The asymptotic size of Selmer groups over function fields

Mohit Hulse
Mentor: Gefei Dang
Project suggested by: Niven Achenjang, Gefei Dang, and Wei Zhang
UROP+ Final Project: Summer 2023

Abstract

Let K be the function field of a smooth projective curve and $\ell \neq \operatorname{char} K$ a prime. We prove an asymptotic bound on the $\mathbb{F}_\ell$-dimension of the ℓ-Selmer groups of elliptic curves over K ordered by height. A short exposition about the Selmer group, reduction, and Néron models is also included.

Contents

1 Introduction **1**

2 Background **2**
2.1 The Selmer and Tate-Shafarevich groups 2
2.2 Types of reduction 3
2.3 Néron models 4
2.3.1 Néron models under reduction 4

3 Notation and conventions **5**

4 Results **5**

5 Proof **5**
5.1 The case of full torsion 6
5.2 Deletion, base-change, and cohomology 7
5.3 Places of split multiplicative reduction 8
5.4 Places of good reduction 9
5.5 Applying inflation-restriction 10

6 Future work **12**

§1. Introduction

Let E be an elliptic curve over a number field K. The weak Mordell-Weil Theorem states that for any integer n, the group $E(K)/nE(K)$ is finite. This is a crucial step in proving the celebrated Mordell-Weil Theorem—that elliptic curves over number fields are finitely generated.

The proof of the weak Mordell-Weil Theorem involves the construction of the *n-Selmer group* $\mathrm{Sel}_n(E)$, a certain subgroup of the Galois cohomology group $H^1(K, E[n])$, where $E[n]$ denotes the n-torsion points on E. The finiteness of this group implies the theorem (see the exact sequence (2.1)).

More generally, we may construct the n-Selmer group in the same way when K is any global field. Ordering the elliptic curves over K by height (see Section 3) allows us to study trends in their size.

Poonen and Rains [PR11] conjectured the average size of $\mathrm{Sel}_n(E)$ to be the sum of divisors of n, a result proven by Bhargava and Shankar when $n = 2, 3, 4, 5$ [BS13c, BS13d, BS13a, BS13b] for elliptic curves over $\mathbb{Q}$. The conjecture is also known to hold for $n = 2, 3$ when we restrict to various families of elliptic curves [BH22, ABS22, SSW19, HB94, SD08, Kan13].

Over $\mathbb{F}_q(t)$, the cases of $n = 2, 3$ have been settled by Hồ, Lê Hùng, and Ngô [HHN14] (over any function field) and de Jong [dJ02] respectively. Landesman [Lan21] proves that the result holds for all n in the limit $q \to \infty$.

In contrast to the average size, the asymptotic behaviour $\#\operatorname{Sel}_n(E)$ seems to have been little studied. In this paper, we take K to be the function field of a curve C over a finite field and bound $\operatorname{Sel}_\ell(E)$, for all primes $\ell \neq \operatorname{char} K$. We prove the following asymptotic result

Theorem 1.1. *Let K be the function field of a smooth projective curve C over a finite field of characteristic p and $\ell \neq p$ a prime. Then as E/K varies over elliptic curves ordered by height,*

$$\dim_{\mathbb{F}_\ell} \operatorname{Sel}_\ell(E) = \mathcal{O}\left(\frac{\operatorname{ht} E}{\log(\operatorname{ht} E)}\right).$$

In Theorem 4.1 we show that the $\mathbb{F}_\ell$-dimension of $\operatorname{Sel}_\ell(E)$ is at most a linear function (with explicit coefficients) in the number of places of bad reduction of E/K and the genus of C.

Our proof of Theorem 4.1 in Section 5 proceeds by first restricting to elliptic curves with full ℓ-torsion. This ensures that only good or split-multiplicative reduction occurs, which simplifies dealing with the Néron model $\mathcal{E}$ of E. Following [Lan21] gives us a way to bound the size of the Selmer group by an étale cohomology group with coefficients in $\mathcal{E}$. The bulk of the proof (Section 5.1) is devoted to bounding this cohomology group. Finally, we extend the to all elliptic curves via a base-change to adjoin all ℓ-torsion.

For the reader's convenience (and the author's), we provide a short exposition of Selmer groups, types of reduction, and Néron models in Section 2.

Acknowledgements

The author is extremely grateful to Gefei Dang for her mentorship and guidance. The author would also like to thank Niven Achenjang, for suggesting the project and approach, and Aaron Landesman, for helpful conversations and pointers. This work took place under the MIT UROP+ program.

§2. Background

We briefly discuss aspects of the theory of elliptic curves used in our proof of Theorem 4.1. In each section, we provide a reference with a more thorough treatment of the topic.

§2.1. The Selmer and Tate-Shafarevich groups

(Reference: [Sil09] Silverman, *The arithmetic of elliptic curves*, X.)

Let K be a global field, E/K an elliptic curve, and $\bar{K}$ a separable closure of K. For each positive integer n, the group law on E allows us to define the multiplication by n map, which we denote $[n]$. The kernel $E[n]$ of this map is the *n-torsion* of E (more generally, we will write $G[n]$ for the n-torsion of a group G).

Taking Galois cohomology of the exact sequence

$$0 \to E(\bar{K})[n] \to E(\bar{K}) \xrightarrow{[n]} E(\bar{K}) \to 0$$

yields the exact sequence

$$0 \to \frac{E(K)}{nE(K)} \to H^1(K, E(\bar{K})[n]) \to H^1(K, E(\bar{K}))[n] \to 0.$$

Similarly, working in the completion K_ν of K at some place ν instead, we obtain

$$0 \to \frac{E(K_\nu)}{nE(K_\nu)} \to H^1(K_\nu, E(\bar{K_\nu})[n]) \to H^1(K_\nu, E(\bar{K_\nu}))[n] \to 0.$$

The inclusions $E(K) \hookrightarrow E(K_\nu)$ and $\mathrm{Gal}(\bar{K}_\nu/K_\nu) \hookrightarrow \mathrm{Gal}(\bar{K}/K)$ (we fix an embedding $\bar{K} \hookrightarrow \bar{K}_\nu$) induce maps on H^1. Taking the product over all places ν, we have a diagram

$$\begin{array}{ccccccccc} 0 \to & \dfrac{E(K)}{nE(K)} & \to & H^1(K, E[n]) & \to & H^1(K, E)[n] & \to & 0 \\ & \downarrow & & \downarrow & & \downarrow & & \\ 0 \to & \displaystyle\prod_\nu \frac{E(K_\nu)}{nE(K_\nu)} & \to & \displaystyle\prod_\nu H^1(K_\nu, E[n]) & \to & \displaystyle\prod_\nu H^1(K_\nu, E)[n] & \to & 0. \end{array}$$

We now define the n-Selmer group and the Tate-Shafarevich group of E

$$\mathrm{Sel}_n(E/K) = \ker\left(H^1(K, E[n]) \to \prod_\nu H^1(K_\nu, E)[n]\right)$$

$$Ш(E/K) = \ker\left(H^1(K, E) \to \prod_\nu H^1(K_\nu, E)\right).$$

These two groups fit together to give us the exact sequence

$$0 \to E(K)/nE(K) \to \mathrm{Sel}_n(E/K) \to Ш(E/K)[n] \to 0. \tag{2.1}$$

The n-Selmer group is a module over $\mathbb{Z}/n\mathbb{Z}$ (since $H^1(K, E[n])$ certainly is). In particular, if $n = \ell$ is prime, $\mathrm{Sel}_\ell(E)$ is a $\mathbb{F}_\ell$-vector space whose dimension we seek to bound.

§2.2. Types of reduction

(Reference: [Sil09] Silverman, *The arithmetic of elliptic curves*, VII.)

Let R be a discrete valuation ring with fraction field K, maximal ideal $\mathfrak{p}$, residue field k, and discrete valuation $\nu_\mathfrak{p}$. If E/K be an elliptic curve, we may consider the Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{2.2}$$

which minimizes $\nu_\mathfrak{p}(\Delta)$, where Δ is the discriminant of (2.2). We call such an equation a *minimal Weierstrass equation* for E and the corresponding Δ the *minimal discriminant*. (In the global case, the minimal discriminant is obtained by simply multiplying together all the local minimal discriminants.)

Reducing (2.2) modulo $\mathfrak{p}$ gives us a curve $\tilde{E}/k$, which may have some singular points. This brings us to the types of reduction:

(i) If $\tilde{E}$ is smooth, E has *good reduction* and $\nu_\mathfrak{p}(\Delta) = 0$.

(ii) If $\tilde{E}$ has a node, E has *multiplicative reduction*. In addition, if the slopes of the tangent line at E are in k the multiplicative reduction is said to be *split*.

(iii) If $\tilde{E}$ has a cusp, E has *additive reduction*.

Deleting any singular points gives us a smooth curve $\tilde{E}_{\mathrm{ns}}$ with a group law coming from that on E. Let E_0 be the locus of points of E whose reduction modulo $\mathfrak{p}$ lies in E_{ns}, and let $E_1 \subset E_0$ consist of those whose reduction is the identity. It turns out that E_0 and E_1 are subgroups of E and there is an exact sequence [Sil09, Proposition VII.2.1]

$$0 \to E_1(K) \to E_0(K) \to \tilde{E}_{\mathrm{ns}}(K) \to 0. \tag{2.3}$$

The group structure of $\tilde{E}_{\mathrm{ns}}$ is qualitatively determined by the reduction type.

Lemma 2.1. *Let K be a discrete valuation ring with perfect residue field k. If E/K is an elliptic curve,*

(i) If E has good reduction, $\tilde{E} = \tilde{E}_{ns}$ is an elliptic curve.

(ii) If E has multiplicative reduction, $\tilde{E}_{ns}(\bar{k}) \simeq \bar{k}^\times$.

(iii) If E has additive reduction, $\tilde{E}_{ns}(\bar{k}) \simeq \bar{k}^+$.

Proof. [Sil09, Proposition VII.5.1] □

§2.3. Néron models

(Reference: [Sil94] Silverman, *Advanced topics in the arithmetic of elliptic curves*, IV.)

Much of our proof thus involves working with the Néron model, and in this section, we briefly define them and outline some important properties.

Let R be a Dedekind domain (or more generally, a Dedekind scheme) with fraction field K and E/K be an elliptic curve[1]. A *Néron model* for E over R is a smooth separated group scheme $\mathcal{E}$ over R, whose generic fiber is (isomorphic to) E and satisfies the *Néron lifting property*:

For any smooth separated scheme X over R with generic fiber X_K, there is a bijection

$$\mathrm{Hom}_K(X_K, E) \simeq \mathrm{Hom}_R(X, \mathcal{E}).$$

In particular, when $X = \operatorname{Spec} R$ its generic fiber is $\operatorname{Spec} K$ and we have $E(K) \simeq \mathcal{E}(R)$.

It can be shown that Neŕon models exist for elliptic curves, and are unique up to unique isomorphism [Sil94, Proposition IV.5.2]. The identity component $\mathcal{E}^0$ is isomorphic to the smooth part of a minimal Weierstrass model for E [Sil94, Corollary IV.9.1].

§2.3.1. Néron models under reduction

We characterize the fiber of the Néron model over $\mathfrak{p}$ in terms of the reduction type of E at p.

We temporarily restrict to the case that R is a discrete valuation ring with maximal ideal $\mathfrak{p}$. The identity component $\mathcal{E}^0$ of the Néron model can be characterized by the type of reduction of E at $\mathfrak{p}$. More precisely, the special fiber $\mathcal{E}^0_{\mathfrak{p}}$ is isomorphic to (see [Sil94, Exercise 4.21])

- an elliptic curve if E has good reduction;
- the multiplicative group scheme $\mathbb{G}_{m,\mathfrak{p}}$ if E has split multiplicative reduction;
- a (quadratic) twist of $\mathbb{G}_{m,\mathfrak{p}}$ if E has non-split multiplicative reduction;
- the additive group scheme $\mathbb{G}_{a,\mathfrak{p}}$ if E has additive reduction.

In the global case, we need the following lemma.

Lemma 2.2. *Let C be smooth projective curve with function field K and E/K an elliptic curve. Let $\mathfrak{p} \in C$ be a place of K where E has split multiplicative reduction. If $\mathcal{E}/C$ is a Néron model for E, then $\mathcal{E}^0_{\mathfrak{p}} \simeq \mathbb{G}_{m,\mathfrak{p}}$.*

Proof. Let R be the valuation ring of $\mathfrak{p}$ (so $\operatorname{Spec} R \subset C$ and contains the generic point) and $\mathcal{E}'/R$ be the base-change $\mathcal{E} \times_C R$. We claim that $\mathcal{E}'$ is a Néron model for E over R. First note that its generic fiber is

$$\mathcal{E}' \times_R K \simeq \mathcal{E} \times_C R \times_R K \simeq \mathcal{E} \times_C K \simeq E.$$

Next, if a scheme T/R has generic fiber T_K the Néron mapping property gives $\mathcal{E}(T) \simeq E(T_K)$ and since $\mathcal{E}' = \mathcal{E} \times_C R$ we have $\mathcal{E}(T) \simeq \mathcal{E}'(T)$ by pulling back. We have shown that $\mathcal{E}'$ has the Néron mapping property.

Taking identity components, we see that

$$\mathcal{E}^0_{\mathfrak{p}} \simeq \mathcal{E}^0 \times_C \mathfrak{p} \simeq \mathcal{E}^0 \times_C R \times_R \mathfrak{p} \simeq \mathcal{E}'^0 \times_R \mathfrak{p} \simeq \mathcal{E}'^0_{\mathfrak{p}}$$

and [Sil94, Exercise 4.21] shows that $\mathcal{E}'^0_{\mathfrak{p}} \simeq \mathbb{G}_{m,\mathfrak{p}}$, so we are done. □

[1] the same definition works for any abelian variety

§3. Notation and conventions

- We work over the function field K of a smooth projective curve $C/\mathbb{F}_q(t)$. Thus, K is a finite (geometric) extension of $\mathbb{F}_q(t)$. We write p for $\operatorname{char} K$ and g for the genus of C.
- Let E/K be an elliptic curve and S be the set of places K where E has bad reduction. Since the places of K are in bijection with points of C, we identify S with a subset of C.
- The *height* $\operatorname{ht} E$ of E is $\frac{1}{12}\deg\Delta$, where Δ is the minimal discriminant of E. When we study asymptotic behavior, we always keep K (and hence also g, p, and q) fixed and order elliptic curves by height.
- Denote the Néron model of E over C by $\mathcal{E}$ and its identity component by $\mathcal{E}^0$.
- Finally, we fix a prime number $\ell \neq p$.

§4. Results

As noted in Section 2.1, the ℓ-Selmer group $\operatorname{Sel}_\ell(E)$ of E is an $\mathbb{F}_\ell$-vector space. We seek to bound its dimension $\dim_{\mathbb{F}_\ell}\operatorname{Sel}_\ell(E)$ in terms of $\#S$ and constants depending only on K. To this end, we have the following main theorem.

Theorem 4.1. *In the notation of Section 3, we have*

$$\dim_{\mathbb{F}_\ell}\operatorname{Sel}_\ell(E) \leq 4r^4 g + (4r^8 + 3r^4)\#S + 2r^4 + 4.$$

where $r = \ell$ for $\ell > 3$, $r = 8$ for $\ell = 2$, and $r = 9$ for $\ell = 3$.

Together with a simple fact about divisors on a curve over a finite field, we can quickly obtain Theorem 1.1.

Proof of Theorem 1.1, assuming Theorem 4.1. First we recall that for divisors D on a curve over a finite field, $\#\operatorname{supp} D = \mathcal{O}(\deg D/\log(\deg D))$ (such a curve has only finitely many points of fixed degree). Taking $D = \Delta$, a divisor on C, we see that

$$\#S = \#\operatorname{supp}\Delta = \mathcal{O}\left(\frac{\operatorname{ht} E}{\log(\operatorname{ht} E)}\right),$$

and note that C (hence g) is fixed as we let E vary to deduce the result from Theorem 4.1. □

We also sketch an approach towards extending these results to the case $p = \ell$ in Section 6.

§5. Proof

We first follow [Lan21] in reducing our problem to bounding a certain étale cohomology group with coefficients in E's Néron model.

Lemma 5.1. *In the notation of Section 3,*

$$\#\operatorname{Sel}_\ell(E) \leq \ell^2 \cdot \#H^1_{\acute{e}t}(C, \mathcal{E}^0[\ell]).$$

Proof. We recall [Lan21, Lemma 3.26]:

$$\#\operatorname{Sel}_\ell(E) \leq \#H^0_{\text{ét}}(C, \mathcal{E}[\ell]) \cdot \#H^1_{\text{ét}}(C, \mathcal{E}^0[\ell]),$$

and then finish by bounding the first factor

$$H^0_{\text{ét}}(C, \mathcal{E}[\ell]) = \mathcal{E}[\ell](C) = \mathcal{E}(C)[\ell] = E(K)[\ell] \leq (\mathbb{Z}/\ell\mathbb{Z})^2,$$

where we have used the Néron mapping property $\mathcal{E}(C) \simeq E(K)$. □

Additive reduction and non-split multiplication complicate matters, so we restrict to elliptic curves with only good reduction or split multiplicative reduction. This way, we only need to deal with when each fiber of $\mathcal{E}^0$ is an elliptic curves or a torus (see Section 2.3.1).

We will also need ℓ-torsion points in $E(K)$, so we also restrict to elliptic curves having full ℓ-torsion. It turns out that this condition also implies the previous one.

Lemma 5.2. *Let E/K be an elliptic curve over any field K of characteristic p. Let $\ell > 4$ be an integer (possibly composite) coprime to p and suppose $E(\bar{K})[\ell] \subset E(K)$. Then E has only good or split multiplicative reduction at every place of K.*

Proof. Assume that E/K has additive or non-split multiplicative reduction at some place $\mathfrak{p}$ of K. Let $K_\mathfrak{p}$ be the completion of K at $\mathfrak{p}$ and k be its residue field.

By [Sil09, Theorem VII.6.1], $E(K_\mathfrak{p})/E_0(K_\mathfrak{p})$ is a finite group of order at most 4, and thus has no ℓ-torsion (as $\ell \geq 5$). Since $E(K_\mathfrak{p})[\ell]$ has order ℓ^2, we see that $E_0(K_\mathfrak{p})[\ell]$ must also have order r^2.

Consider the exact sequence (2.3),

$$0 \to E_1(K_\mathfrak{p}) \to E_0(K_\mathfrak{p}) \to \tilde{E}_{\mathrm{ns}}(k) \to 0,$$

whence taking ℓ-torsion yields another:

$$0 \to E_1(K_\mathfrak{p})[\ell] \to E_0(K_\mathfrak{p})[\ell] \to \tilde{E}_{\mathrm{ns}}(k)[\ell].$$

We now use Lemma 2.1 to identify the last term. If E has additive reduction at $\mathfrak{p}$ then $\tilde{E}_{\mathrm{ns}}(\bar{k}) \simeq \bar{k}^+$ and thus has no ℓ-torsion (since $\ell \neq p$). On the other hand, multiplicative reduction means that $\tilde{E}_{\mathrm{ns}}(\bar{k}) \simeq \bar{k}^\times$, so its ℓ-torsion has order ℓ. In either case, $\#\tilde{E}_{\mathrm{ns}}(k)[\ell] \leq \ell$ and

$$\ell^2 = \#E_0(K_\mathfrak{p})[\ell] \leq \#E_1(K_\mathfrak{p})[\ell] \cdot \#\tilde{E}_{\mathrm{ns}}(k)[\ell] \leq \ell,$$

where we have used the fact that $E_1(K_\mathfrak{p})$ has no ℓ-torsion [Sil09, Proposition VII.3.1]. This is the desired contradiction. □

Finally in Section 5.5, we show that performing a base change to an extension of K to make E have full ℓ-torsion. The general result will then follow via an application of inflation-restriction.

§5.1. The case of full torsion

In this section, we assume that E has full ℓ-torsion and prove Theorem 4.1 for such E. The main results are

Lemma 5.3. *Adopt the notation of Section 3 and assume E has full ℓ-torsion. Then,*

$$\#H^1_{\acute{e}t}(C, \mathcal{E}^0[\ell]) \leq \ell^{4g+3\#S+2}$$

Theorem 5.4. *Adopt the notation of Section 3 and assume E has full ℓ-torsion. Then,*

$$\dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell(E) \leq 4g + 3\#S + 4.$$

Proof. Immediate from Lemma 5.1 and Lemma 5.3. □

To prove Lemma 5.3 we will deal with the two possible kinds of reduction separately, by repeatedly deleting places with split multiplicative reduction until we are left with only places of good reduction.

§5.2. Deletion, base-change, and cohomology

We prove some general results about the behaviour cohomology under the operations of cutting away a closed subscheme and fiber products. At the end of the section, we apply these to the problem at hand.

Lemma 5.5. *If $f\colon X \to Y$ is an étale morphism of schemes and $\mathcal{F}$ is an abelian sheaf on $X_{ét}$, there is an injection*

$$0 \to H^1_{ét}(Y, f_*\mathcal{F}) \to H^1_{ét}(X, \mathcal{F}).$$

Proof. These are simply the first three terms of the low-degree exact sequence arising from the Leray spectral sequence. □

Lemma 5.6. *Let X be a scheme and $\mathcal{G}$ be a group scheme over X. If $f\colon Y \to X$ is an étale morphism of schemes then $f^{-1}\mathcal{G}$ and $\mathcal{G}_Y \simeq \mathcal{G} \times_X Y$ are isomorphic as sheaves on $Y_{ét}$.*

Proof. If $U \to Y$ is an étale morphism, then $\Gamma(U, f^{-1}\mathcal{G}) = \mathrm{Hom}_X(\mathcal{G}, U)$. On the other hand,

$$\Gamma(U, \mathcal{G}_Y) = \mathrm{Hom}_Y(\mathcal{G}_Y, U) \simeq \mathrm{Hom}_X(\mathcal{G}, U),$$

with the isomorphism of Hom-sets arising from the fiber product. □

We need an analogue of the previous result, but for the inclusion of a closed point. We remark that this also easily implies the result for discrete unions of closed points.

Lemma 5.7. *Let X be a scheme, $i\colon \mathfrak{p} \hookrightarrow X$ a closed point, and $\mathcal{G}/X$. Then $i^{-1}\mathcal{G}$ and $\mathcal{G}_{\mathfrak{p}}$ are isomorphic as étale sheaves on $\mathfrak{p}$.*

Proof. We show that the natural map $i^{-1}\mathcal{G} \to \mathcal{G}_{\mathfrak{p}}$ induces an isomorphism on stalks. Let $\bar{\mathfrak{p}} \to \mathfrak{p}$ be a (the) geometric point of $\mathfrak{p}$. The stalk of $i^{-1}\mathcal{G}$ at $\bar{\mathfrak{p}} \to \mathfrak{p}$ is the same as that of $\mathcal{G}$ at $\bar{\mathfrak{p}} \to \mathfrak{p} \to X$,

$$\mathrm{colim}_U\, \mathcal{G}(U) = \mathcal{G},$$

where U runs over étale neighborhoods of $\bar{p} \to X$. On the other hand, the stalk of $\mathcal{G}_{\mathfrak{p}}$ at $\bar{\mathfrak{p}}$ is

$$\mathrm{colim}_V\, \mathcal{G}_{\mathfrak{p}}(V) = \mathrm{colim}_V\, \mathcal{G}(V)$$

where V runs over étale neighborhoods of $\bar{p} \to X$ (the equality follows from the definition of the fiber product). To see that these two colimits are the same, we note that any U gives us a V by base-change from X to $\mathfrak{p}$ and conversely, [Gro67, Proposition 18.I.I] tells us that any V comes from some U by base-change. We are done. □

The first of the next two lemmas lets us break up cohomology across two complementary subschemes. The second helps us go the other way, from the part to the whole.

Lemma 5.8. *Let $\mathcal{G}/X$ be a group scheme, $Z \subset X$ a discrete union of finitely many closed points of X , and $U = X \setminus Z$. If $j\colon U \to X$ denotes the open immersion of U, then*

$$\#H^1_{ét}(X, \mathcal{G}) \leq \#H^1_{ét}(C, j_!\mathcal{G}_U) \cdot \#H^1_{ét}(Z, \mathcal{G}_Z).$$

Proof. Let $i\colon Z \to X$ be the closed immersion of Z. From [Sta18, Lemma 095L], we have an exact sequence of sheaves

$$0 \to j_!j^{-1}\mathcal{G} \to \mathcal{G} \to i_*i^{-1}\mathcal{G} \to 0,$$

so taking cohomology we have

$$\#H^1_{\text{ét}}(X, \mathcal{G}) \leq \#H^1_{\text{ét}}(X, j_!j^{-1}\mathcal{G}) \cdot \#H^1_{\text{ét}}(X, i_*i^{-1}\mathcal{G}).$$

Through Lemma 5.6 and Lemma 5.7 we turn the inverse images into fiber products:

$$\#H^1_{\text{ét}}(X, \mathcal{G}) \leq \#H^1_{\text{ét}}(X, j_!\mathcal{G}_U) \cdot \#H^1_{\text{ét}}(X, i_*\mathcal{G}_Z).$$

Lemma 5.5 then finishes the proof. □

Lemma 5.9. *Let $\mathcal{G}/X$ be a group scheme, $Z \subset X$ a discrete union of finitely many closed points of X , and $U = X \setminus Z$. If $j\colon U \to X$ denotes the open immersion of U, then*

$$\#H^1_{\acute{e}t}(X, j_!\mathcal{G}_U) \leq \#\mathcal{G}_Z(Z) \cdot \#H^1_{\acute{e}t}(X, \mathcal{G})$$

Proof. Let $i\colon Z \to X$ be the closed immersion of Z. As in the previous lemma, we have an exact sequence from [Sta18, Lemma 095L],

$$0 \to j_!j^{-1}\mathcal{G} \to \mathcal{G} \to i_*i^{-1}\mathcal{G} \to 0,$$

and taking cohomology shows that

$$\#H^1_{\text{ét}}(C, j_!\mathcal{G}_U) \leq \#\Gamma(C, i_*\mathcal{G}_Z) \cdot \#H^1_{\text{ét}}(C, \mathcal{G}) = \#\Gamma(Z, \mathcal{G}_Z) \cdot \#H^1_{\text{ét}}(C, \mathcal{G})$$

which is the desired result. Note that we have used Lemma 5.6 and Lemma 5.7 to identify inverse images and fiber products. □

We now turn our attention back to Néron models, obtaining a corollary of Lemma 5.8.

Notation 5.10. In addition to the usual notation of Section 3, we assume that $E(K)$ has full ℓ-torsion. Let U be the open subscheme of C consisting of the places where E has good reduction and set $Z = C \setminus U$ (thus, $Z = S$ as a set and is thus finite). Let $i\colon Z \to C$ and $j\colon U \to C$ be the respective inclusions.

Corollary 5.11. *In the notation of 5.10, we have*

$$\#H^1_{\acute{e}t}(C, \mathcal{E}^0[\ell]) \leq \#H^1_{\acute{e}t}(C, j_!\mathcal{E}^0_U[\ell]) \cdot \#H^1_{\acute{e}t}(Z, \mathcal{E}^0_Z[\ell])$$

Proof. Since kernels and pullbacks commute, we may replace $\mathcal{E}^0_U[\ell]$ with $\mathcal{E}^0[\ell] \times_C U$ and $\mathcal{E}^0_Z[\ell]$with $\mathcal{E}^0[\ell] \times_C Z$. The result then follows from Lemma 5.8. □

Consequently, we can work with the two types of 'nice' reduction separately. They are dealt with in the next two sections.

§5.3. Places of split multiplicative reduction

We first bound $H^1_{\text{ét}}(\mathfrak{p}, \mathcal{E}^0_{\mathfrak{p}}[\ell])$ for each $\mathfrak{p} \in S$ and then combine them all into Z.

Lemma 5.12. *With notation as in 5.10, if $\mathfrak{p} \in Z$ then $H^1_{\acute{e}t}(\mathfrak{p}, \mathcal{E}^0_{\mathfrak{p}}[\ell]) \leq \ell$.*

Proof. Recall from Lemma 2.2 that $\mathcal{E}^0_{\mathfrak{p}}[\ell] \simeq \mathbb{G}_{m,\mathfrak{p}}[\ell] \simeq \mu_{\ell,\mathfrak{p}}$. The cohomology long exact sequence coming from the Kummer sequence

$$0 \to \mu_{\ell,\mathfrak{p}} \to \mathbb{G}_{m,\mathfrak{p}} \xrightarrow{(-)^\ell} \mathbb{G}_{m,\mathfrak{p}} \to 0$$

yields the short exact sequence

$$0 \to \frac{H^0_{\text{ét}}(\mathfrak{p}, \mathbb{G}_{m,\mathfrak{p}})}{\ell H^0_{\text{ét}}(\mathfrak{p}, \mathbb{G}_{m,\mathfrak{p}})} \to H^1_{\text{ét}}(\mathfrak{p}, \mu_{\ell,\mathfrak{p}}) \to H^1_{\text{ét}}(\mathfrak{p}, \mathbb{G}_{m,\mathfrak{p}})[\ell] \to 0.$$

Let k denote the residue field of $\mathfrak{p}$. It is a finite extension of $\mathbb{F}_q$, so

$$\#\frac{H^0_{\text{ét}}(\mathfrak{p}, \mathbb{G}_{m,\mathfrak{p}})}{\ell H^0_{\text{ét}}(\mathfrak{p}, \mathbb{G}_{m,\mathfrak{p}})} = \#(k^\times / k^{\times \ell}) \leq \ell,$$

since k has at most ℓ roots of unity.

By Hilbert's Theorem 90, we know $H^1_{\text{ét}}(\mathfrak{p}, \mathbb{G}_{m,\mathfrak{p}}) = H^1(k, k^\times) = 0$. The result follows. □

Lemma 5.13. *In the notation of 5.10, $\#H^1_{\acute{e}t}(Z, \mathcal{E}^0_Z[\ell]) \leq \ell^{\#S}$.*

Proof. Since Z is finite and discrete, the open (and closed) immersion $j\colon (Z \setminus \mathfrak{p}) \to Z$ is finite and étale for any place $\mathfrak{p} \in Z$. Thus, [Sta18, Lemma 03S7] ensures that $j_! \mathcal{F} \simeq j_* \mathcal{F}$ for any étale sheaf $\mathcal{F}$ on $Z \setminus \mathfrak{p}$.

Noting that kernels and pullbacks commute, Lemma 5.8 and Lemma 5.5 show that

$$\#H^1_{\text{ét}}(Z, \mathcal{E}^0_Z[\ell]) \leq \#H^1_{\text{ét}}(Z \setminus \mathfrak{p}, \mathcal{E}^0_{Z\setminus\mathfrak{p}}[\ell]) \cdot \#H^1_{\text{ét}}(\mathfrak{p}, \mathcal{E}^0_{Z\setminus\mathfrak{p}}[\ell]).$$

We repeat this, deleting a point from $Z \setminus \mathfrak{p}$ and so on until we have

$$\#H^1_{\text{ét}}(Z, \mathcal{E}^0_Z[\ell]) \leq \prod_{\mathfrak{p}\in Z} \#H^1_{\text{ét}}(\mathfrak{p}, \mathcal{E}^0_{Z\setminus\mathfrak{p}}[\ell])$$

and we are done by Lemma 5.12. □

§5.4. Places of good reduction

To handle the other term in Corollary 5.11, we first need some bounds on the cohomology of C.

Lemma 5.14. *In the notation of Section 3,*

$$\#H^1_{\acute{e}t}(C, \mu_{\ell,C}) \leq \ell^{2g+1}.$$

Proof. Let $\bar{C}/\bar{\mathbb{F}}_q$ be the base-change of $C/\mathbb{F}_q$ to an algebraic closure of $\mathbb{F}_q$. The low-degree exact sequence coming from the Hochschild-Serre spectral sequence as in [Mil80, Remark III.2.21 (b)] yields

$$0 \to H^1(\mathbb{F}_q, \mu_\ell(\bar{\mathbb{F}}_q)) \to H^1_{\text{ét}}(C, \mu_{\ell,C}) \to H^1_{\text{ét}}(\bar{C}, \mu_{\ell,\bar{C}})^{G_{\mathbb{F}_q}}$$

where $G_{\mathbb{F}_q}$ is the absolute Galois group $\mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$. We know from [Sta18, Lemma 03RQ] that

$$H^1_{\text{ét}}(\bar{C}, \mu_{\ell,\bar{C}}) \simeq \mathrm{Pic}(\bar{C})[\ell] \simeq (\mathbb{Z}/\ell\mathbb{Z})^{2g}$$

By the Kummer sequence and Hilbert 90 we know that $H^1(\mathbb{F}_q, \mu_\ell(\bar{\mathbb{F}}_q)) \simeq \mathbb{F}_q^\times/\mathbb{F}_q^{\times\ell}$, whose order cannot exceed ℓ. Thus,

$$\#H^1_{\text{ét}}(C, \mu_{\ell,C}) \leq \#H^1_{\text{ét}}(\bar{C}, \mu_{\ell,\bar{C}}) \cdot \#H^1(\mathbb{F}_q, \mu_\ell(\bar{\mathbb{F}}_q)) = \ell^{2g} \cdot \ell,$$

as claimed. □

Lemma 5.15. *In the notation of Section 3,*

$$\#H^1_{\acute{e}t}(C, \underline{\mathbb{Z}/\ell\mathbb{Z}}_C) \leq \ell^{2g+1}.$$

Proof. The proof is nearly identical to that of Lemma 5.14. Again, let $\bar{C}/\bar{\mathbb{F}}_q$ be the base-change of $C/\mathbb{F}_q$ to an algebraic closure of $\mathbb{F}_q$ and consider the low-degree exact sequence coming from the Hochschild-Serre spectral sequence. We have

$$0 \to H^1(\mathbb{F}_q, \Gamma(\underline{\mathbb{Z}/\ell\mathbb{Z}}_{\bar{C}}, \bar{C})) \to H^1_{\text{ét}}(C, \underline{\mathbb{Z}/\ell\mathbb{Z}}_C) \to H^1_{\text{ét}}(\bar{C}, \underline{\mathbb{Z}/\ell\mathbb{Z}}_{\bar{C}})^{G_{\mathbb{F}_q}}$$

Now [Sta18, Lemma 03RQ] gives

$$H^1_{\text{ét}}(\bar{C}, \underline{\mathbb{Z}/\ell\mathbb{Z}}_{\bar{C}}) \simeq (\mathbb{Z}/\ell\mathbb{Z})^{2g}$$

so we have

$$\#H^1_{\text{ét}}(C, \underline{\mathbb{Z}/\ell\mathbb{Z}}_C) \leq \#H^1_{\text{ét}}(\bar{C}, \underline{\mathbb{Z}/\ell\mathbb{Z}}_{\bar{C}}) \cdot \#H^1(\mathbb{F}_q, \mathbb{Z}/\ell\mathbb{Z})) \leq \ell^{2g} \cdot \ell.$$

Here, we have used that for the trivial $G_{\mathbb{F}_q}$-module $\mathbb{Z}/\ell\mathbb{Z}$

$$H^1(\mathbb{F}_q, \mathbb{Z}/\ell\mathbb{Z}) \simeq \mathrm{Hom}_{\text{cts}}(G_{\mathbb{F}_q}, \mathbb{Z}/\ell\mathbb{Z})$$

and $G_{\mathbb{F}_q}$ is generated (as a topological group) by the Frobenius morphism $x \mapsto x^q$. Thus, $\mathrm{Hom}_{\text{cts}}(G_{\mathbb{F}_q}, \mathbb{Z}/\ell\mathbb{Z}) = \ell$ and we are done. □

Note that because of good reduction $\mathcal{E}_U = \mathcal{E}_U^0$ by [Sil94, Corollary IV.6.3], so henceforth we drop the 0.

Lemma 5.16. *In the notation of 5.10, we have an exact sequence of group schemes*

$$0 \to \underline{\mathbb{Z}/\ell\mathbb{Z}}_U \to \mathcal{E}_U[\ell] \to \mu_{\ell,U} \to 0.$$

Proof. Let P be an ℓ-torsion point in $E(K)$. Thus, we have a map $\mathbb{Z}/\ell\mathbb{Z} \to E$ given by $n \mapsto nP$. By the Néron mapping property, this extends to a map $f\colon \underline{\mathbb{Z}/\ell\mathbb{Z}}_U \to \mathcal{E}_U$. Let E'/U be its cokernel, which is an elliptic scheme since [Sil09, Proposition III.4.12] ensures that each fiber is an elliptic curve. Let $q\colon \mathcal{E}_U \to \mathcal{G}$ be the cokernel of f.

Now $[\ell] \circ f = 0$ (for example, by looking at the functors of points), so $[\ell]$ factors through q and we obtain $[\ell] = q' \circ q$ for some map $q'\colon \mathcal{E}' \to \mathcal{E}_U$. Thus, q is an isogeny of degree ℓ and q' is its Cartier dual (because q is an epimorphism) and we have an exact sequence

$$0 \to \ker(q) \to \mathcal{E}_U[\ell] \to \ker(q') \to 0.$$

We already know $\ker(q) \simeq \underline{\mathbb{Z}/\ell\mathbb{Z}}_U$: all we need for this is that $\ker(f) = 0$, which is true since if a map hf then it is also zero on the generic fiber. But f is injective on the generic fiber (since P has order ℓ), so h is 0 on the generic fiber. The Néron mapping property then yields $h = 0$. By [Oda69, Corollary 1.3 (ii)], $\ker(q')$ is the Cartier dual of $\ker(q) \simeq \underline{\mathbb{Z}/\ell\mathbb{Z}}$, namely $\mu_{\ell,U}$. This completes the proof. □

Lemma 5.17. *In the notation of 5.10, $\#H^1_{\text{ét}}(C, j_!\mathcal{E}_U[\ell]) \le \ell^{4g+2\#S+2}$.*

Proof. We start with Lemma 5.16

$$0 \to \underline{\mathbb{Z}/\ell\mathbb{Z}}_U \to \mathcal{E}_U[\ell] \to \mu_{\ell,U} \to 0. \tag{5.1}$$

Since $j_!$ is exact, we may apply it to each term and take cohomology to obtain the relation

$$\#H^1_{\text{ét}}(C, j_!\mathcal{E}_U[\ell]) \le \#H^1_{\text{ét}}(C, j_!\underline{\mathbb{Z}/\ell\mathbb{Z}}_U) \cdot \#H^1_{\text{ét}}(C, j_!\mu_{\ell,U})$$

From Lemma 5.9 (identifying inverse images as usual) we bound the $j_!$ terms to obtain

$$\#H^1_{\text{ét}}(C, j_!\mathcal{E}_U[\ell]) \le \#\Gamma(Z, \underline{\mathbb{Z}/\ell\mathbb{Z}}_Z) \cdot \#\Gamma(Z, \mu_{\ell,Z}) \cdot \#H^1_{\text{ét}}(C, \underline{\mathbb{Z}/\ell\mathbb{Z}}_C) \cdot \#H^1_{\text{ét}}(C, \mu_{\ell,C}). \tag{5.2}$$

Since Z is a discrete union of $\#S$ points which are the spectra of finite fields, we see that

$$\#\Gamma(Z, \underline{\mathbb{Z}/\ell\mathbb{Z}}_Z) = \#(\mathbb{Z}/\ell\mathbb{Z})^{\#S} = \ell^{\#S} \quad \text{and} \quad \#\Gamma(Z, \mu_{\ell,Z}) = \prod_{\mathfrak{p}\in S} \#\mu_\ell(\mathfrak{p}) \le \ell^{\#S}.$$

Combining these with Lemma 5.14 and Lemma 5.15 in (5.2) yields the result. □

We can finish of the main theorem for elliptic curves with full ℓ-torsion.

Proof of Lemma 5.3. This is immediate from Corollary 5.11, Lemma 5.13, and Lemma 5.17:

$$\#H^1_{\text{ét}}(C, \mathcal{E}[\ell]) \le H^1_{\text{ét}}(C, j_!\mathcal{E}_U[\ell]) \cdot \#H^1_{\text{ét}}(Z, \mathcal{E}_Z[\ell]) \le \ell^{4g+2\#S+2} \cdot \ell^{\#S} = \ell^{4g+3\#S+2}.$$

□

§5.5. Applying inflation-restriction

To generalize our results from Section 5.1 to all elliptic curves, we will adjoin all of E's ℓ-torsion to K. Lemma 5.18 ensures that we do not lose much by doing so.

Lemma 5.18. *In the notation of Section 3, let K'/K be a finite extension of degree d unramified outside S.*

If g' is the genus of (the smooth projective curve corresponding to) K' and S' is the set of places of bad reduction for E/K', then

$$\textit{(i) } \#S' \leq d\,\#S \quad \textit{and} \quad \textit{(ii) } g' \leq dg + \frac{d(d-1)}{2}\,\#S - d + 1.$$

In particular, if d is fixed, $\#S' = \mathcal{O}(\#S)$ and $g' = \mathcal{O}(g + \#S)$.

Proof. Every bad place $\mathfrak{p}'$ of E/K' lies over a bad place $\mathfrak{p}$ of E/K, for otherwise the minimal discriminant of E/K is not divisible by $\mathfrak{p}$ and so the minimal discriminant of E'/K' cannot be divisible by $\mathfrak{p}'$. Since each $\mathfrak{p} \in S$ lies under at most d places of S', we obtain part (i) of the lemma.

Applying the Riemann-Hurwitz formula, and noting that K'/K is unramified outside S, yields

$$2g' - 2 = d(2g-2) + \sum_{\mathfrak{q} \in S'} (e_{\mathfrak{q}} - 1) \leq 2d\,g + d(d-1)\,\#S - 2d,$$

where the inequality follows from $e_{\mathfrak{q}} \leq d$ and part (i). The result follows. □

We may now finally prove our main theorem.

Proof of Theorem 4.1. Let $K' = K(E[r])$ where r is ℓ, 8, or 9 for $\ell > 3$, $\ell = 2$, or $\ell = 3$ respectively. So we have a Galois extension K'/K, whose Galois group is contained in $\mathrm{GL}_2(\mathbb{Z}/r\mathbb{Z})$ and thus has degree at most r^4. Further, the criterion of Néron-Ogg-Shafarevich [Sil09, Theorem VII.7.1] ensures that K'/K is unramified outside S.

The inflation-restriction exact sequence gives

$$0 \to H^1(\mathrm{Gal}(K'/K), E(K')[\ell]) \to H^1(K, E[\ell]) \to H^1(K', E[\ell]).$$

Noting that

$$\mathrm{Sel}_\ell(E/K) \subseteq H^1(K, E[\ell]) \quad \text{and} \quad \mathrm{Sel}_\ell(E/K') \subseteq H^1(K', E[\ell])$$

as F_ℓ-vector spaces and that the map $\mathrm{Sel}_\ell(E/K) \to \mathrm{Sel}_\ell(E/K')$ is induced by the map on cohomology, we have

$$\dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell(E/K) \leq \dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell(E/K') + \dim_{\mathbb{F}_\ell} H^1(\mathrm{Gal}(K'/K), E[\ell]).$$

Let g' be the genus of K' and S' be the set of places of K' where E/K' has bad reduction. Now, Theorem 5.4 shows that

$$\dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell(E/K') \leq 4g' + 3\#S' + 4$$

Using the bounds from Lemma 5.18 we have

$$\dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell(E/K') \leq 4(r^4 g + r^8 \#S) + 3r^4 \#S + 4 = 4r^4 g + (4r^8 + 3r^4)\#S + 4$$

Finally, $\#H^1(\mathrm{Gal}(K'/K), E[\ell])$ is less than the number of functions $\mathrm{Gal}(K'/K) \to E[\ell]$ since the former counts equivalence classes of cocycles. Since $\#\,\mathrm{Gal}(K'/K) < r^4$ and $\#E[\ell] \leq \ell^2$ this quantity is at most ℓ^{2r^4}.

Putting everything together, we have

$$\dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell(E/K) \leq 4r^4 g + (4r^8 + 3r^4)\#S + 2r^4 + 4,$$

as desired. □

§6. Future work

The following questions haven not been considered in this paper, and are may be interesting avenues for future research.

(i) *A solution for the case $\ell = p$.*
We expect most parts of this approach to remain the same, although much of it will have to re-proved using fppf cohomology instead of étale cohomology (in particular, [Lan21, Lemma 3.26] should still work when E has no additive reduction).

However, we will not be able to use the exact sequence (5.1). Instead, we can factor the map $[p]$ on $\mathcal{E}_U$ into $V \circ F$ where $F\colon \mathcal{E}_U \to \mathcal{E}_U^{(p)}$ is the Frobenius and $V\colon \mathcal{E}_U^{(p)} \to \mathcal{E}_U$ is its Cartier dual (see [KM85] for more on this). Thus we have an exact sequence

$$0 \to \ker F \to \mathcal{E}_U[p] \to \ker V \to 0.$$

Every geometric fiber (at places of ordinary reduction) of $\ker F$ looks like μ_ℓ and dually $\ker V$ looks like $\mathbb{Z}/\ell\mathbb{Z}$. Globally, however, the occurrence of certain twisting phenomena makes this difficult to use.

(ii) *Is Theorem 1.1 asymptotically tight?*
One could ask if there is a family of elliptic curves E whose ℓ-Selmer groups grow as $\operatorname{ht} E/\log(\operatorname{ht} E)$. Similarly, one could ask if there is an elliptic curve whose ℓ-Selmer groups have dimension $\mathcal{O}(\ell^8)$.

(iii) *Can we produce similar results for composite ℓ?*
The ℓ-Selmer group is still a $\mathbb{Z}/\ell Z$ module, so we can bound its rank. Much of the proof may still go through, but some care must be taken for example when $\gcd(6p, \ell) \neq 1$.

(iv) *Can we produce similar results over number fields?*

References

[ABS22] Levent Alpöge, Manjul Bhargava, and Ari Shnidman, *Integers expressible as the sum of two rational cubes*, 2022.

[BH22] Manjul Bhargava and Wei Ho, *On average sizes of selmer groups and ranks in families of elliptic curves having marked points*, 2022.

[BS13a] Manjul Bhargava and Arul Shankar, *The average number of elements in the 4-selmer groups of elliptic curves is 7*, 2013.

[BS13b] ———, *The average size of the 5-selmer group of elliptic curves is 6, and the average rank is less than 1*, 2013.

[BS13c] ———, *Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves*, 2013.

[BS13d] ———, *Ternary cubic forms having bounded invariants, and the existence of a positive proportion of elliptic curves having rank 0*, 2013.

[dJ02] A. J. de Jong, *Counting elliptic surfaces over finite fields*, Moscow Mathematical Journal **2** (2002), 281–311.

[Gro67] Alexander Grothendieck, *éléments de géométrie algébrique : IV. étude locale des schémas et des morphismes de schémas, Quatrième partie*, Publications Mathématiques de l'IHÉS **32** (1967), 5–361 (fr).

[HB94] D.R. Heath-Brown, *The size of selmer groups for the congruent number problem, ii.*, Inventiones mathematicae **118** (1994), no. 2, 331–370.

[HHN14] Q.P. Hô , V.B. Lê Hùng, and B.C. Ngô, *Average size of 2-selmer groups of elliptic curves over function fields*, Mathematical Research Letters **21** (2014), no. 6, 1305–1339.

[Kan13] Daniel Kane, *On the ranks of the 2-selmer groups of twists of a given elliptic curve*, Algebra & Number Theory **7** (2013), no. 5, 1253–1279.

[KM85] Nicholas M. Katz and Barry Mazur, *Arithmetic moduli of elliptic curves. (am-108)*, Princeton University Press, 1985.

[Lan21] Aaron Landesman, *The geometric average size of selmer groups over function fields*, Algebra & Number Theory **15** (2021), no. 3, 673–709.

[Mil80] J. S. Milne, *Etale cohomology (pms-33)*, Princeton University Press, 1980.

[Oda69] Tadao Oda, *The first de rham cohomology group and dieudonné modules*, Annales Scientifiques De L Ecole Normale Superieure **2** (1969), 63–135.

[PR11] Bjorn Poonen and Eric Rains, *Random maximal isotropic subspaces and selmer groups*, Journal of the American Mathematical Society **25** (2011), no. 1, 245–269.

[SD08] Peter Swinnerton-Dyer, *The effect of twisting on the 2-selmer group*, Mathematical Proceedings of the Cambridge Philosophical Society **145** (2008), 513 – 526.

[Sil94] J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate texts in mathematics, Springer-Verlag, 1994.

[Sil09] ———, *The Arithmetic of Elliptic Curves*, Graduate texts in mathematics, Springer, Dordrecht, 2009.

[SSW19] Ananth N. Shankar, Arul Shankar, and Xiaoheng Wang, *Families of elliptic curves ordered by conductor*, 2019.

[Sta18] The Stacks Project Authors, *Stacks Project*, `https://stacks.math.columbia.edu`, 2018.