcal{E}_{f,p}) = \mathrm{Sel}_p E_f$$

Since $\mathcal{E}_{f,p}$ is a smooth commutative group scheme, we know that $\mathrm{H}^1_{\mathrm{fppf}}(C, \mathcal{E}_{f,p})$ is isomorphic to $\mathrm{H}^1_{\acute{e}t}(C, \mathcal{E}_{f,p})$. (See [PR12, Remark 6.6.3])

We now examine whether there is a way to explicitly compute the size of $\mathrm{H}^1_{\acute{e}t}(C, \mathcal{E}_{f,p})$. Chris Hall gives an explicit computation of the étale cohomology groups of $\mathcal{E}_{f,p}$ over $C_{\bar{\mathbb{F}}_q}$ under certain conditions on the size of the Galois group $\mathrm{Gal}(K(E[p])/K)$.

Definition 2.11. *Let E/K be an elliptic curve. The geometric Galois group H_p is the subgroup of the Galois group $\mathrm{Gal}(K(E[p])/K)$ whose fixed field is $(K(E[p]) \cap \bar{\mathbb{F}}_q)/K$ given by adjoining a primitive pth root of unity. We say that E has big monodromy at p if the geometric Galois group contains $\mathrm{SL}_2(\mathbb{F}_p)$.*

In fact, for any prime $p \geq 5$, any twist E_f has big monodromy at p if and only if E has big monodromy at p. This is because $\mathrm{SL}_2(\mathbb{F}_p)$ does not have index 2 subgroups, so $K(E_f[p])$ and $k(\sqrt{f})$ are geometrically disjoint extensions of K. We note that E having no $\mathbb{F}_q(t)$-rational p-torsion points is sufficient for E having big monodromy at p.

Theorem 2.12. *Let $C/\mathbb{F}_q$ be a proper smooth geometrically connected curve, and let K be its function field. Let E/K be a non-isotrivial elliptic curve. Then there exists a constant $c(K)$ such that E has big monodromy at p for any $p \geq c(K)$ and p coprime to $\mathrm{Char}(K)$. The constant $c(K)$ is defined as follows.*

$$c(K) := 2 + \max\{l \mid l \text{ is prime}, \frac{1}{12}(l - (6 + 3e_2 + 4e_3)) \leq \mathrm{genus}(C)\}$$

Here, e_2 and e_3 are constants defined as follows.

$$e_2 = \begin{cases} 1 & \text{if } l \equiv 1 \bmod 4 \\ -1 & \text{otherwise} \end{cases}$$

$$e_3 = \begin{cases} 1 & \text{if } l \equiv 1 \bmod 3 \\ -1 & \text{otherwise} \end{cases}$$

Proof. See [CH05, Theorem 1.1]. □

In particular, let $C = \mathbb{P}^1$ and K be the function field of C. Fix a non-isotrivial elliptic curve E/K. Let $\{E_f\}$ be the family of quadratic twists of E, where f is any square-free polynomial over $\mathbb{F}_q$. The theorem above implies that E/K has big monodromy at p for any prime $p \geq 15$ and coprime to q. Hence, for any prime $p \geq 15$ and coprime to q, the twist E_f/K also has big monodromy at p. Under the aforementioned conditions on p, we can give an explicit calculation of the étale cohomology group $\mathrm{H}^1(C_{\mathbb{F}_q}, \mathcal{E}_{f,p})$ for any E_f.

Lemma 2.13. *Let $C/\mathbb{F}_q$ be a proper smooth geometrically connected curve, and let K be its function field. Fix an elliptic curve E/K. Let p be a prime such that E has big monodromy at p. In particular, we further assume that E has no $\mathbb{F}_q(t)$-rational p-torsion points. Then for any square-free polynomial f over $\mathbb{F}_q$, the étale cohomology groups of $\mathcal{E}_{f,p}$ over $C_{\bar{\mathbb{F}}_q}$ are $\mathbb{F}_p$-vector spaces with the following dimensions.*

$$\dim_{\mathbb{F}_p}(\mathrm{H}^i_{\acute{e}t}(C_{\bar{\mathbb{F}}_q}, \mathcal{E}_{f,p})) = \begin{cases} \deg(M_f) + 2\deg(A_f) - 4(\mathrm{genus}(C) - 1) & \text{if } i = 1 \\ 0 & \text{otherwise} \end{cases}$$

Here, M_f and A_f are the divisors of multiplicative and additive reduction of $\mathcal{E}_{f,p} \to C$.

Proof. See [CH05, Lemma 6.2]. □

In particular, if $C = \mathbb{P}^1$, then the dimension of $\mathrm{H}^1(C_{\mathbb{F}_q}, \mathcal{E}_{f,p})$ as an $\mathbb{F}_p$-vector space is $\deg(M_f) + 2\deg(A_f) + 4$ for any twist E_f.

Remark 2.14. *The Weil pairing on $E_f[p]$ induces a non-degenerate skew-symmetric pairing on $\mathcal{E}_{f,p}$. Hence the Weil pairing induces a non-degenerate symmetric pairing on $\mathrm{H}^1_{\acute{e}t}(C_{\bar{\mathbb{F}}_q}, \mathcal{E}_{f,p})$ as follows.*

$$\begin{aligned} \mathrm{H}^1_{\acute{e}t}(C_{\bar{\mathbb{F}}_q}, \mathcal{E}_{f,p}) \times \mathrm{H}^1_{\acute{e}t}(C_{\bar{\mathbb{F}}_q}, \mathcal{E}_{f,p}) &\to H^2_{\acute{e}t}(C_{\bar{\mathbb{F}}_q}, \mathcal{E}_{f,p} \otimes \mathcal{E}_{f,p}) \\ &\to H^2_{\acute{e}t}(C_{\bar{\mathbb{F}}_q}, \mathbb{F}_p(1)) \end{aligned}$$

The first map comes from the cup product of cohomology classes and Poincaré duality, while the second map comes from the induced Weil pairing $\mathcal{E}_{f,p} \times \mathcal{E}_{f,p} \to \mathbb{F}_p(1)$. Note that the

following isomorphism holds (See [Mil13, Chapter 14]*).*

$$H^2_{ét}(C_{\bar{\mathbb{F}}_q}, \mathbb{F}_p(1)) \cong \mathbb{F}_p$$

Therefore, the Weil pairing on $E_f[p]$ induces a non-degenerate symmetric bilinear pairing of first étale cohomology groups.

$$\mathrm{H}^1_{ét}(C_{\bar{\mathbb{F}}_q}, \mathcal{E}_{f,p}) \times \mathrm{H}^1_{ét}(C_{\bar{\mathbb{F}}_q}, \mathcal{E}_{f,p}) \to \mathbb{F}_p$$

Using the above lemma and the Leray spectral sequence, we can derive a relation between étale cohomology groups of $\mathcal{E}_{f,p}$ over C and those over $C_{\bar{\mathbb{F}}_q}$.

Theorem 2.15 (Leray Spectral Sequence)**.** *Let $\phi : Y \to X$ be a morphism of schemes, and let $\mathcal{F}$ be a sheaf on Y_{et}. Then there exists the following spectral sequence.*

$$E^2_{r,s} = \mathrm{H}^r_{ét}(X, R^s\phi_*\mathcal{F}) \Rightarrow \mathrm{H}^{r+s}_{ét}(Y, \mathcal{F})$$

Proof. See [Mil13, Theorem 12.7]. □

Lemma 2.16. *Fix an elliptic curve $E/K : y^2 = x^3 + Ax + B$ such that no prime factors π of Δ_E satisfy the condition that $\pi^2 | A$ and $\pi^3 | B$. Suppose p is a prime satisfying these conditions.*

1. *$p \geq 15$*
2. *$(p, \mathrm{Char}(K)) = 1$*
3. *p does not divide any local Tamagawa factors of E.*

Then for any quadratic twist E_f, the following isomorphism exists.

$$H^1_{ét}(C_{\bar{\mathbb{F}}_q}, \mathcal{E}_{f,p})^{\mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)} \cong \mathrm{Sel}_p E_f$$

Proof. Consider the morphism of schemes $\phi : C \to \mathrm{Spec}(\mathbb{F}_q)$. By the Leray spectral sequence, the following spectral sequence exists.

$$E^2_{r,s} = \mathrm{H}^r(\mathbb{F}_q, \mathrm{H}^s_{ét}(C_{\bar{\mathbb{F}}_q}, \mathcal{E}_{f,p})) \Rightarrow \mathrm{H}^{r+s}_{ét}(C, \mathcal{E}_{f,p})$$

By lemma 3.7, the cohomology group $\mathrm{H}^r(\mathbb{F}_q, \mathrm{H}^s_{\acute{e}t}(C_{\bar{\mathbb{F}}_q}, \mathcal{E}_{f,p}))$ is trivial whenever $s \neq 1$. Hence, the entries of the E^2 page of the spectral sequence are given as follows.

r	0	$\mathrm{H}^r(\mathbb{F}_q, \mathrm{H}^1_{\acute{e}t}(C_{\bar{\mathbb{F}}_q}, \mathcal{E}_{f,p}))$	0	$\cdots$	0
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
2	0	$\mathrm{H}^2(\mathbb{F}_q, \mathrm{H}^1_{\acute{e}t}(C_{\bar{\mathbb{F}}_q}, \mathcal{E}_{f,p}))$	0	$\cdots$	0
1	0	$\mathrm{H}^1(\mathbb{F}_q, \mathrm{H}^1_{\acute{e}t}(C_{\bar{\mathbb{F}}_q}, \mathcal{E}_{f,p}))$	0	$\cdots$	0
0	0	$\mathrm{H}^0(\mathbb{F}_q, \mathrm{H}^1_{\acute{e}t}(C_{\bar{\mathbb{F}}_q}, \mathcal{E}_{f,p}))$	0	$\cdots$	0
	0	1	2	$\cdots$	s

The Leray spectral sequence implies the following isomorphism.

$$\mathrm{H}^0(\mathbb{F}_q, \mathrm{H}^1_{\acute{e}t}(C_{\bar{\mathbb{F}}_q}, \mathcal{E}_{f,p})) \cong \mathrm{H}^1_{\acute{e}t}(C, \mathcal{E}_{f,p})$$

Recall the following isomorphism.

$$\mathrm{H}^1_{\acute{e}t}(C, \mathcal{E}_{f,p}) \cong \mathrm{H}^1_{\mathrm{fppf}}(C, \mathcal{E}_{f,p})$$

Note that the 0-th cohomology group is precisely the fixed subgroup of $\mathrm{H}^1_{\acute{e}t}(C_{\bar{\mathbb{F}}_q}, \mathcal{E}_{f,p})$ by $\mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$.

$$\mathrm{H}^1_{\acute{e}t}(C_{\bar{\mathbb{F}}_q}, \mathcal{E}_{f,p})^{\mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)} \cong \mathrm{H}^0(\mathbb{F}_q, \mathrm{H}^1_{\acute{e}t}(C_{\bar{\mathbb{F}}_q}, \mathcal{E}_{f,p}))$$

Corollary 3.3 implies the following isomorphism holds for all but finitely many p.

$$\mathrm{H}^1_{\mathrm{fppf}}(C, \mathcal{E}_{f,p}) \cong \mathrm{Sel}_p E_f$$

Hence, for all but finitely many p, the following isomorphism holds.

$$\mathrm{H}^1_{\acute{e}t}(C_{\bar{\mathbb{F}}_q}, \mathcal{E}_{f,p})^{\mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)} \cong \mathrm{Sel}_p E_f$$

□

2.3.2 Construction of Étale $\mathbb{F}_p$-lisse Sheaf

In this subsection, we follow through Chris Hall's construction of étale $\mathbb{F}_p$-lisse sheaf over a subset of square-free polynomials f of fixed degree over $\mathbb{F}_q$. The construction will help us calculate the average size of $\mathrm{Sel}_p(E_f)$ for a subfamily of quadratic twists of E.

As before, let $C = \mathbb{P}^1$ over $\mathbb{F}_q$, and let K be the function field of C. Fix a non-isotrivial elliptic curve $E/K : y^2 = x^3 + Ax + B$ that has no $\mathbb{F}_q(t)$-rational p-torsion points. We recall the construction of the space F_n over $\bar{\mathbb{F}}_q$, as mentioned in section 2.

$$F_n = \{f \in \bar{\mathbb{F}}_q[t] \mid f \text{ is square-free}, \deg f = n, (f, \Delta_E) = 1\}$$

As constructed in [CH05, Chapter 5.3], consider the étale $\mathbb{F}_p$-lisse sheaf $\tau_{n,p,E} \to F_n$ whose geometric fiber over $f \in F_n(\mathbb{F}_q)$ is $\mathrm{H}^1(\mathrm{Conf}^n_{\bar{\mathbb{F}}_q}, \mathcal{E}_{f,p})$. Note that Chris Hall's construction of $\tau_{n,p,E}$ is an $\mathbb{F}_p$-analogue of Katz's construction of étale $\bar{\mathbb{Q}}_p$-lisse sheaves using middle convolutions. We refer to [Kat98, Proposition 5.2.1] for a detailed explanation on the construction of the étale $\bar{\mathbb{Q}}_p$-lisse sheaves.

We state the following theorem by Chris Hall, which gives an explicit computation of the geometric monodromy group of $\tau_{n,p,E} \to F_n$.

Theorem 2.17. *Let E be an elliptic curve over K such that there exists at least one quadratic twist of E whose Néron model admits a multiplicative reduction away from ∞. Let p be a prime such that E has big monodromy at p, i.e. $p \geq 15$. Suppose further that E has no $\mathbb{F}_q(t)$-rational p-torsion points. Let $O(\mathrm{H}^1_{\acute{e}t}(\mathrm{Conf}^n_{\bar{\mathbb{F}}_q}, \mathcal{E}_{f,p}))$ be the orthogonal group of $\mathrm{H}^1_{\acute{e}t}(\mathrm{Conf}^n_{\bar{\mathbb{F}}_q}, \mathcal{E}_{f,p})$ which preserves the non-degenerate symmetric bilinear pairing μ. (See Remark 3.7 for the construction of μ.)*

Then the geometric monodromy group of $\tau_{n,p,E} \to F_n$ is isomorphic to a subgroup of the orthogonal group $O(\mathrm{H}^1_{\acute{e}t}(\mathrm{Conf}^n_{\bar{\mathbb{F}}_q}, \mathcal{E}_{f,p}))$ of index at most 2 and is not isomorphic to $SO(\mathrm{H}^1_{\acute{e}t}(\mathrm{Conf}^n_{\bar{\mathbb{F}}_q}, \mathcal{E}_{f,p}))$.

Proof. See [CH05, Theorem 5.3]. □

Note that the commutator subgroup of $O(\mathrm{H}^1_{\acute{e}t}(\mathrm{Conf}^n_{\bar{\mathbb{F}}_q}, \mathcal{E}_{f,p}))$ is of index 4. Hence, in order to understand the number of orbits of the desired geometric monodromy group, it suffices to understand the number of orbits of both $O(\mathrm{H}^1_{\acute{e}t}(\mathrm{Conf}^n_{\bar{\mathbb{F}}_q}, \mathcal{E}_{f,p}))$ and its commutator subgroup. We finish this section with the following lemma, which describes the number of the orbits of the aforementioned two groups.

Lemma 2.18. *Let V be an $\mathbb{F}_p$-vector space of dimension d where $\mathrm{char}(\mathbb{F}_p) \neq 2$. Given a non-degenerate symmetric bilinear pairing $\mu : V \times V \to \mathbb{F}_p$, let $O(V)$ be the orthogonal group of V. Then the number of orbits of $O(V)$ is $p+1$, and the number of orbits of the commutator subgroup $[O(V), O(V)]$ is $p+1$ if $d \geq 5$.*

Proof. We first show that the number of orbits of $O(V)$ on V is $p+1$ for any d. It suffices to show that the orthogonal group acts transitively on the set of nonzero vectors of a given norm. Suppose $v, w \in V$ are two non-zero vectors of the same norm. Then there exists an isometry $\phi : Span(v) \to Span(w)$ given by $v \mapsto w$. By Witt's Theorem, ϕ extends to an isometry $\tilde{\phi} : V \to V$, which proves the claim. Note that the orthogonal group has 1 orbit on the set of vectors of non-zero norm, and 2 orbits on the set of vectors norm zero. In the latter case, the two orbits are $\{0\}$ and the set of non-zero vectors of norm zero.

We now show that the number of orbits of the commutator subgroup $[O(V), O(V)]$ on V is $p+1$ for $d \geq 5$. Again, it suffices to show that the commutator subgroup $[O(V), O(V)]$ acts transitively on the set of nonzero vectors of a given norm. Suppose $v, w \in V$ are two non-zero vectors of the same norm. Then by the aforementioned argument, there exists an isomtery $\tilde{\phi} \in O(V)$ such that $\tilde{\phi}(v) = w$. We want to show that there exists $\tilde{\psi}, \tilde{\varphi} \in O(V)$ such that the following equation holds.

$$\tilde{\phi}(v) = \tilde{\psi}\tilde{\varphi}\tilde{\psi}^{-1}\tilde{\varphi}^{-1}(v)$$

It suffices to consider the case when $\mu(v, w) = 0$. If not, then $v = w$ and we can take $\tilde{\phi}$ to be the identity element in $O(V)$. Suppose v, w are orthogonal. Let $\{v, w, u_1, u_2, \cdots, u_{d-2}\}$ be the orthogonal basis of V. Without loss of generality, we can assume that the norms of the basis vectors are the same.

Suppose $d \geq 5$. Let W be the span of $\{v, u_1, u_2, u_3, w\}$. Then consider the following isometries $\psi, \varphi : W \to W$. Here, the matrices are given with respect to the orthogonal basis $\{v, u_1, u_2, u_3, w\}$.

$$\psi = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}, \qquad \varphi = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

Note that $\psi^{-1} = \psi$ and $\varphi^{-1} = \varphi$ as isometries over W. The matrix form of $\psi\varphi\psi^{-1}\varphi^{-1}$ is given as follows, which implies that $\psi\varphi\psi^{-1}\varphi^{-1}$ maps v to w.

$$\psi\varphi\psi^{-1}\varphi^{-1} = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \end{pmatrix}$$

By Witt's theorem, there exist isometries $\tilde{\psi}, \tilde{\varphi} \in O(V)$ such that $\tilde{\psi}\tilde{\varphi}\tilde{\psi}^{-1}\tilde{\varphi}^{-1}$ maps v to w. A similar argument as for the case of $O(V)$ shows that the number of orbits of $[O(V), O(V)]$ on V is $p + 1$. □

Using the above lemma, we can calculate the average size of $\mathrm{Sel}_p E_f$ for $f \in F_n(\mathbb{F}_q)$.

Theorem 2.19. *Fix a non-isotrivial elliptic curve $E : y^2 = x^3 + Ax + B$ over $\mathbb{F}_q[t]$ such that E has no $\mathbb{F}_q(t)$-rational p-torsion points, and there exists at least one quadratic twist of E whose Néron model admits a multiplicative reduction away from ∞. Let E_0 be the quadratic twist of E with minimal height among the family of quadratic twists of E. Let n be an integer such that $n \geq 5$. Let p be a prime such that $p \geq 15$, and coprime to q and all local Tamagawa factors of E_0. Then the average size of $\mathrm{Sel}_p E_f$ for a subfamily of quadratic twists $\{E_f\}_{f \in F_n(\mathbb{F}_q)}$ is $p + 1$ when $q \to \infty$, i.e.*

$$\lim_{q \to \infty} \frac{\sum_{f \in F_n(\mathbb{F}_q)} |\mathrm{Sel}_p(E_f)|}{|F_n(\mathbb{F}_q)|} = p + 1$$

Proof. Denote by $\{E_f\}$ the family of quadratic twists of E. Then note the E_0 must have at least one place of multiplicative reduction by the proof of Corollary 3.3. Indeed, E_0 satisfies the condition for Corollary 3.3. Note that the quadratic twist families $\{E_f\}$ and $\{(E_0)_g\}$ are equal. Hence, we can apply lemma 3.10 to the subfamily of quadratic twists $\{E_f\}_{f\in F_n(\mathbb{F}_q)}$.

Since F_n is an open subscheme of $\mathbb{A}^{n+1}$, it holds that $|F_n(\mathbb{F}_q)| = q^{n+1} + O_n(q)$. Then the Grothendieck-Lefschetz trace formula (i.e. Section 2) and lemma 3.10 shows the following equation.

$$\begin{aligned}\lim_{q\to\infty} \frac{\sum_{f\in F_n(\mathbb{F}_q)} |\mathrm{Sel}_p(E_f)|}{|F_n(\mathbb{F}_q)|} &= \lim_{q\to\infty} \frac{\sum_{f\in F_n(\mathbb{F}_q)} |\mathrm{H}^1_{\acute{e}t}(C_{\bar{\mathbb{F}}_q}, \mathcal{E}_{f,p})^{\mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)}|}{|F_n(\mathbb{F}_q)|} \\ &= \lim_{q\to\infty} \frac{|\tau_{n,p,E}(\mathbb{F}_q)|}{|F_n(\mathbb{F}_q)|} \\ &= \lim_{q\to\infty} \#\text{ of orbits of } \Gamma_0 \text{ fixed by } [q]\end{aligned}$$

We recall that Γ is the image of $\pi_1(F_n)$ in $O(\mathrm{H}^1_{\acute{e}t}(C_{\bar{\mathbb{F}}_q}, \mathcal{E}_{f,p}))$, and Γ_0 is the image of $\pi_1((F_n)_{\bar{\mathbb{F}}_q})$ in $O(\mathrm{H}^1_{\acute{e}t}(C_{\bar{\mathbb{F}}_q}, \mathcal{E}_{f,p}))$. The class $[q]$ is the image of the Frobenius $\mathrm{Frob}_q \in \mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$ in Γ/Γ_0.

By theorem 3.11, the geometric monodromy group $\pi_1((F_n)_{\bar{\mathbb{F}}_q})$ is isomorphic to a subgroup of $O(\mathrm{H}^1_{\acute{e}t}(C_{\bar{\mathbb{F}}_q}, \mathcal{E}_{f,p}))$ of index at most 2 and is not $SO(\mathrm{H}^1_{\acute{e}t}(C_{\bar{\mathbb{F}}_q}, \mathcal{E}_{f,p}))$. Recall from remark 3.8 that the Weil pairing on $E_f[p]$ induces a non-degenerate symmetric bilinear pairing μ on $\mathrm{H}^1_{\acute{e}t}(C_{\bar{\mathbb{F}}_q}, \mathcal{E}_{f,p})$.

$$\mathrm{H}^1_{\acute{e}t}(C_{\bar{\mathbb{F}}_q}, \mathcal{E}_{f,p}) \times \mathrm{H}^1_{\acute{e}t}(C_{\bar{\mathbb{F}}_q}, \mathcal{E}_{f,p}) \to \mathbb{F}_p$$

Hence, the frobenius map Frob_q preserves the pairing on $\mathrm{H}^1_{\acute{e}t}(C_{\bar{\mathbb{F}}_q}, \mathcal{E}_{f,p})$. We apply lemma 3.12 by setting $V = \mathrm{H}^1_{\acute{e}t}(C_{\bar{\mathbb{F}}_q}, \mathcal{E}_{f,p})$ and μ to be the non-degenerate symmetric bilinear pairing induced from the Weil pairing over $E_f[p]$.

Note that the elliptic curve E_f has additive reduction at all primes π dividing f. Hence, lemma 3.7 implies that for $n \geq 5$, the dimension of the vector space V is greater than 5. Hence for $n \geq 5$, the orbits of $\pi_1((F_n)_{\bar{\mathbb{F}}_q})$ are the sets of non-zero vectors of a fixed norm and the set $\{0\}$. Therefore, Frob_q preserves the orbits of $\pi_1((F_n)_{\bar{\mathbb{F}}_q})$. Hence, the number of orbits of $\pi_1((F_n)_{\bar{\mathbb{F}}_q})$ fixed by Frob_q is $p+1$ for all q.

Hence, we have the following equation, which proves the theorem.

$$\lim_{q\to\infty} \frac{\sum_{f\in F_n(\mathbb{F}_q)} |\mathrm{Sel}_p(E_f)|}{|F_n(\mathbb{F}_q)|} = p+1$$

□

2.4 Main Theorem

In this section, we prove the main theorem by using theorem 2.19. Fix a non-isotrivial elliptic curve $E : y^2 = x^3+Ax+B$ over $\mathbb{F}_q[t]$ such that E has no $\mathbb{F}_q(t)$-rational p-torsion points, and there exists at least one quadratic twist of E whose Néron model admits a multiplicative reduction away from ∞. We also assume that $\mathrm{char}(F_q) \geq 5$. Denote by Δ_E the discriminant of the elliptic curve E. We then order the family of quadratic twists $\{E_f\}$ with square-free polynomials f over $\mathbb{F}_q$ based on the canonical height of E_f.

The idea of the proof is as follows. Let E_0 be the quadratic twist of E with minimal height among the family of quadratic twists of E. Then by corollary 3.3, the Néron model of E_0 admits a multiplicative reduction away from ∞. Note the quadratic twist families $\{E_f\}$ and $\{(E_0)_f\}$ are the same. Hence, we can reorder the family $\{E_f\}$ by $\{(E_0)_f\}$. Such reordering of family of quadratic twists will allow us to ensure that the subfamily of quadratic twists whose p-Selmer rank is undetermined does not affect the average size of p-Selmer group of $\{E_f\}$ as $q \to \infty$.

Remark 2.20. *One may ask whether it is possible to compute the average size of p-Selmer groups by ordering the family of quadratic twists $\{E_f\}$ by the degree of the twisting polynomial f. The problem with this approach is that Chris Hall's construction of étale $\mathbb{F}_p$-lisse sheaf only works for elliptic curves E with at least one multiplicative reduction. Suppose E has at least one place of multiplicative reduction. Then the quadratic twist family $\{E_f\}$ can be decomposed into the following two disjoint sets.*

$$\{E_f\} = \{E_f\}_{\{f \mid (f,\Delta_E)=1\}} \sqcup \{E_f\}_{\{f \mid (f,\Delta_E)\neq 1\}}$$

The subfamily $\{E_f\}_{\{f \mid (f,\Delta_E)=1\}}$*, which dominates the family* $\{E_f\}$ *when* $\deg f \to \infty$*, consists of quadratic twists of* E *having at least one place of multiplicative reduction, the subfamily on which the average* p*-Selmer rank is known to be* $p+1$*.*

However, the elliptic curve $E' := E_{\Delta_E}$ *has no multiplicative reduction. Note that* $\Delta_{E'} = \Delta_E^7$*. Contrary to* $\{E_f\}$*, the family of quadratic twists of* $\{E'_f\}$ *is given as follows.*

$$\{E'_f\} = \{E'_f\}_{\{f \mid (f,\Delta_{E'})=(f,\Delta_E)=1\}} \sqcup \{E_f\}_{\{f \mid (f,\Delta_{E'})=(f,\Delta_E)\neq 1\}}$$

Here, the subfamily $\{E'_f\}_{\{f \mid (f,\Delta_E)=1\}}$*, which dominates the family* $\{E'_f\}$ *when* $\deg f \to \infty$*, consists of quadratic twists of* E' *having no multiplicative reductions, the subfamily on which the average size of* p*-Selmer group is unknown.*

But notice that $\{E_f\}$ *and* $\{E'_f\}$ *are the same family of quadratic twists. Hence, we cannot determine the average size of* p*-Selmer group by ordering the family of quadratic twists based on the degree of the twisting polynomials.*

Before we present the proof of the main theorem, we state the following definitions and notations.

Definition 2.21. *Denote by* $F(n)$ *the following scheme defined over* $\bar{\mathbb{F}}_q$*.*

$$F(n) := \{f \in \bar{\mathbb{F}}_q[t] \mid f \in F_d \text{ for } d \leq n\} = \bigsqcup_{d=1}^{n} F_d$$

As mentioned before $F(n)$ is an open subscheme of $\mathbb{A}^{n+1}$. Hence, the following equation holds

$$|F(n)(\mathbb{F}_q)| = q^{n+1} - \mathrm{O}(q^n)$$

Definition 2.22. *Denote by* $\tilde{\tau}(n,p,E)$ *the sheaf over* $F(n)$ *obtained by gluing étale* $\mathbb{F}_p$*-lisse sheaves* $\{\tau_{d,p,E} \to F_d\}$ *for all* $d \leq n$*.*

The following theorem states an analogue of Theorem 3.12 for the subfamily of quadratic twists $\{E_f\}_{f \in F(n)(\mathbb{F}_q)}$ such that E satisfies the aforementioned two conditions.

Theorem 2.23. *Fix a non-isotrivial elliptic curve $E : y^2 = x^3 + Ax + B$ over $\mathbb{F}_q[t]$ such that E has no $\mathbb{F}_q(t)$-rational p-torsion points, and there exists at least one quadratic twist of E whose Néron model admits a multiplicative reduction away from ∞. Let E_0 be the quadratic twist of E with minimal height among the family of quadratic twists of E. Let n be an integer such that $n \geq 5$. Let p be a prime such that $p \geq 15$, and coprime to q and all local Tamagawa factors of E_0. Then the average size of $\mathrm{Sel}_p E_f$ for the subfamily of quadratic twists $\{E_f\}_{f \in F(n)(\mathbb{F}_q)}$ is $p+1$ as $q \to \infty$, i.e.*

$$\lim_{q\to\infty} \frac{\sum_{f\in F(n)(\mathbb{F}_q)} |\mathrm{Sel}_p(E_f)|}{|F(n)(\mathbb{F}_q)|} = p+1$$

Proof. As stated before, $|F(n)(\mathbb{F}_q)| = q^{n+1} + O(q^n)$. As in the proof of theorem 3.13, the Grothendieck-Lefschetz trace formula and lemma 3.10 shows the following equation, where $\mathrm{Frob}_q \in \mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$.

$$\begin{aligned}
\lim_{q\to\infty} \frac{\sum_{f\in F(n)(\mathbb{F}_q)} |\mathrm{Sel}_p E_f|}{|F(n)(\mathbb{F}_q)|} &= \lim_{q\to\infty} \frac{\sum_{d=1}^n \sum_{f\in F_d(\mathbb{F}_q)} |\mathrm{Sel}_p E_f|}{\sum_{d=1}^n |F_d(\mathbb{F}_q)|} \\
&= \lim_{q\to\infty} \frac{\sum_{d=1}^n \sum_{f\in F_d(\mathbb{F}_q)} |\mathrm{Sel}_p E_f|}{\sum_{d=1}^n |F_d(\mathbb{F}_q)|} \\
&= \lim_{q\to\infty} \frac{\sum_{d=1}^n \sum_{f\in F_d(\mathbb{F}_q)} |\mathrm{H}^1_{\acute{e}t}(C_{\bar{\mathbb{F}}_q}, \mathcal{E}_{f,p})^{\mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)}|}{\sum_{d=1}^n |F_d(\mathbb{F}_q)|} \\
&= \lim_{q\to\infty} \frac{\sum_{d=1}^n |\tau_{d,p,E}(\mathbb{F}_q)|}{\sum_{d=1}^n |F_d(\mathbb{F}_q)|} \left(= \lim_{q\to\infty} \frac{|\tilde{\tau}(n,p,E)(\mathbb{F}_q)|}{|F(n)(\mathbb{F}_q)|} \right) \\
&= \lim_{q\to\infty} \sum_{d=1}^n \left(\frac{|\tau_{d,p,E}(\mathbb{F}_q)|}{|F_d(\mathbb{F}_q)|} \frac{|F_d(\mathbb{F}_q)|}{|F(n)(\mathbb{F}_q)|} \right)
\end{aligned}$$

By theorem 3.13, the following equation holds.

$$\begin{aligned}
\lim_{q\to\infty} \frac{\sum_{f\in F(n)(\mathbb{F}_q)} |\mathrm{Sel}_p E_f|}{|F(n)(\mathbb{F}_q)|} &= \lim_{q\to\infty} \sum_{d=1}^n \left((p+1) \frac{|F_d(\mathbb{F}_q)|}{|F(n)(\mathbb{F}_q)|} \right) \\
&= \lim_{q\to\infty} (p+1) \frac{|F_n(\mathbb{F}_q)|}{|F(n)(\mathbb{F}_q)|} \\
&= p+1
\end{aligned}$$

□

We now order the family of quadratic twist of elliptic curves based on the canonical height of the elliptic curve. Recall that the canonical height of the elliptic curve is given as follows, where $E' : y^2 = x^3 + C(t)x + D(t)$ is an elliptic curve isomorphic to E.

$$h(E) := \inf_{E' \cong E} (\max\{3 \deg C, 2 \deg D\})$$

Remark 2.24. *There is a unique equation for E of the form $y^2 = x^3 + Ax + B$ satisfying that for any prime $p \in \mathbb{F}_q[t]$, $p^4|A$ implies $p^6 \nmid B$. In such case, $h(E)$ is equal to $max\{3 \deg A, 2 \deg B\}$.*

In particular E has the least height among all quadratic twists if and only if for any prime $p \in \mathbb{F}_q[t]$, $p^2|A$ implies $p^3 \nmid B$. Otherwise, there exists a quadratic twist $E_p : py^2 = x^3 + Ax + B \simeq y^2 = x^3 + \frac{A}{p^2}x + \frac{B}{p^3}$, which has smaller height than E.

Remark 2.25. *In order to apply the construction of the étale $\mathbb{F}_p$-lisse sheaf $\tau_{n,p,E} \to F_n$ from* [CH05]*, we need the assumption that the quadratic twist family we start with has members whose Néron model admits at least one multiplicative reduction away from ∞.*

This is essentially necessary because one can find families of quadratic twists of some given elliptic curves, such that the whole family has no elliptic curve whose Néron model has multiplicative reductions. For instance, suppose 4 and 27 are invertible over the field $\mathbb{F}_q$. Then there are $\pi_1, \pi_2 \in \mathbb{F}_q[t]$ such that $4\pi_1 t^3 + 27\pi_2(t+1)^2 = 1$ with $deg(\pi_1) = 1$ and $deg(\pi_2) = 2$. One can readily check that the elliptic curve $E : y^2 = x^3 + \pi_1\pi_2 t + \pi_1\pi_2^2(t+1)$ has discriminant $\Delta_E = \pi_1^2\pi_2^3(4\pi_1 t^3 + 27\pi_2(t+1)^2) = \pi_1^2\pi_2^3$. Therefore, the Néron model of E has no multiplicative reduction by Tate's algorithm. This elliptic curve E has the least height in the quadratic twist family by remark 4.5. So, the whole quadratic twist family has no member whose Néron model admits multiplicative reductions away from ∞ by remark 3.4.

Now we prove the main theorem.

Proof of Theorem 1.1. Let $E : y^2 = x^3 + A_0x + B_0$ be any non-isotrivial elliptic curve over $\mathbb{F}_q[t]$. We can always replace E by $E_0 \in \{E_f\}$ that has minimal canonical height among all quadratic twists. Since we assumed that there exists at least one quadratic twist of E

whose Néron model admits a multiplicative reduction away from ∞, E admits at least one multiplicative reduction.

Setup

Choose large enough q such that the discriminant of $E/\mathbb{F}_q[t]$, denoted by Δ_E, splits completely into linear factors as follows.

$$\Delta_E = \pi_0^{r_0}\pi_1^{r_1}\cdots\pi_m^{r_m}$$

Without loss of generality, assume E has multiplicative reduction at π_0. Note we can guarantee that the primes π_i's are all linear. For those large enough q, we will explicitly determine the collection of all possible quadratic twists of $E/\mathbb{F}_q[t]$ whose height is bounded by n.

We order the family of quadratic twists of E by canonical height. For any elliptic curve $E/\mathbb{F}_q[t]$, there exists a unique way to write E as $y^2 = x^3+Ax+B$ such that for any irreducible polynomial $p \in \mathbb{F}_q[t]$, if $p^4|A$, then $p^6 \nmid B$. Then the canonical height of E is given as follows.

$$h(E) = \max\{3\deg A, 2\deg B\}$$

In particular, we chose E to have the least height in the family of quadratic twists of E_0. Hence, the coefficients A, B of E satisfy the aforementioned condition.

Any quadratic twist of $E/\mathbb{F}_q[t]$ can be uniquely written as $E_f : fy^2 = x^3+Ax+B$ such that $f \in \mathbb{F}_q[t]$ is square-free. Assume $f = \pi_0^a\pi_{i_1}\pi_{i_2}\cdots\pi_{i_s}g$ where π_{i_j}'s are distinct primes belong to the set $\{\pi_1,\cdots,\pi_m\}$, $a = 0$ or 1, and g is a square-free polynomial such that $(g,\Delta_E) = 1$ in $\bar{\mathbb{F}}_q[t]$. Denote by J the subset $\{\pi_{i_1},\pi_{i_2},\cdots,\pi_{i_s}\}$ of $\{\pi_1,\pi_2,\cdots,\pi_m\}$.

Fix a positive integer n. We now consider the quadratic twists $\{E_f\}$ whose height $h(E_f) \leq n$.

Case 1

Suppose that $a = 0$, i.e. π_0 is not a prime factor of f. Remark 4.5 implies that the twist E_f is isomorphic to the following elliptic curve, which is a minimal model.

$$y^2 = x^3 + \left(\prod_{\pi_{i_j}\in J}\pi_{i_j}^2\right)g^2Ax + \left(\prod_{\pi_{i_j}\in J}\pi_{i_j}^3\right)g^3B \qquad (*)$$

We will use use $(*)$ to explicitly compute the height of E_f. We also note that for any prime $p|g$, $v_p(A) = 0$ or $v_p(B) = 0$. Otherwise, g is not coprime to Δ_E. Therefore, we have the following equivalent relation.

$$h(E_f) \leq n \Longleftrightarrow \max\left\{\deg\left(\left(\prod_{\pi_{i_j}\in J}\pi_{i_j}^6\right)g^6A^3\right), \deg\left(\left(\prod_{i_j\in J}\pi_{i_j}^6\right)g^6B^2\right)\right\} \leq n$$

We set $M := \max\{3\deg A, 2\deg B\}$ and $M_J := M + 6\deg\left(\prod_{i_j\in I}\pi_{i_j}\right) = M + 6|J|$. Hence the following equivalent relation holds.

$$h(E_f) \leq n \Longleftrightarrow \deg g \leq \frac{n - M_J}{6}$$

It is crucial to notice that the twist E_f still has at least one place of multiplicative reduction at π_0, which can be checked using Tate's algorithm.

Denote by E_J the following elliptic curve, which is minimal by remark 4.5.

$$E_J : y^2 = x^3 + \left(\prod_{\pi_{i_j}\in J}\pi_{i_j}^2\right)Ax + \left(\prod_{\pi_{i_j}\in J}\pi_{i_j}^3\right)B$$

Then the following equation holds.

$$\begin{aligned}\sum_{\substack{f=\pi_{i_1}\pi_{i_2}\cdots\pi_{i_s}g\\(g,\Delta_E)=1\\h(E_f)\leq n}}|\mathrm{Sel}_pE_f| &= \sum_{g\in F\left(\frac{n-M_J}{6}\right)(\mathbb{F}_q)}|\mathrm{Sel}_p(E_J)_g| \\ &= \left|\tilde{\tau}\left(\frac{n-M_J}{6}, p, E_J\right)(\mathbb{F}_q)\right| \\ &= (p+1)\left(q^{\frac{n-M_J}{6}+1} + \mathrm{O}_{n,p}(q^{\frac{n-M_J}{6}})\right)\end{aligned}$$

Case 2

Now assume $a = 1$, i.e. $f = \pi_0\pi_{i_1}\pi_{i_2}\cdots\pi_{i_s}g$ such that $(g, \Delta_E) = 1$ and $J = \{\pi_{i_1}, \pi_{i_2}, \cdots, \pi_{i_s}\}$ is a subset of $\{\pi_1, \pi_2, \cdots, \pi_m\}$. Define M and M_J analogously to Case 1. Then, by the aforementioned argument in Case 1, we have that E_f is isomorphic to the following minimal model.

$$y^2 = x^3 + \left(\prod_{\pi_{i_j}\in J}\pi_{i_j}^2\right)\pi_0^2g^2Ax + \left(\prod_{\pi_{i_j}\in J}\pi_{i_j}^3\right)\pi_0^3g^3B \qquad (*)$$

Thus the height of E_f can be written as follows.

$$h(E_f) \leq n \Longleftrightarrow \deg g \leq \frac{n - M_J - 6\deg \pi_0}{6} = \frac{n - M_J}{6} - 1$$

We will use the bound of $h(E_f)$ to estimate the summation of the size of the p-Selmer group for quadratic twists E_f by using lemma 3.7. Corollary 3.3 and lemma 3.7 implies that the maximal size of p-Selmer group of E_f is the following.

$$|\mathrm{Sel}_p E_f| \leq p^{2\deg \Delta_{E_f}+4} \leq p^{2h(E_f)+4} = p^{2n+4}$$

Therefore, the following equation gives the approximation on the size of the p-Selmer group over $\{E_f\}$ for the desired collection of f.

$$\begin{aligned}\sum_{\substack{f=\pi_0\pi_{i_1}\pi_{i_2}\cdots\pi_{i_s}g \\ (g,\Delta_E)=1 \\ h(E_f)\leq n}} |\mathrm{Sel}_p E_f| &= \sum_{g\in F\left(\frac{n-M_J}{6}-1\right)(\mathbb{F}_q)} \mathrm{Sel}_p(E_J)_g \\ &= \mathcal{M}\left(q^{\frac{n-M_J}{6}} + \mathrm{O}_{n,p}(q^{\frac{n-M_J}{6}-1})\right)\end{aligned}$$

Here, $\mathcal{M}$ is a positive integer such that $1 \leq \mathcal{M} \leq p^{2n+4}$.

Average Size

Using both aforementioned cases, we can now calculate the average size of p-Selmer group as $k \to \infty$. Recall that $\mathbb{E}_{n,k,p}$ is the average value of p-Selmer groups over families of quadratic twists of canonical height at most n. Then the following equation holds for any fixed $n \geq 30$. Note that we may need to require $n \geq 30$ because of the conditions on the

degree of twisting polynomials from lemma 3.12 and theorem 3.13.

$$\begin{aligned}
\lim_{q\to\infty}\mathbb{E}_{n,p} &= \lim_{q\to\infty}\frac{\sum_{J\subset\{\pi_1,\cdots,\pi_m\}}(p+1)\left(q^{\frac{n-M_J}{6}+1}+\mathrm{O}_{n,p}(q^{\frac{n-M_J}{6}})\right)+\mathcal{M}\left(q^{\frac{n-M_J}{6}}+\mathrm{O}_{n,p}(q^{\frac{n-M_J}{6}-1})\right)}{\sum_{J\subset\{\pi_1,\cdots,\pi_m\}}|F(\frac{n-M_J}{6})(\mathbb{F}_q)|+|F(\frac{n-M_J}{6}-1)(\mathbb{F}_q)|}\\
&= \lim_{q\to\infty}\sum_{J\subset\{\pi_1,\cdots,\pi_m\}}\frac{(p+1)\left(q^{\frac{n-M_J}{6}+1}+\mathrm{O}_{n,p}(q^{\frac{n-M_J}{6}})\right)+\mathcal{M}\left(q^{\frac{n-M_J}{6}}+\mathrm{O}_{n,p}(q^{\frac{n-M_J}{6}-1})\right)}{|F(\frac{n-M_J}{6})(\mathbb{F}_q)|+|F(\frac{n-M_J}{6}-1)(\mathbb{F}_q)|}\\
&\times\lim_{q\to\infty}\frac{|F(\frac{n-M_J}{6})(\mathbb{F}_q)|+|F(\frac{n-M_J}{6}-1)(\mathbb{F}_q)|}{\sum_{J\subset\{\pi_1,\cdots,\pi_m\}}|F(\frac{n-M_J}{6})(\mathbb{F}_q)|+|F(\frac{n-M_J}{6}-1)(\mathbb{F}_q)|}\\
&= \lim_{q\to\infty}\sum_{J\subset\{\pi_1,\cdots,\pi_m\}}\frac{(p+1)\left(q^{\frac{n-M_J}{6}+1}+\mathrm{O}_{n,p}(q^{\frac{n-M_J}{6}})\right)+\mathcal{M}\left(q^{\frac{n-M_J}{6}}+\mathrm{O}_{n,p}(q^{\frac{n-M_J}{6}-1})\right)}{q^{\frac{n-M_J}{6}+1}+\mathrm{O}_{n,p}(q^{\frac{n-M_J}{6}})+q^{\frac{n-M_J}{6}}+\mathrm{O}_{n,p}(q^{\frac{n-M_J}{6}-1})}\\
&\times\lim_{q\to\infty}\frac{|F(\frac{n-M_J}{6})(\mathbb{F}_q)|+|F(\frac{n-M_J}{6}-1)(\mathbb{F}_q)|}{\sum_{J\subset\{\pi_1,\cdots,\pi_m\}}|F(\frac{n-M_J}{6})(\mathbb{F}_q)|+|F(\frac{n-M_J}{6}-1)(\mathbb{F}_q)|}\\
&= \lim_{q\to\infty}\sum_{J\subset\{\pi_1,\cdots,\pi_m\}}(p+1)\frac{|F(\frac{n-M_J}{6})(\mathbb{F}_q)|+|F(\frac{n-M_J}{6}-1)(\mathbb{F}_q)|}{\sum_{J\subset\{\pi_1,\cdots,\pi_m\}}|F(\frac{n-M_J}{6})(\mathbb{F}_q)|+|F(\frac{n-M_J}{6}-1)(\mathbb{F}_q)|}\\
&= (p+1)\lim_{q\to\infty}\sum_{J\subset\{\pi_1,\cdots,\pi_m\}}\frac{|F(\frac{n-M_J}{6})(\mathbb{F}_q)|+|F(\frac{n-M_J}{6}-1)(\mathbb{F}_q)|}{\sum_{J\subset\{\pi_1,\cdots,\pi_m\}}|F(\frac{n-M_J}{6})(\mathbb{F}_q)|+|F(\frac{n-M_J}{6}-1)(\mathbb{F}_q)|}\\
&= p+1
\end{aligned}$$

Therefore, the average size of p-Selmer groups of family of quadratic twists of any elliptic curve E over $\mathbb{F}_q[t]$ is given by $p+1$:

$$\lim_{n\to\infty}\lim_{q\to\infty}\mathbb{E}_{n,p}=p+1$$

□

Chapter 3

The case of 2-Selmer group

3.1 Introduction

In this chapter, we will turn our focus from general p-Selmer group to 2-Selmer group of elliptic curves defined over function field.

let E be an elliptic curve defined over a function field K and we denote by $Sel_2(E/K)$ its 2-Selmer group. 2-Selmer rank $d_2(E/K)$ is defined as

$$d_2(E/K) := \dim_{\mathbb{F}_2} \mathrm{Sel}_2(E/K) - \dim_{\mathbb{F}_2} E(K)[2]$$

There has been substantial study on the distribution of 2-Selmer groups in the case of number field:

Health-Brown proved in 1994 [Bro94] that the 2-Selmer ranks of all the quadratic twists of the congruent number curve $E/\mathbb{Q}$ given by $y^2 = x^3 - x$ have a nice distribution which is characterized by explicit constants $\alpha_1, \alpha_2, \alpha_3, \cdots$ that sum to 1 such that

$$\lim_{X\to\infty} \frac{|\{\mathrm{d\ squarefree}\ |\mathrm{d}| < \mathrm{X} : d_2(E^d/\mathbb{Q}) = r\}|}{|\{\mathrm{d\ squarefree}\ |\mathrm{d}| < \mathrm{X}\}|} := \alpha_r$$

for every $r \in \mathbb{Z}^{\geq 0}$, where E^d is the quadratic twist of E by d.

A similar result was proved by Swinnerton-Dyer and Kane for all elliptic curves E over $\mathbb{Q}$ with $E(\mathbb{Q})[2] \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ that do not have a cyclic 4-isogeny defined over $\mathbb{Q}$ [Kan10], [SD08]. Another case was shown by Klagsbrun, Mazur, and Rubin for elliptic curves E defined over a number field K with $\mathrm{Gal}(K(E[2])/K) \simeq S_3$, where d is replaced by quadratic characters of K [KMR11].

There also have been examples where this type of result do not hold true in the number field case. Klagsbrun and Oliver proved that when $E(K)[2] \simeq \mathbb{Z}/2\mathbb{Z}$ there does not exist a distribution function on 2-Selmer ranks for the quadratic twist family of E [KO15].

This chapter shows that the same result extends to the function field case. For the rest of this chapter, we use K exclusively to denote the function field $\mathbb{F}_q(t)$. We state our main theorem first:

Theorem 3.1. *Define $C(K,X) := \{$square free $f \in K$: deg(f) $< X\}$, Let E be an elliptic curve defined over K with $E(K) \simeq \mathbb{Z}/2\mathbb{Z}$ that does not have a cyclic isogeny defined over $K(E[2])$. Then for any fixed r,*

$$\liminf_{X\to\infty} \frac{|\{\text{sqaure free } f \in C(K,X)\text{: } T(E'_f/E_f) \geq r \mid}{|C(K,X)|} \geq \frac{1}{2}$$

where E' is the dual elliptic curve of E under 2-isogeny and E_f (resp. E'_f) denotes the quadratic twist of E (resp. E') by f. $T(E'_f/E_f)$ denotes the ratio of the rank of the Selmer groups of E'_f and E_f.

Let E_1 be an elliptic curve defined over $K = \mathbb{F}_q(t)$ with a rational point of order 2. Such a curve can be written in Weierstrass equation of the form $y^2 = x^3 + Ax^2 + Bx$, where the rational two torsion $C = E(K)[2]$ is generated by $P = (0,0)$.

Since $E_1(K)$ has a single point of order two, there is a 2 -isogeny $v_1 : E_1 \longrightarrow E_2$ between E_1 and E_2 with kernel $C = E(K)[2]$, where the dual elliptic curve $E_2 : y^2 = x^3 - 2Ax + (A^2 - 4B)x$ can be constructed explicitly. The map of the 2 -isogeny v_1 could also be explicitly given by $(x,y) \longrightarrow ((\frac{x}{y})^2, \frac{y(B-x^2)}{x^2})$.

We outline the idea for the proof to this theorem. First of all, we would like to show

Theorem 3.2. [Cas65, Theorem 1.1 in number field case] *The Tamagawa ratio* $\mathrm{T}(E_2/E_1)$ *is given by*

$$\mathrm{T}(E_2/E_1) := \frac{S_2}{S_1} = \prod_p \frac{1}{2}|H^1_{v_2}(K_p, \Delta_2)|$$

where S_i denotes the Semler group of E_i, the product is taken over all the prime ideals $p \in K = \mathbb{F}_q(t)$, v_2 is the 2 -isogeny $E_2 \longrightarrow E_1$ whose composition with v_1 is the multiplication by 2 map [2] and Δ_i denotes the kernel of v_i.

After proving this, We take advantage of the fact that everything is given explicitly so we can study the size of $H^1_{v_2}(K_p, \Delta_2)$ and relate that to the size of their Tamagawa numbers.

3.2 Outline of the strategy

The number field version of theorem 3.2 was proven by Cassels, we follow his approach by reproving the main lemmas used in the number field case and then restore the proof as a whole. We show that we have the following.

Lemma 3.3.

$$\frac{S_2}{S_1} = \prod_p \frac{(G_{1p})_{v_1}}{(WC_{2p})_{v_2}} \cdot \frac{(G_2)_{v_2}}{(G_1)_{v_1}}$$

where G_i denotes the group of points defined over $\mathbb{F}_q(t)$ for E_i and G_{ip} denotes the group of points defined over the local field K_p, the subindex $()_{v_i}$ denotes the kernel of these maps with respect to the isogeny v_i between the 2 elliptic curves.

We show first that the above lemma 2.1 implies theorem 1.2. As v_i are maps of degree 2 and E_i has 2-torsion points, it's easy to find out that $(G_i)_{v_i}$ has size 2 as the explicit 2-torsion $(0,0)$ must be over $\mathbb{F}_q(t)$. In addition to that, $(G_{1p})_{v_1}$ also has size 2 for the same reason.

We can compute the size of $(WC_{2p})_{v_2}$ through an exact sequence

$$0 \longrightarrow G_{1p}/G_{2p} \longrightarrow H^1(\Gamma_p, \Delta_2) \longrightarrow (WC_{2p})_{v_2} \longrightarrow 0$$

Therefore, we then have

$$\frac{|S_2|}{|S_1|} = \prod_p \frac{2 \cdot |G_{1p}/v_2 G_{2p}|}{|H^1(\Gamma_p, \Delta_2)|}$$

where Γ_p stands for the Galois group $\mathrm{Gal}(((\mathbb{F}_q(t)^{sep})_p/(\mathbb{F}_q(t))_p)$.

Here we take advantage of the fact that $H^1(\Gamma_p, \Delta_2) \simeq H^1(\Gamma_p, \pm 1)$ has trivial Galois action. We know that in this case it is equal to $\mathrm{Hom}(\Gamma_p, \pm 1)$ = index 2 subgroup of $\Gamma_p \simeq$ quadratic extension $/K_p \simeq (K_p)^*/(K_p^*)^2$ where K_p is some local field that resembles $\mathbb{F}_q((t))$ and it

has the structure $\mathbb{Z} \oplus \mathbb{Z}/(q-1)\mathbb{Z}_p^N$. The notation here is slight ambiguous, p refers to the characteristic of the field $K = \mathbb{F}_q(t)$ and $q = p^N$. This concludes that the size of $H^1(\Gamma_p, \Delta_2)$ is always 4, thus we have

$$\frac{|S_2|}{|S_1|} = \prod_p \frac{1}{2} \cdot \frac{|G_{1p}|}{|v_2(G_{2p})|}$$

as expected. Because the definition of $H^1_{v_2}(K_p, \Delta_2) \subset H^1(K_p, \Delta_2)$ is the image of $E_1(K_p)/v_2(E_2(K_p))$ under Kummer map.

3.3 The computation of cohomology groups

We need to show that [Cas65, Lemma 7.2 and Lemma 7.3] remain true in our case. Firstly we need to restore [Cas65, Lemma 6.1]. Here we use the notations $\Gamma = \mathrm{Gal}(\mathbb{F}_q(t)^{sep}/\mathbb{F}_q(t))$, $M = \Delta_2/\mathbb{F}_q(t)$. $\Omega \in (\mathbb{F}_q(t)^{sep})^* =$ 2nd roots of unity. Notice that since we required $q \neq 2$, so $\Omega = +1$, $M^* = Hom(\Delta, \Omega) \simeq \mathbb{Z}/2$.

The exact statement of the first Lemma in Cassel that we need to prove is the following:

Lemma 3.4. *Let Γ be the Galois group of $\bar{k}/k$, where $\bar{k}$ is the algebraic closure of the number field k and let M be a Γ-module of prime order q. Denote by q^η,q^ε respectively the number of elements of M and of*

$$M^* = Hom(M, \Omega)$$

which are fixed under Γ, where $\Omega \subset \bar{k}^*$ is the group of q-th roots of unity and Γ acts on M^* in the usual way. Let Π be a finite set of valuations of k which includes all the non-archimedean ones and denote by $H^1_\Pi(\Gamma, M)$ the group of elements of $H^1(\Gamma, M)$ which do not ramify outside Π. Then

$$|H^1_\Pi(\Gamma, M)| = q^{P+\eta-\varepsilon}$$

where P is the number of $p \in \Pi$ such that the splitting field Γ_p acts trivally on M^*, provided that the set Π is large enough in the following sense:

(i) Π contains all p such that $|q|_p \neq 1$.

(ii) Let $\Gamma^* \subset \Gamma$ be the subgroup which leaves M^* elementwise fixed and let K be the corresponding algebraic extension of k. Then every divisor class (ideal class) of K contains a prime divisor $\mathfrak{P}$ which is he extension to K of one of the $p \in \Pi$.

We can take advantage of that in our specific case things are a lot more computable, and find the size of $|H^1_\Pi(\Gamma, M)|$ directly.

Recall the definition for an element $x \in H^1(\Gamma, M)$ to be unramified out of the set Π which consists of a few primes. We have the exact sequence:

$$1 \longrightarrow G_{\bar{K}/K^{ur}} \longrightarrow G_{\bar{K}/K} \longrightarrow G_{K^{ur}/K} \longrightarrow 1$$

locally we have

$$\text{inf: } H^1(\mathrm{Gal}(K_{p,ur}), M) \longrightarrow H^1(\mathrm{Gal}(\bar{K_p}/K_p), M)$$

Consider $H^1(K, M) \longrightarrow \prod_p H^1(K_p, M)$, say $x \in H^1(K, M)$ is unramified at p if

$$x_p \in H^1_{ur}(K_p, M) \quad \text{(i.e. im(inf))}$$

In our setting, the two constraints for the choice of Π in Lemma 3.1. become trivially true for any case because the field $K = \mathbb{F}_q(t)$ has class number 1. We choose to keep the statement there to demonstrate that this is not any less than the original lemma of Cassels so that the rest of proof would follow the the course.

We choose $\Pi = \{p = (f), \infty\}$, then for all $x \in H^1_\Pi(G_{K^{sep}/K}, M)$, we claim

$$x_{p'} \ (p' \neq p) \text{ must be trivial.} \tag{3.3.1}$$

If it were true, notice that $x \in H^1_\Pi(\Gamma, M)$ corresponds to a quadratic field extension over $\mathbb{F}_q(t)$ (we could do it here because all quadratic extensions are separable). Hence it must be isomorphic to $\mathbb{F}_q(\sqrt{g})$ or $\mathbb{F}_{q^2}(t)$. Also notice that since $K^{sep} \cap K_p = K$, we have the following exact sequence:

$$\mathrm{Gal}(K_p^{sep}/K_p) \longrightarrow \mathrm{Gal}(K^{sep}/K) \longrightarrow \mathbb{Z}/2$$

which deduces the equivalence between the choice of elements:

choose $x \iff$ choose index 2 subgroup of $\mathrm{Gal}(K_p^{sep}/K_p)$ s.t. every corresponding $x_{p'}$ is trivial $\iff$ choose index 2 subgroup s.t. it acts trivially on all $\sqrt{g}$ (where $p' = (g)$) and only potentially acts on $\sqrt{f}$ and $\mathbb{F}_{q^2}$

To show (3.1) is true, consider the following

$$\mathbb{F}_q((t))^{unr} = \varinjlim \text{finite unr. extensions} = \mathbb{F}_q((t))[\mu'(\bar{\mathbb{F}}_q)]$$

by adjoining all roots of unity of order prime to q.

We also have

$$H^1(G_{K^{sep}/K}, \mathbb{Z}/2) \longrightarrow H^1(K_p^{sep}/K_p, \mathbb{Z}/2)$$

the unramified (with respect to p) elements of $H^1(G_{K^{sep}/K}, \mathbb{Z}/2)$ correspond to the index 2 subgroups H such that

$$H \longrightarrow G_{K^{sep}/K} \longrightarrow \mathbb{Z}/2$$

factors through $G_{K_p^{sep,ur}/K_p}$ ($K_p^{sep,ur}$ will be denoted by K_p^{ur} for simplicity)

Suppose there existed some index 2 subgroup H acts on K_p^{sep} that moves $\sqrt{f}$ where $p = (f) \neq (g)$. We know that $G_{K_p^{sep}/K_p}$ only permutes the $\bar{\mathbb{F}}_q$ part of $\mathbb{F}_q((t))[\mu'(\bar{\mathbb{F}}_q)]$. This would imply that one can find $\sigma \in H^c$ (which should be sent to -1) that fixes $\mathbb{F}_q^{sep}$ such that $\sigma|_{\sqrt{f}} = -\sqrt{f}$, then we would have $\sigma|_{K_p^{ur}} = id$ but $\sigma \longrightarrow -1$ through the composition with $G_{K_p^{ur}/K_p} \longrightarrow \mathbb{Z}/2$. Therefore, in order to be unramified at $p = (f)$, x_p has to be the index 2 subgroup that fixes $\sqrt{f}$.

As x_p is induced from $x \in H^1(G_{K^{sep}/K}, \mathbb{Z}/2)$, this deduces that x also has to fix every $\sqrt{f}$ but $\sqrt{g}$. The above argument also shows that such x is allowed to move the $\mathbb{F}_{q^2}$ part of $(\mathbb{F}_q(t))^{sep}$.

To summarize, this shows

$$|H^1_\Pi(G_{K^{sep}/K}, \mathbb{Z}/2)| = 4$$

given our choice of $M = \{(g), \infty\}$, so Lemma 3.1 holds in our case. (∞ here corresponds to the local field $\mathbb{F}_q((\frac{1}{t}))$ which only admits unramified quadratic extension $\mathbb{F}_{q^2}((\frac{1}{t}))$, so those 4 elements except for the identity all ramify at ∞)

Here is another lemma in Cassels's proof that we need to recover for our case:

Lemma 3.5. *Under the above settings and conditions, there is a finite set of valuations* Π_1 *of* $K = \mathbb{F}_q(t)$ *such that the obvious maps*

$$H^1_{\Pi}(K^{sep}/K, \Delta_j) \longrightarrow \prod_{p \in \Pi} H^1(K_p^{sep}/K_p, \Delta_j) \tag{3.3.2}$$

are injections for any finite set Π *of valuations containing* Π_1.

Since G_{K_p} acts trivially on $\Delta_j \simeq \pm 1$, we have

$$H^1(K_p^{sep}/K_p, \mathbb{Z}/2) \simeq (\mathbb{F}_q(t))_p^*/(\mathbb{F}_q(t))_p^2$$

Then based on the preceding calculation of $H^1_{\Pi}(K_p^{sep}/K_p, \mathbb{Z}/2)$, we have that

$$H^1_{\Pi}(K_p^{sep}/K_p, \mathbb{Z}/2) \simeq K_{\Pi}/K_{\Pi}^2$$

where K_{Π} consists of elements of $(\mathbb{F}_q(t))^*$ that are units outside Π, which are basically characterized by $\sqrt{f_1 \cdot f_k}$ with $f_i \in \Pi$. But it is a well-known fact that

$$K_{\Pi}/K_{\Pi}^2 \longrightarrow (K)_p^*/(K)_p^2$$

is an injection if and only if the set Π is large enough.

3.4 Proof of theorem 3.2

This is a function field version of Cassels's proof, the original statement was made on the number field case. As we have discussed, the calculation in our case is simpler because the kernel of the 2-isogeny has trivial Galois action.

Proof. Let Π be a finite set of valuations on K which contains all the infinite valuations, all the valuations where either E_1 or E_2 or the isogenies v_1, v_2 have a bad reduction, and which is large enough so that the conclusions of above Lemmas 3.1 and 3.2 hold. Let

$$I_j = \prod_{p \in \Pi} H^1(G_{K_p}, \Delta_j)$$

and let L_j be the image of $H^1_\Pi(K^{sep}/K, \Delta_j) \longrightarrow \prod_{p\in\Pi} H^1(K_p^{sep}/K_p, \Delta_j)$. Then

$$L_j \simeq H^1_\Pi(G_K, \Delta_j)$$

by Lemma 3.2. Let

$$N_j = \prod_{p\in\Pi} M_p^j \subset I_j$$

where M_p^1 (resp. M_p^2) is the image of G_{2p}/v_1G_{1p} (resp. G_{1p}/v_2G_{2p}) in $H^1(G_{K_p}, \Delta_1)$ (resp. $H^1(G_{K_p}, \Delta_2)$). By the definition of the Selmer group, we have

$$S_j = L_j \cap N_j$$

Now recall that the canonical pairing of Δ_1, Δ_2 with values in ± 1 gives rise to a duality

$$H^1(G_{K_p}, \Delta_1) \otimes H^1(G_{K_p}, \Delta_2) \longrightarrow H^2(G_{K_p}, \pm 1) \longrightarrow \mathbb{Q}/\mathbb{Z} \tag{3.4.1}$$

say

$$\xi_P \otimes \mu_p \longrightarrow \lambda_p(\xi_p, \mu_p) \in \mathbb{Q}/\mathbb{Z}$$

where the first map is a cup-product and the second is taking the invariant map. Further

$$\lambda_p(\xi_p, \mu_p) = 1(\xi_p \in M_p^1, \mu_p \in M_p^2) \tag{3.4.2}$$

We note that the existence of the duality (4.1) implies that

$$|H^1(G_{K_p}, \Delta_1)| = |H^1(G_{K_p}, \Delta_2)|$$

(We've actually computed that in our specific case, they are both equal to 4) and so

$$|I_1| = |I_2|$$

We now define a duality between I_1 and I_2 by putting

$$\Lambda(\bar{\xi}, \bar{\mu}) = \prod_{p\in\Pi} \lambda_p(\xi_p, \mu_p)$$

where

$$\bar{\xi} = \{\xi_p\}_{p\in\Pi} \in I_1, \bar{\mu} = \{\mu_p\}_{p\in\Pi} \in I_2.$$

Further we have

$$\Lambda(\bar{\xi}, \bar{\mu}) = 0$$

for $\bar{\xi} \in N_1$, $\bar{\mu} \in N_2$ because of (4.2), and also for $\bar{\xi} \in L_1$, $\bar{\mu} \in L_2$ because then the local cup-products in (4.1) are the localization of a global cup-product, and the sum of the local invariants of an element of the global $H^2(G_K, \pm 1)$ is zero. (class field theory holds for the entirety of global fields, so the same argument holds for our case) This then implies that

$$\Lambda(\bar{\xi}, \bar{\mu}) = 0$$

for $\bar{\xi} \in N_1 \cap L_1$ and $\bar{\mu} \in N_2 \cup L_2$, where $N_2 \cup L_2$ is the subgroup of I_2 generated by N_2 and L_2, and so

$$|N_1 \cap L_1||N_2 \cup L_2| \leq |I_1| = |I_2|$$

because Λ is non-degenerate. On the other hand

$$|N_2 \cap L_2||N_2 \cup L_2| = |N_2||L_2|$$

so by taking the quotient of the above two formulas, we get

$$\frac{|S_1|}{|S_2|} \leq \frac{|I_2|}{|N_2||L_2|}$$

where we are able to compute the RHS. by definition

$$\frac{|I_2|}{|N_2|} = \prod_{p\in\Pi} \frac{H^1(G_{K_p}, \Delta_2)}{M_p^2}$$

where $M_p^2 = \mathrm{im}(G_{1p}/v_2 G_{2p})$, and then using the exact sequence

$$0 \longrightarrow G_{1p}/v_2 G_{2p} \longrightarrow H^1(G_{K_p}, \Delta_2) \longrightarrow (WC_{2p})_{v_2} \longrightarrow 0$$

we get that

$$\frac{|I_2|}{|N_2|} = \prod_{p\in\Pi} |(WC_{2p})_{v_2}|$$

And $|L_2| = |H^1_\Pi(G_K, \Delta_2)| = 2^P$ by lemma 3.1. All these combined would imply that

$$\frac{|S_1|}{|S_2|} \geq \prod_{p\in\Pi} \frac{2}{|(WC_{1p})_{v_1}|}$$

By switching the index 1 and 2, we also have

$$\frac{|S_1|}{|S_2|} \leq \prod_{p\in\Pi} \frac{2}{|(WC_{2p})_{v_2}|}$$

In our specific case, we could show that $|(WC_{2p})_{v_2}||(WC_{1p})_{1_2}| = 4$ as this is equivalent to show

$$|\frac{H^1(G_{K_p}, \Delta_1)}{G_{2p}/v_1 G_{1p}}||\frac{H^1(G_{K_p}, \Delta_2)}{G_{1p}/v_1 G_{2p}}| = 4$$

i.e.

$$|G_{2p}/v_1 G_{1p}||G_{1p}/v_1 G_{2p}| = 4$$

there are only 4 cases out there which depend on whether elliptic curves E_1 (resp. E_2) have 2 or 4 K_p-rational 2 torsion points. We can show that in the cases where $E_1(K_p)[2] \simeq E_2(K_p)[2]$ (either $\mathbb{Z}/2$ or $\mathbb{Z}/2\times\mathbb{Z}/2$) then $|G_{2p}/v_1 G_{1p}| = |G_{1p}/v_1 G_{2p}| = 2$ while in the cases $E_1(K_p)[2] \neq E_2(K_p)[2]$ □

3.5 Compute $H^1_{v_2}(K_p, \Delta_2)$

We have shown so far that under our setting, we have

$$\mathrm{T}(E_2/E_1) := \frac{S_2}{S_1} = \prod_p \frac{1}{2}|H^1_{v_2}(K_p, \Delta_2)|$$

To use this formula for explicit computation which we will give in the next section to prove theorem 1.1, we examine exactly the size of $\frac{1}{2}|H^1_{v_2}(K_p, \Delta_2)|$. To this end, we need the following lemma of Klagsbrun:

Lemma 3.6. *Suppose E has good reduction at a prime v away from 2 and F/K is a quadratic extension ramified at v. Then $E^F(K_v)$ contains no points of order 4. It follows that $H^1_f(K_v, E^F[2])$ is the image of $E^F(K_v)[2]$ under the Kummer map.*

Proof. This directly follows from [Kla17, Lemma 2.6] which is in the number field version. □

Lemma 3.7.

$$\mathrm{T}(E_2/E_1) := \frac{S_2}{S_1} = \prod_p \frac{1}{2}|H^1_{v_2}(K_p, \Delta_2)| = \prod_p \frac{c_p(E_f)}{c_p(E'_f)}$$

Proof. First of all, we show that for most $p \in K$, $\frac{1}{2}|H^1_{v_2}(K_p, \Delta_2(E'_f))| = \frac{c_p(E_f)}{c_p(E'_f)}$, where $c_p(E)$ is the Tamagawa number at prime p. This can be checked through direct computation. For convenience, assume that we are checking this only for the case where $(\Delta_E \Delta_{E'}, f) = 1$ and for $p|f$.

In this case, we have good reduction at those primes. Subsequently we can apply lemma 5.1. and in particular we have that $E_f(K_p)$ has no point of order 4.

Notice that $\frac{1}{2}|H^1_{v_2}(K_p, \Delta_2(E'_f))|$ is equal to the following by definition

$$E'_f(K_p)/v_1(E_f(K_p)) = E'_f(K_p)[2^\infty]/v_1(E_f(K_p)[2^\infty])$$

as $v_1 : E \longrightarrow E'$ is a 2-isogeny. While the fact that $E_f(K_p)$ and $E'_f(K_p)$ have no point of order 4 deduces

$$E'_f(K_p)[2^\infty]/v_1(E_f(K_p)[2^\infty]) = E'_f(K_p)[2]/v_1(E_f(K_p)[2])$$

Notice that the quadratic twist E_f can be explicitly written into the formula $y^2 = x^3 + Af \cdot x^2 + Bf^2 \cdot x = x(x^2 + Af \cdot x + Bf^2)$. We have $E_f(K_p)[2] \simeq \mathbb{Z}/2 \times \mathbb{Z}/2$ equivalent to the cubic $x(x^2 + Af \cdot x + Bf^2)$ has all its root in K_p which happens if and only if $(\frac{\Delta_{E_f}}{p}) = (\frac{A^2 - 4B}{p}) = 1$.

One can explicitly compute the Tamagawa number $c_p(E_f)$ of E_f and check that for such curve $y^2 = x^3 + Af \cdot x^2 + Bf^2 \cdot x$, we have $(\frac{\Delta_{E_f}}{p}) = (\frac{A^2 - 4B}{p}) = 1$ if and only if $c_p(E_f) = 4$.

Therefore, we have

$$\frac{1}{2}|H^1_{v_2}(K_p, \Delta_2(E'_f))| = E'_f(K_p)/v_1(E_f(K_p)) = E'_f(K_p)[2]/v_1(E_f(K_p)[2]) = \frac{c_p(E_f)}{c_p(E'_f)}$$

and this completes the proof □

3.6 Proof of the main theorem

We recall the notations that will be used in this proof: Elliptic curve $E : y^2 = x^3+Ax^2+Bx$ is defined over $K = \mathbb{F}_q(t)$ and we have a 2-isogeny $v_1 : E \longrightarrow E'$, where $E' : y^2 = x^3 - 2Ax + (A^2 - 4B)x$, is the dual of E. The Tamagawa factor is defined as follows:

$$T(E'/E) := \frac{S_2}{S_1} = \prod_{p \in K} \frac{c_p(E')}{c_p(E)}$$

where p are places of K and $c_p(E)$ denotes the Tamagawa number of E at place p. Explicitly $c_p(E)$ is given by the following ratio $|E(K_p)|/|E_0(K_p)|$ where K_p denotes the local field of K at prime p.

We denote by E_f a quadratic twist of E with $f(t)$ being a square free polynomial that belongs to K. E_f has an explicit Weierstrass equation:

$$fy^2 = x^3 + Ax^2 + Bx$$

Notice $c_p(E_f) = 1$ at all places that E_f has a good reduction, so we only need to count those primes p where p either divides $\Delta(E_f)$ or $\Delta(E'_f)$. We can compute explicitly that $\Delta(E_f) = 16B^2(A^2 - 4B) \cdot f^6$ and $\Delta(E'_f) = 16B(A^2 - 4B)^2 \cdot f^6$.

We define $C(K, X) :=$ {square free $f \in K$: deg(f) $<$ X} and assume that E has $E(K) \simeq \mathbb{Z}/2\mathbb{Z}$ that does not have a cyclic isogeny defined over $K(E[2])$.

We show that as f varies through all square free polynomials in K, at least half of the quadratic twists of E have arbitrarily large Tamagawa factor. i.e. for any fixed r, we have

$$\liminf_{X \to \infty} \frac{|\{\text{sqaure free } f \in C(K, X) \text{: } T(E'_f/E_f) \geq r \mid}{|C(K, X)|} \geq \frac{1}{2}$$

Proof. It suffices to prove the claim for a subset of $C(K, X)$ which consists of all polynomials f with $(f, \Delta\Delta') = 1$. Because for those f such that $(f, \Delta\Delta') = p(t)$ where $p(t) \neq 1$ is some fixed square free polynomial, it would be equivalent to prove the coprime version of the statement for alternative elliptic curves E_p and E'_p.(Notice the real condition that the later proof relies upon is that $\Delta_E\Delta_{E'}$ is a non-square polynomial in K, and this would be preserved by $\Delta_{E_p}\Delta_{E'_p}$)

From this point on, we slightly abuse the notation $C(K, X)$ to refer to the collection of all square free polynomials $f \in K$ such that $(f, \Delta_E \Delta_{E'}) = 1$. A computation of Tamagawa factors using Tate's algorithm shows that for all $p|f$, we have

$$C_p = \begin{cases} 4 & \text{if } (\frac{A^2-4B}{p}) = (\frac{\Delta_E}{p}) = 1 \\ 2 & \text{if } (\frac{\Delta_E}{p}) = -1 \end{cases}$$

There are only finitely many p that divides $\Delta_E \Delta_{E'}$ and each of them is universally bounded by some fixed constant through the entire quadratic twist family, so we can simplify and rewrite $T(E'_f/E_f)$ into:

$$T(E'_f/E_f) = \prod_{p|f} \frac{c_p(E'_f)}{c_p(E_f)} + O(1)$$

If we could show that Theorem 5.1 is true for $\prod_{p|f} \frac{c_p(E'_f)}{c_p(E_f)}$, then it would also hold for $T(E'_f/E_f)$ as they only differ by some bounded constant. Define

$$t(f) = \sum_{p|f} log_2 \frac{c_p(E'_f)}{c_p(E_f)} = \sum_{p|f} \frac{(\frac{\Delta}{p}) - (\frac{\Delta'}{p})}{2}$$

We want to show that $t(f)$ converges to a normal distribution as the degree of f approaches ∞.

Define the set $A_N = \{$ f | square free polynomials with deg(f) $\leq$ N$\}$ and endow a uniform discrete probability on it. Define two functions on this probability space as following:

$$g_p(f) = \mathbb{1}_{p|f} \cdot \mathbb{1}_{(\frac{\Delta}{p})=1} \cdot \mathbb{1}_{(\frac{\Delta'}{p})=-1}$$

$$h_p(f) = \mathbb{1}p|f \cdot \mathbb{1}(\frac{\Delta}{p}) = -1 \cdot \mathbb{1}(\frac{\Delta'}{p}) = 1$$

Fix $\epsilon > 0$, for all primes p with $\deg(p) \leq \epsilon \cdot N$, we have the following estimate:

$$\mathbb{E}_N(g_p(f)) = \mathbb{P}_N(p|f) = \frac{1}{q^p + 1} + O(\frac{1}{q^{(1-\epsilon)N}})$$

Recall what we want to study here is the variance of $t(f) := \sum_p g_p(f) - \sum_p h_p(f)$. Define $G(N) := \sum_{p<\epsilon N} g_p(f)$ and $H(N) := \sum_{p<\epsilon N} h_p(f)$. For any f whose degree $\leq N$, it could have at

most $\frac{1}{\epsilon}$ prime factors with degrees $\geq \epsilon \cdot N$. Thus we have

$$t(f) = G(N) - H(N) + \mathcal{O}_\epsilon(1)$$

Now we can define random variables to model the aforementioned $g_p(f)$ and $h_p(f)$:

$$X_p = \begin{cases} 1 & \text{with probability } \frac{1}{q^p+1} \\ 0 & \text{with probability } \frac{q^p}{q^p+1} \end{cases}$$

if $(\frac{\Delta}{p}) = 1$ and $(\frac{\Delta'}{p}) = -1$, and likewise define

$$Y_p = \begin{cases} 1 & \text{with probability } \frac{1}{q^p+1} \\ 0 & \text{with probability } \frac{q^p}{q^p+1} \end{cases}$$

if $(\frac{\Delta}{p}) = -1$ and $(\frac{\Delta'}{p}) = 1$. Roughly speaking, X_p is the probability of $p|f$ without the constraint that $\deg(p) \leq N$.

We can directly compare $P(X_p = x, Y_p = y)$ to $P(X_p = x) \cdot P(Y_p = y)$. We get that $\{X_p\}_p \cup \{Y_p\}_p$ are independent except at $X_p = 1$ and $Y_p = 1$. As $\{X_p\}_p$ is a sequence of independent random variables with finite expected values $\sim \frac{1}{q^P}$ (here P is the degree of the polynomial p) and variance $\sim \frac{1}{q^P}$. Denote $\sum_{P \leq \epsilon N} X_p$ by X_N, then Lyapunov central limit theorem deduces that

$$X_N \longrightarrow N(\frac{1}{4}\text{loglogN} + \mathcal{O}(1), \frac{1}{4}\text{loglogN} + \mathcal{O}(1)) + \mathcal{O}(1)$$

The same argument also applies to $Y_N = \sum_{P \leq \epsilon N} Y_p$.

The reason that we could use X_N and Y_N to model G_N and H_N is that they would finally approach the same distribution as $N \longrightarrow \infty$. By method of moments, it suffices to check that the mixed moments of $F(N)$ and $G(N)$ converge to those of X_N and Y_N. We have by construction:

$$\begin{aligned} \mathbb{E}_N(G_N^k H_N^k) &= \sum_{\substack{P_1 \cdots P_k \leq \epsilon N \\ q_1 \cdots q_k \leq \epsilon N}} \mathbb{P}_N(p_i | f \text{ and } q_j | f) \\ &= \mathbb{E}(X_N^k Y_N^k) + \mathcal{O}(\frac{(logN)^{k+l+1}}{q^{(1-\epsilon)N}}) \end{aligned}$$

from which we can compute

$$\mathbb{E}_N((G_N - \mathbb{E}_N(F_N))^k (H_N - \mathbb{E}_N(H_N))^l) = \mathbb{E}((X_N - \mathbb{E}_N(X_N))^k (Y_N - \mathbb{E}_N(Y_N))^l) + O(\frac{(logN)^{k+l+1}}{q^{(1-\epsilon)N}})$$

This shows that the distribution $G_N \longrightarrow X_N$ and $H_N \longrightarrow Y_N$ as N approaches ∞.

Hence we can conclude that $t_N := log_2(S_2/S_1) = G_N - H_N$ eventually converges to a normal distribution $N(O(1), \frac{1}{2}\text{loglog}N)$ which implies that $\mathbb{P}(t(f) \geq r) \longrightarrow \frac{1}{2}$ as N approaches ∞ for any fixed constant r as claimed.

□

Bibliography

[JGZ74] Ju. G. Zarhin, *Noncommutative cohomology and Mumford groups*, Mat. Zametki **15** (1974), 415-419. ↑5

[PR12] Bjorn Poonen and Eric Rains, *Random maximal isotropic subspaces and Selmer groups*, J. Amer. Math. Soc. **25** (2012), no. 1, 245-269, DOI 10.1090/s0894-0347-2011-00710-8. ↑5, 7

[CP80] David Cox and Walter Parry, *Torsion in elliptic curves over k(t)*, Compositio Mathematica **41.3** (1980), 337-354. ↑8

[Ces16] Kestutis Cesnavicius, *Selmer groups as flat cohomology groups*, J. Ramanujan Math. Soc. **31.1** (2016), 31-61. ↑12

[CH05] Alina Carmen Cojocaru and Chris Hall, *Uniform Results for Serre's Theorem for Elliptic Curves*, IMRN **50** (2005), 3065-3080. ↑8, 14, 15, 18, 25

[Ell14] Jordan S Ellenberg, *Arizona Winter School 2014 Course Notes: Geometric Analytic Number Theory*, 2014. Available at https://swc.math.arizona.edu/aws/2014/2014EllenbergNotes.pdf. ↑9

[Lan21] Aaron Landesman, *The geometric average size of Selmer groups over function field*, Algebra & Number Theory **15** (2021), 673-709, DOI 10.2140/ant.2021.15.673. ↑8

[Hal08] Chris Hall, *Big Symplectic Or Orthogonal Monodromy Modulo l*, Duke Math. J. **141.1** (2008), 179-203. ↑

[Kat98] Nicholas M Katz, *Twisted L-Functions and Monodromy*, Princeton University Press, 1998. https://web.math.princeton.edu/ nmk/twistedLfctnov052001.pdf. ↑18

[FLR20] Tony Feng, Aaron Landesman, and Eric Rains, *The geometric distribution of Selmer groups of elliptic curves over function fields* (2020). Preprint available at https://arxiv.org/abs/2003.07517 (2020). ↑8

[Mil13] James S Milne, *Lectures on Etale Cohomology*, 2013. Available at https://jmilne.org/math/2013. ↑9, 16

[Poo10] Bjorn Poonen, *Rational Points on Varieties*, American Mathematical Society, 2010. ↑

[Sil91] Joseph H Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves* (1991). ↑4, 13

[PR12] Bjorn Poonen and Eric Rains, *Random maximal isotropic subspaces and Selmer groups*, J. Amer. Math. Soc. **25.1** (2012), 245-269. ↑14

[Bro94] Heath Brown, *The size of Selmer groups for the congruent number problem*, Inventiones mathematicae **2** (1994), 331-370. ↑30

[KO15] Zev Klagsbrun and Robert Oliver, *The distribution of 2-Selmer ranks of quadratic twists of elliptic curves with partial two-torsion*, Methematika **62** (2015), 67-78, DOI 10.1112/S0025579315000121. ↑31

[Kla17] Zev Klagsbrun, *Selmer ranks of quadratic twists of elliptic curves with partial rational two-torsion*, Tans. Amer. Math. Soc. **369** (2017), 3355-3385, DOI https://doi.org/10.1090/tran/6744. ↑40

[Kan10] D.M. Kane, *On the ranks of the 2-Selmer groups for the congruent number problem* (2010). available at http://arxiv. org/abs/1009.1365. ↑30

[SD08] P. Swinnerton-Dyer, *The effect of twisting on the 2-Selmer group*, Cambridge University Press, 2008. In Mathematical Proceedings of the Cambridge Philosophical Society. ↑30

[KMR11] Z Klagsbrun, B Mazur, and K Rubin, *Selmer ranks of quadratic twists of elliptic curves* (2011). available at http://arxiv.org/pdf/1111.2321v1. ↑30

[Cas65] J.W.S. Cassels, *Arithmetic on curves of genus 1. VIII. On conjectures of Birch and Swinnerton-Dyer*, Jour. fur die reine und ang. Mathematik **217** (1965), 180-199. ↑31, 33