Elliptic Curves and Their Torsion

SIYAN "DANIEL" LI*

CONTENTS

INTRODUCTION

Elliptic curves are bountiful geometric objects that are simultaneously of great arithmetic interest.

Definition 1.1. An *elliptic curve* is a pair $(E/K, O)$, where E/K is a smooth curve of genus one and O is a point in $E(K)$. The distinguished point O is usually implicit, so we often denote elliptic curves simply with E/K.

Now let K be a number field, and let C/K be a smooth curve of genus g with nonempty $C(K)$. It is a basic result that $C(K)$ is infinite when $g = 0$, while a deep theorem of Faltings proclaims $C(K)$ is finite in the $g \geq 2$ case [Fal83].

When $g = 1$, elliptic curves come into view and expose their rich behavior. Elliptic curves can be equipped with a group structure given by morphisms, making them a first example of abelian varieties. It is here, at this group structure, where arithmetic and geometry interact and produce many beautiful theorems. Consider the following result of Weil generalizing an earlier theorem of Mordell:

Theorem 1.2 (Mordell–Weil [Mor22, Wei29])**.** *Let K be a number field, and let E/K be an elliptic curve. Then $E(K)$ is a finitely-generated abelian group.*

This yields a decomposition $E(K) \cong E(K)_{\text{tors}} \times \mathbb{Z}^r$. Depending on whether r is positive, we see $E(K)$ could be either finite or infinite—an intermediary between the $g = 0$ and $g \geq 2$ cases. We now turn to the torsion factor $E(K)_{\text{tors}}$, which will remain the focus for the rest of this report.

*PRINCETON UNIVERSITY, PRINCETON, NJ 08544. Email address: dsli@princeton.edu

Mathematicians have developed much general theory for analyzing the torsion part of $E(K)$. Here, one can powerfully restrict the possibilities for $E(K)_{\text{tors}}$ in terms of $n = [K : \mathbb{Q}]$, the degree of our number field. More precisely, we can uniformly bound $E(K)_{\text{tors}}$ using n as follows:

Theorem 1.3 (Merel [Mer96])**.** *Let $n \geq 1$ be an integer. There exists a constant $C(n)$ such that, for all number fields K with degree $[K : \mathbb{Q}]$ at most n and all elliptic curves E/K, we get $\#E_{tors}(K) \leq C(n)$.*

This celebrated theorem of Merel is the culmination of a landmark result of Mazur classifying all possibilities for $E_{\text{tors}}(K)$ for $K = \mathbb{Q}$ [Maz77]. Note that this is the $n = 1$ case of Merel's theorem. In addition to Merel's results, the torsion theorem of Mazur also inspired similar classifications of $E_{\text{tors}}(K)$ for all number fields with degree $n \leq 14$ [Kam92, KM95, Abr95].

But how does one actually calculate $E_{\text{tors}}(K)$? That is, given an elliptic curve E/K over a number field, what are some methods of discerning the torsion subgroup of $E(K)$? This is the question we shall tackle in our report.

The contents of this report are based on a reading course of [Sil09], though we aim to take a different perspective on the theory. Throughout this report, we assume familiarity with algebraic geometry and algebraic number theory at the level of a first course. Background equivalent to [Kem93], [Cas67], and [Frö67] is more than enough.

1.1 Acknowledgments

We learned the material contained in this report during an REU program at the University of Michigan. We thank Ian Shipman for advising this project and for the endless help he provided.

ELLIPTIC CURVES AND MAPS BETWEEN THEM

To begin our study, we set up some preliminary facts concerning the category of elliptic curves. Since we intend to do number theory, we lose nothing by letting our base field K be perfect. We shall maintain this assumption throughout this report.

2.1 The Group Operation

In §1, we advertised that elliptic curves can be given a natural group structure. Our first construction of this group operation is very intrinsic and relies on the Picard group. Here, the following lemma is invaluable.

Lemma 2.1. *Let E/K be a smooth curve of genus one, and let P and Q be points in E. Then the divisors (P) and (Q) are linearly equivalent if and only if $P = Q$.*

For this lemma, we shall need a corollary of the Riemann–Roch theorem, and we reproduce it below.

Theorem 2.2 (Riemann–Roch)**.** *Let C/K be a smooth curve of genus g, and let D be a divisor of C satisfying $\deg D > 2g - 2$. Then $\ell(D) = \deg D - g + 1$.*

Proof. See Corollary II.5.5.(c) in [Sil09]. □

Proof of Lemma 2.1. One direction is immediate, so start by writing $\operatorname{div} f = (P) - (Q)$ for some f in $\overline{K}(E)$. Now f lies in $\mathcal{L}((Q))$, and since E is smooth of genus one, the Riemann–Roch theorem yields $\ell((Q)) = 1$. Because $\mathcal{L}((Q))$ includes $\overline{K}$, we see in fact $\mathcal{L}((Q)) = \overline{K}$. So f is a constant, which implies $\operatorname{div} f = 0$ and consequently $P = Q$. □

Note that this already differs from the genus zero case, where smooth curves are isomorphic to $\mathbb{P}^1$ and thus have distinct points with linearly equivalent divisors. Next, recall the definition of $\operatorname{Pic}^0(E)$.

Definition 2.3. Let C/K be a curve. Its divisors of degree zero form a subgroup, which we denote by $\mathrm{Div}^0(C)$. This subgroup contains the principal divisors, and we denote the image of $\mathrm{Div}^0(C)$ under the quotient map $\mathrm{Div}(C) \longrightarrow \mathrm{Pic}(C)$ by $\mathrm{Pic}^0(C)$.

Returning to the task at hand, let $(E/K, O)$ be an elliptic curve. Using Lemma 2.1, we now construct a bijection between E and $\mathrm{Pic}^0(E)$ with the intent of inducing a group structure on E from that of $\mathrm{Pic}^0(E)$.

Proposition 2.4. *Let $[D]$ be an element of $\mathrm{Pic}^0(E)$, where $D \in \mathrm{Div}^0(E)$ is a representative of $[D]$. There exists a unique point P in E satisfying $[D] = [(P) - (O)]$, and the map $\mathrm{Pic}^0(E) \xrightarrow{\sigma} E$ sending $[D]$ to its corresponding point P is a bijection.*

Proof. As E is smooth of genus one, we see $\ell(D + (O)) = 1$ by Riemann–Roch. Therefore we may choose a nonzero f in $\mathcal{L}(D + (O))$. This f satisfies $\operatorname{div} f \geq -D - (O)$, and the right hand side has $\deg(-D - (O)) = -1$. Yet $\deg \operatorname{div} f = 0$, so we must have $\operatorname{div} f = -D - (O) + (P)$ for some point P of E.

This relation shows D and $(P) - (O)$ are linearly equivalent. We want to show this P is independent of our choice for D, but first let's take a step back. Let D' be any divisor in $\mathrm{Div}^0(E)$. Let P' be a point of E satisfying $[D'] = [(P') - (O)]$, at least one of which is guaranteed to exist by the above paragraph. Subtracting this from $[D] = [(P) - (O)]$ yields $[D - D'] = [(P) - (P')]$. Now if $[D] = [D']$, this indicates $[(P)] = [(P')]$ and hence $P = P'$ by Lemma 2.1. Therefore the point P corresponding to $[D]$ is unique, so the map σ is well-defined.

The injectivity of σ also follows from this equation, for $\sigma[D] = P$ and $\sigma[D'] = P'$. When $\sigma[D] = \sigma[D']$, we see $[D - D'] = 0$. Finally, for all points P in E, clearly $\sigma[(P) - (O)] = P$, which makes σ surjective as well. □

Definition 2.5. Let $(E/K, O)$ be an elliptic curve, and let $\mathrm{Pic}^0(E) \xrightarrow{\sigma} E$ be the bijection constructed in Proposition 2.4. The *(algebraic) group operation* of $(E/K, O)$ is the group structure induced on E by σ, that is, the group whose identity element is given by $\sigma(0)$ and whose binary operation and inverse are

$$E \times E \xrightarrow{\sigma^{-1} \times \sigma^{-1}} \mathrm{Pic}^0(E) \times \mathrm{Pic}^0(E) \xrightarrow{\otimes} \mathrm{Pic}^0(E) \xrightarrow{\sigma} E\,, \quad E \xrightarrow{\sigma^{-1}} \mathrm{Pic}^0(E) \xrightarrow{^{-1}} \mathrm{Pic}^0(E) \xrightarrow{\sigma} E$$

where $\otimes$ and $^{-1}$ are the usual addition and negation in $\mathrm{Pic}^0(E)$, respectively. We denote the group operations by $E \times E \xrightarrow{\boxplus} E$ and $E \xrightarrow{\boxminus} E$.

Remark 2.6. We shall give a geometric definition for the group operation in the next subsection.

The group axioms for E follow from those for $\mathrm{Pic}^0(E)$. In particular, we see E is abelian and notice that $\sigma(0) = \sigma[(O) - (O)] = O$. Thus for any elliptic curve the identity is precisely the distinguished point: specifying this point is akin to specifying the identity of a group. This choice does not affect the elliptic curve structure much, however—see Example 2.27.

2.2 Weierstrass Equations

Observe that Definition 1.1 captures the essential abstract qualities of elliptic curves—the fact that E/K is smooth of genus one is crucial in our applications of the Riemann–Roch theorem, and the distinguished point O plays a central role in the group operation as the designed identity element. Similarly, Definition 2.5's characterization of the group structure helps verify various algebraic properties.

However, these definitions offer little, if any geometric intuition about elliptic curves and their group structures. The abstract nature of these definitions also render explicit calculations difficult. In this section, we intend to remedy both these issues. The titular Weierstrass equations make elliptic curves more concrete.

Definition 2.7. A *Weierstrass equation* is the curve E/K in $\mathbb{P}^2$ given by the projective closure of

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

where the coefficients a_i lie in K. Using the coordinates $x = X/Z$ and $y = Y/Z$, one can easily check the only point at infinity on E is $O = [0, 1, 0]$.

Note the similarities in notation between the above definition and Definition 1.1. We shall connect them more explicitly soon, but we first offer a few simplifying changes of variables and important quantities associated with any Weierstrass equation.

Proposition 2.8. *Let $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ be a Weierstrass equation over K. If $\operatorname{char} K \neq 2$, the quantities*

$$b_2 = a_1^2 + 4a_2, \qquad b_4 = 2a_4 + a_1a_3, \qquad b_6 = a_3^2 + 4a_6$$

and change of variables $y \mapsto \frac{1}{2}(y - a_1x - a_3)$ yield the Weierstrass equation $y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6$.

Proof. This is a simple polynomial calculation. □

Proposition 2.9. *Suppose $\operatorname{char} K \neq 2, 3$, and let $E : y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6$ be the Weierstrass equation obtained in Proposition 2.8 after a change of variables. Setting*

$$c_4 = b_2^2 - 24b_4, \qquad c_6 = -b_2^3 + 35b_2b_4 - 216b_6, \qquad \text{and substituting} \quad (x, y) \mapsto \left(\frac{x - 3b_2}{36}, \frac{y}{108}\right)$$

gives the Weierstrass equation $y^2 = x^3 - 27c_4x - 54c_6$.

Proof. This too is a straightforward exercise in polynomial manipulation. □

Remark 2.10. Proposition 2.9 shows that, when K is a number field or some associated completion, we need only consider Weierstrass equations in the form $y^2 = x^3 + Ax + B$. But, in the spirit of number theory we are also naturally led to consider objects over finite fields, so the most general form of Definition 2.7 remains relevant. As one might expect, proofs using the simplified Weierstrass equations of Propositions of 2.8 and 2.9 are much simpler than the general case—and we stress that Weierstrass equations over arbitrary characteristic are important.

At this point, notice the quantities defined in Propositions 2.8 and 2.9 are well-defined for any Weierstrass equation E/K regardless of $\operatorname{char} K$.

Definition 2.11. Define three more values

$$b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2 \quad \Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 \quad \text{and } j = \frac{c_4^3}{\Delta} \text{ if } \Delta \neq 0$$

The quantity Δ is the *discriminant* of E, and the quantity j is the *j-invariant* of E.

Remark 2.12. Recall the Weierstrass equation $y^2 = f(x)$ provided by Proposition 2.8. Letting Δ_2 be the discriminant of $f(x)$, a straightforward calculation reveals $\Delta_2 = 16\Delta$.

We shall further justify our nomenclature for Δ and j with the following proposition.

Proposition 2.13. *(a) A Weierstrass equation is smooth if and only if $\Delta \neq 0$.*

(b) Let E/K and E'/K be two smooth Weierstrass equations. Then E and E' are isomorphic over $\overline{K}$ if and only they share the same j-invariant.

(c) For any j_0 in $\overline{K}$, there exists a Weierstrass equation $E/K(j_0)$ with j-invariant equal to j_0.

Proof. See Proposition III.1.4 in [Sil09]. This proposition results from myriad casework and polynomial calculations. The $\operatorname{char} K \neq 2, 3$ cases are much easier than that of general characteristic; here the principle outlined in Remark 2.10 already comes into play. □

Remark 2.14. For non-smooth Weierstrass equations, one can obtain finer information about their singularities. This data is dictated by the value of c_4—see Propositions III.1.4.(a) and III.2.5 in [Sil09].

Thus the j-invariant offers a complete parameterization of the geometry of Weierstrass equations, that is, their isomorphism classes over the algebraic closure $\overline{K}$. However, two Weierstrass equations with the same j-invariant $j_0 \in \overline{K}$ are not necessarily isomorphic over $K(j_0)$!

Example 2.15. Consider the Weierstrass equations given in Examples 4.3 and 4.4. Both easily have j-invariant $j = 0$, yet they have differing torsion subgroups $E_{\text{tors}}(\mathbb{Q})$ and hence nonisomorphic subgroups of rational points $E(\mathbb{Q})$. Thus they are not isomorphic over $\mathbb{Q}(0) = \mathbb{Q}$.

Earlier, we asserted that Weierstrass equations provide a more concrete approach to elliptic curves. We now make good on our promise and explicitly relate the two.

Theorem 2.16. *Let $(E/K, O)$ be an elliptic curve.*

(a) There exist x and y in $K(E)$ such that the map $E \xrightarrow{\phi} \mathbb{P}^2$ defined by $\phi = [x, y, 1]$ is an isomorphism from E to a Weierstrass equation with coefficients in K and ϕ maps O to $[0, 1, 0]$.

(b) Let E_1/K and E_2/K be two Weierstrass equations for E satisfying the properties enumerated in (a). Then E_1 and E_2 are isomorphic by a change of variables in the form

$$X_2 = u^2 X_1 + r \qquad Y_2 = u^3 Y_1 + s u^2 X_1 + t \qquad \text{for some } u \text{ in } K^\times \text{ and } r, s, t \text{ in } K.$$

(c) Conversely, by choosing a distinguished point O, every smooth Weierstrass equation E/K is an elliptic curve $(E/K, O)$.

Proof. See Proposition III.3.1 in [Sil09]. Notice the smoothness and genus of E are crucial for applying the Riemann–Roch theorem and subsequently obtaining a Weierstrass equation relation. □

Definition 2.17. Let $(E/K, O)$ be an elliptic curve. Any pair of functions x and y in $K(E)$ satisfying the properties listed in Theorem 2.16.(a) are called *Weierstrass coordinate functions*.

In light of Theorem 2.16, every elliptic curve admits Weierstrass coordinate functions. Therefore we may view elliptic curves and smooth Weierstrass equations as the same objects—with the distinguished point $O = [0, 1, 0]$ at infinity being understood—and we shall readily make this identification throughout this report.

Part (b) of Theorem 2.16 answers the important question of how flexible one can be when choosing Weierstrass coordinates for an elliptic curve. For a fixed elliptic curve, we naturally wonder how our menagerie of associated quantities changes as we vary these Weierstrass coordinates.

Proposition 2.18. *Let E/K be an elliptic curve, and consider the change of variables*

$$x = u^2 x' + r \qquad y = u^3 y' + s u^2 x' + t \qquad \text{for some } u \text{ in } K^\times \text{ and } r, s, t \text{ in } K.$$

The associated quantities for these primed coordinates are

$$\begin{aligned}
a_1' &= u^{-1}(a_1 + 2s) & c_4' &= u^{-4}c_4 \\
a_2' &= u^{-2}(a_2 - sa_1 + 3r - s^2) & c_6' &= u^{-6}c_6 \\
a_3' &= u^{-3}(a_3 + ra_1 + 2t) & \Delta' &= u^{-12}\Delta \\
a_4' &= u^{-4}(a_4 - sa_3 + 2ra_2 - (t + rs)a_1 + 3r^2 - 2st) & j' &= j \\
a_6' &= u^{-6}(a_6 + ra_4 + r^2a_2 + r^3 - ta_3 - t^2 - rta_1) \\
b_2' &= u^{-2}(b_2 + 12r) \\
b_4' &= u^{-4}(b_4 + rb_2 + 6r^2) \\
b_6' &= u^{-6}(b_6 + 2rb_4 + r^2b_2 + 4r^3) \\
b_8' &= u^{-8}(b_8 + 3rb_6 + 3r^2b_4 + r^3b_2 + 3r^4)
\end{aligned}$$

Proof. This follows by a routine polynomial calculation. □

Note the j-invariant remains unchanged, as expected. Proposition 2.21 is invaluable whenever one tries to extract intrinsic information about elliptic curves from their corresponding Weierstrass equations, which we shall do in §3.

Now that we have Weierstrass equations under our belt, let us use them to present an equivalent, geometric definition of the group operation. This alternative construction is heavily dependent on secant lines.

Definition 2.19. Let C/K be a smooth curve, and let P and Q be points on C. The *secant line on C defined by P and Q* is the smooth curve L in $\mathbb{P}^2$ given as follows. If $P \neq Q$, let L be the unique line going through P and Q—otherwise, let L be the line tangent to C at $P = Q$.

Theorem 2.16 shows elliptic curves are plane curves, which allows us to use Bezout's theorem.

Definition 2.20. Let E/K be an elliptic curve. Let P and Q be points on E, and let L be the secant line on E defined by P and Q. Since Weierstrass equations are given by cubics, Bezout's theorem shows $E \cap L = \{P, Q, R\}$ as a multiset. Next, let L' be the secant line on E defined by O and R. Applying Bezout again indicates $E \cap L' = \{O, R, S\}$ as a multiset. Finally, let L'' be the secant line on E defined by O and P. As usual $E \cap L'' = \{O, P, T\}$ by Bezout's theorem.

The *(geometric) group operation* is given by the binary operation $E \times E \xrightarrow{\oplus} E$ mapping $(P, Q) \mapsto S$ and the inverse map $E \xrightarrow{\ominus} E$ that sends $P \mapsto T$.

For an illustration, see Figure 1. First, we verify this yields the same group structure given in Definition 2.5.

Proposition 2.21. *Let E/K be an elliptic curve. The algebraic group operation $E \times E \xrightarrow{\boxplus} E$ and geometric group operation $E \times E \xrightarrow{\oplus} E$ are the same map, as are $E \xrightarrow{\boxminus} E$ and $E \xrightarrow{\ominus} E$.*

Proof. In the situation of Definition 2.20, let $f(X, Y, Z)$ and $f'(X, Y, Z)$ be the homogeneous linear equations defining L and L', respectively. Then f/Z and f'/Z lie in $\overline{K}(E)$. From the definitions of L and L', we see $\{P, Q, R\}$ are precisely the zeros of f on E and $\{O, R, S\}$ are precisely the zeroes of f' on E. The function Z defines the line at infinity, which only intersects E at O and thus does so with multiplicity 3 by Bezout. This information lets us calculate

$$\begin{aligned}
&\operatorname{div}(f/Z) = (P) + (Q) + (R) - 3(O), \quad \operatorname{div}(f'/Z) = (R) + (S) - 2(O) \\
\implies &\operatorname{div}(f'/f) = (S) - (P) - (Q) + (O) \implies 0 = [(S) - (O)] - [(P) - (O)] - [(Q) - (O)] \\
&\qquad = \sigma^{-1}(P \oplus Q) - \sigma^{-1}(P) - \sigma^{-1}(Q) \implies P \oplus Q = \sigma(\sigma^{-1}(P) + \sigma^{-1}(Q)) = P \boxplus Q
\end{aligned}$$

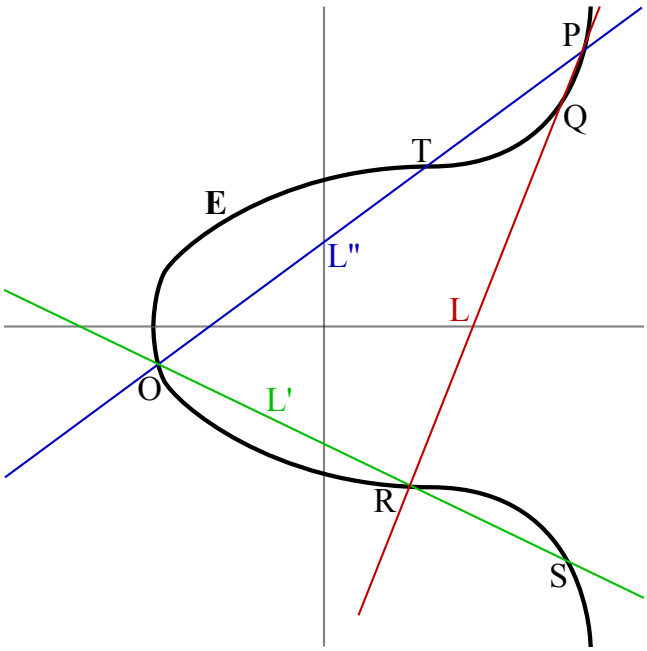

Figure 1: The geometric group operation on an elliptic curve E/K. Here $S = P \oplus Q$ and $T = \ominus P$.

as desired. Letting $f''(X, Y, Z)$ be the homogeneous linear equation defining L'' indicates its zeroes on E are exactly $\{O, P, T\}$, and the similar calculation

$$\begin{aligned} &\operatorname{div}(f''/Z) = (P) + (T) - 2(O) \implies 0 = [(P) - (O)] + [(T) - (O)] \\ \implies &\sigma^{-1}(\ominus P) = [(T) - (O)] = -[(P) - (O)] = -\sigma^{-1}(P) \implies \ominus P = \sigma(-\sigma^{-1}(P)) = \boxminus P \end{aligned}$$

shows the inverse maps are also the same. □

Proposition 2.21 enables us to interchangeably use the algebraic and geometric definitions for the group operation, which we will simply denote by $E \times E \xrightarrow{+} E$ and $E \xrightarrow{-} E$. The geometric description of addition in E allows explicit calculations with polynomial equations—see Group Law Algorithm III.2.3 in [Sil09]. As a corollary, we see elliptic curves are abelian varieties.

Corollary 2.22. Let E/K be an elliptic curve. Then the addition and negation maps $E \times E \xrightarrow{+} E$ and $E \xrightarrow{-} E$ are morphisms defined over K.

Proof. See Theorem II.3.6 in [Sil09]. While Silverman uses translation maps to offer a cleaner proof, this is merely another application of these explicit group operation formulas; see Remark II.3.6.1 in [Sil09]. □

This in turn shows the rational points of an elliptic curve form a subgroup.

Corollary 2.23. Let E/K be an elliptic curve. Then $E(K)$ is a subgroup of E.

Proof. The identity O is in $E(K)$, and $E(K)$ is closed under addition since $E \times E \xrightarrow{+} E$ is a morphism defined over K. □

2.3 Maps Between Elliptic Curves

We have seen that elliptic curves are abelian varieties, that is, projective varieties and abelian groups in a compatible way. As is standard category-theoretical practice, next we turn to morphisms of elliptic curves. To reflect that elliptic curves are both varieties and abelian groups, their hom-sets should be the intersection of variety and abelian group hom-sets. We also expect morphisms of elliptic curves to have abelian group and ring structures similar to those of abelian group homomorphisms.

To obtain all this structure, it is enough to require that morphisms preserve the identity.

Definition 2.24. Let $(E_1/K, O_1)$ and $(E_2/K, O_2)$ be elliptic curves. An *isogeny* from E_1 to E_2 is a morphism $E_1 \xrightarrow{\phi} E_2$ that sends $\phi(O_1) = O_2$. If ϕ is constant, it must be valued on O_2. We call this the *zero isogeny* and denote it by $\phi = [0]$.

If ϕ is not the zero isogeny, it is a non-constant morphism of smooth curves, which makes it finite and surjective. Therefore we may consider the degree $\deg \phi$. For the zero isogeny, we set $\deg[0] = 0$.

Before we get too carried away, let us verify that isogenies automatically preserve addition.

Proposition 2.25. *Let $E_1 \xrightarrow{\phi} E_2$ be an isogeny. Then ϕ is a group homomorphism.*

Proof. Of course $[0]$ is the trivial homomorphism, so suppose ϕ is non-constant. Here ϕ induces a homomorphism $\mathrm{Pic}^0(E_1) \xrightarrow{\phi_*} \mathrm{Pic}^0(E_2)$, and since ϕ sends O_1 to O_2 it forms the commutative diagram below.

$$\begin{array}{ccc} \mathrm{Pic}^0(E_1) & \xrightarrow{\sigma_1} & E_1 \\ \downarrow{\scriptstyle \phi_*} & & \downarrow{\scriptstyle \phi} \\ \mathrm{Pic}^0(E_2) & \xrightarrow{\sigma_2} & E_2 \end{array}$$

But the group structure on E_i is induced from that of $\mathrm{Pic}^0(E_i)$ via σ_i. Therefore ϕ is also a group homomorphism. □

Thus we see isogenies are precisely the morphisms of elliptic curves we want.

Example 2.26. Let E/K be a smooth curve of genus one, and let O and O' be two points in $E(K)$. We can define a morphism of varieties $E/K \xrightarrow{\tau_{O'}} E/K$ by sending $P \mapsto P + O'$, where $+$ is taken in the elliptic curve $(E/K, O)$. Corollary 2.22 indicates this is an isogeny $(E/K, O) \xrightarrow{\tau_{O'}} (E/K, O')$. Letting $-$ be negation in the elliptic curve $(E/K, O)$, note that $\tau_{-O'}$ provides an inverse for $\tau_{O'}$. Therefore the elliptic curves $(E/K, O)$ and $(E/K, O')$ are canonically isomorphic over K, so the choice of distinguished point does not truly affect our elliptic curve.

Example 2.27. Let $E/\mathbb{F}_q$ be an elliptic curve, and let $E \xrightarrow{\phi_q} E$ be the *Frobenius endomorphism* defined by sending $(x, y) \mapsto (x^q, y^q)$. The Frobenius endomorphism is well-defined since taking q-th powers fixes $\mathbb{F}_q$ and therefore preserves the equation defining E. In fact, Galois theory tells us $E(\mathbb{F}_q)$ is precisely the set fixed by ϕ_q. Since ϕ_q fixes O, it is an isogeny.

Definition 2.28. Let E_1/K and E_2/K be elliptic curves. We write $\mathrm{Hom}(E_1, E_2)$ for the set of isogenies $E_1 \xrightarrow{\phi} E_2$. From here, we form the special hom-sets $\mathrm{End}(E_1)$ and $\mathrm{Aut}(E_1)$ as usual.

Corollary 2.22 indicates $\mathrm{Hom}(E_1, E_2)$ is closed under pointwise addition, making it an abelian group. Using composition of isogenies as multiplication turns $\mathrm{End}(E_1)$ into a ring. Elliptic curve hom-sets lack torsion, a fact that shall play a key role in the classification of elliptic curve endomorphism rings.

Theorem 2.29. *Let E_1/K and E_2/K be elliptic curves.*

(a) The abelian group $\mathrm{Hom}(E_1, E_2)$ is torsion-free.

(b) The ring $\mathrm{End}(E_1)$ has no zerodivisors. In particular, it has characteristic 0.

Proof. See Proposition III.4.2 in [Sil09]. Note that, after applying explicit group law calculations, the multiplicativity of $\deg$ plays a crucial role in reducing to the fact that $\mathbb{Z}$ is an integral domain. □

Let E/K be an elliptic curve. Extending our nomenclature for the zero isogeny, for any integer m we denote the image of m under the unique ring homomorphism $\mathbb{Z} \longrightarrow \mathrm{End}(E)$ by $[m]$. Theorem 2.29 shows this homomorphism is injective, so for nonzero m the morphism $[m]$ is a finite map. This makes the m-torsion subgroup of E finite, since $E[m] = \ker[m] = [m]^{-1}(O)$. Here we make our first step towards analyzing the torsion subgroup of elliptic curves.

2.4 Dual Isogenies

Let $E_1 \xrightarrow{\phi} E_2$ be a nonzero isogeny. While proving Proposition 2.25, we noticed that, under the identification $\mathrm{Pic}^0(E_i) \xrightarrow{\sigma_i} E_i$, our isogeny ϕ corresponds to the homomorphism $\mathrm{Pic}^0(E_1) \xrightarrow{\phi_*} \mathrm{Pic}^0(E_2)$. But ϕ induces a homomorphism on Picard groups in the other direction as well, namely $\mathrm{Pic}^0(E_2) \xrightarrow{\phi^*} \mathrm{Pic}^0(E_1)$. It turns out this ϕ^* also corresponds to an important isogeny.

Proposition 2.30. *Let $E_1 \xrightarrow{\phi} E_2$ be a nonzero isogeny. Then the map $E_2 \xrightarrow{\widehat{\phi}} E_1$ defined by*

$$E_2 \xrightarrow{\sigma_2^{-1}} \mathrm{Pic}^0(E_2) \xrightarrow{\phi^*} \mathrm{Pic}^0(E_1) \xrightarrow{\sigma_1} E_1$$

is an isogeny. Setting $\widehat{\phi} = [0]$ when ϕ is the zero isogeny, in any case $\widehat{\phi}$ is the unique isogeny that satisfies $\widehat{\phi} \circ \phi = [\deg \phi]$.

Proof. See Theorem III.6.1 in [Sil09]. □

Definition 2.31. Let $E_1 \xrightarrow{\phi} E_2$ be an isogeny. The *dual isogeny to ϕ* is the isogeny $E_2 \xrightarrow{\widehat{\phi}} E_1$ constructed in Proposition 2.30.

The dual isogeny satisfies many nice algebraic properties, from which one can deduce much information about elliptic curves. We begin by providing some of these properties—we promise to give applications immediately afterwards.

Proposition 2.32. *Let $E_1 \xrightarrow{\phi} E_2$, $E_1 \xrightarrow{\psi} E_2$, and $E_2 \xrightarrow{\lambda} E_3$ be isogenies.*

(a) We get $\deg \widehat{\phi} = \deg \phi$ and $\widehat{\widehat{\phi}} = \phi$.

(b) For all integers m, we obtain $\widehat{[m]} = [m]$ and $\deg[m] = m^2$.

(c) We have $\widehat{\lambda \circ \phi} = \widehat{\phi} \circ \widehat{\lambda}$ and $\widehat{\phi + \psi} = \widehat{\phi} + \widehat{\psi}$.

Proof. See Theorem III.6.2 in [Sil09]. Note that proving $\widehat{\lambda \circ \phi} = \widehat{\phi} \circ \widehat{\lambda}$ presents the most difficulty. □

Let E/K be an elliptic curve. With these properties in hand, we provide a characterization of the possibilities for $\mathrm{End}(E)$. This relies on the following abstract lemma.

Lemma 2.33. *Let R be a ring. If R satisfies the following properties*

(a) R has characteristic zero and has no zerodivisors.

(b) R is a free $\mathbb{Z}$-module of rank at most four.

(c) R has an anti-involution $R \xrightarrow{\widehat{\cdot}} R$ that fixes $\mathbb{Z}$.

(d) For all a in R, the product $a\widehat{a}$ is a non-negative integer for which $a\widehat{a} = 0$ if and only if $a = 0$.

then R is isomorphic to one of the following rings:

(i) The integers $\mathbb{Z}$.

(ii) An order in an imaginary quadratic number field.

(iii) An order in a quaternion algebra over $\mathbb{Q}$.

Proof. See Theorem III.9.3 in [Sil09]. □

To apply Lemma 2.33, we need only borrow fact (b) from elsewhere.

Lemma 2.34. *Let E/K be an elliptic curve. Then $\mathrm{End}(E)$ is a free $\mathbb{Z}$-module of rank at most four.*

Proof. See Corollary III.7.5 in [Sil09]. The *Tate module* is central to the proof and in fact to much of the theory of elliptic curves, but we shall not cover it here. For reference, see III.7 in [Sil09]. □

Corollary 2.35. Let E/K be an elliptic curve. Then $\mathrm{End}(E)$ is either $\mathbb{Z}$, an order in an imaginary quadratic number field, or an order in a quaternion algebra over $\mathbb{Q}$.

Proof. Refer to the hypotheses of Lemma 2.33. Theorem 2.29 shows $\mathrm{End}(E)$ satisfies (a), Lemma 2.34 indicates $\mathrm{End}(E)$ satisfies (b), Proposition 2.32 shows the dual isogeny provides the anti-involution needed for (c), and Proposition 2.32 shows $a\widehat{a} = \deg a$ here, which clearly satisfies (d). The corollary follows from Lemma 2.33. □

Next we shall prove the *Hasse bound*, which restricts the number of rational points on elliptic curves over finite fields. This will be useful later when we reduce questions about elliptic curves over local fields to ones about elliptic curves over finite fields.

Using the connections between duals and degree established in Proposition 2.32, we start by showing the $\deg$ function provides a positive-definite quadratic form on hom-sets.

Corollary 2.36. Let E_1/K and E_2/K be elliptic curves. Then $\mathrm{Hom}(E_1, E_2) \xrightarrow{\deg} \mathbb{Z}$ is a positive-definite quadratic form.

Proof. Once we show the degree map is indeed a quadratic form, it follows immediately from the definition of $\deg$ and our convention $\deg[0] = 0$ that $\deg$ is positive-definite. For any isogeny $E_1 \xrightarrow{\phi} E_2$, we easily have $\deg(-\phi) = \deg[-1] \circ \phi = \deg[-1] \deg \phi = \deg \phi$. Finally, let $E_1 \xrightarrow{\psi} E_2$ be another isogeny. we use the embedding $\mathbb{Z} \longrightarrow \mathrm{End}(E_1)$ given by Theorem 2.29 and the properties in Proposition 2.32 to see

$$[\deg(\phi + \psi) - \deg \phi - \deg \psi] = (\phi + \psi) \circ \widehat{(\phi + \psi)} - \phi \circ \widehat{\phi} - \psi \circ \widehat{\psi} = \phi \circ \widehat{\psi} + \psi \circ \widehat{\phi}.$$

Now this is $\mathbb{Z}$-bilinear in ϕ and ψ, so $\deg$ is indeed a quadratic form. □

We intend to apply this positive-definite quadratic form using the following general inequality.

Lemma 2.37. *Let A be an abelian group, and let $A \xrightarrow{d} \mathbb{Z}$ be a positive-definite quadratic form. Then for all a and b in A, we have $\left|d(a-b) - d(a) - d(b)\right| \leq 2\sqrt{d(a)d(b)}$.*

Proof. See Lemma V.1.2 in [Sil09]. □

Before we can proceed with the Hasse bound, we need a lemma regarding the separability of the Frobenius endomorphism.

Lemma 2.38. *Let $E/\mathbb{F}_q$ be an elliptic curve, and let $E \xrightarrow{\phi_q} E$ be the Frobenius endomorphism. Then the morphism $[1] - \phi_q$ is separable.*

Proof. See Corollary III.5.5 in [Sil09]. This depends on the *invariant differential*, which reduces questions about elliptic curve addition to vector space addition—for more on the invariant differential, see III.5 in [Sil09]. □

Theorem 2.39 (Hasse)**.** *Let $E/\mathbb{F}_q$ be an elliptic curve. Then $\left|\#E(\mathbb{F}_q) - q - 1\right| \leq 2\sqrt{q}$.*

Proof. Let $E \xrightarrow{\phi_q} E$ be the Frobenius endomorphism. We remarked in Example 2.27 that $E(\mathbb{F}_q)$ consists precisely of the fixed points of ϕ_q, which in turn are simply the elements of $\ker([1] - \phi_q)$. This kernel is the fiber $([1] - \phi_q)^{-1}(O)$. Now E is infinite, and almost all fibers have cardinality $\deg_s([1] - \phi_q)$. Since $[1] - \phi_q$ is a homomorphism, all fibers in fact have the same cardinality. Thus $\#E(\mathbb{F}_q) = \#\ker([1] - \phi_q) = \deg_s([1] - \phi_q)$, and Lemma 2.38 indicates this is $\deg([1] - \phi_q)$. As we know $\deg[1] = 1$ and $\deg \phi_q = q$, applying Lemma 2.37 with $a = [1]$ and $b = \phi_q$ finishes the proof. □

Let m be a positive integer. We can also use Proposition 2.32 to gleam much information about the specific m-torsion of elliptic curves. First, we give a lemma concerning the separability of $[m]$.

Lemma 2.40. *Let E/K be an elliptic curve. If $\operatorname{char} K \nmid m$, then $[m]$ is separable.*

Proof. See Corollary III.5.4 in [Sil09]. As in Lemma 2.37, this relies on the invariant differential. □

Proposition 2.41. *Let E/K be an elliptic curve, and let m be a positive integer. If $\operatorname{char} K \nmid m$, then $E[m]$ is isomorphic to $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ as abstract groups.*

Proof. Lemma 2.40 indicates $\deg_s[m] = \deg[m]$, and as in the proof of Hasse's bound we obtain $\#\ker[m] = \deg_s[m]$. Now Proposition 2.32 provides $\deg[m] = m^2$, and $\ker[m]$ is precisely $E[m]$. Therefore $\#E[m] = m^2$. We know $E[m]$ is a finite abelian group, and by induction the structure theorem for finite abelian groups shows $E[m]$ must be isomorphic to $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$. □

Remark 2.42. When $\operatorname{char} K$ is positive and divides m, the nature of $E[m]$ depends on whether the dual of the p-th power Frobenius endomorphism is separable. In fact, this property has a variety of equivalent characterizations—see V.3 in [Sil09].

Since $E(K)[m]$ is a subgroup of $E[m]$, Proposition 2.41 significantly bounds the torsion of $E(K)$.

LOCAL THEORY

Let K be a number field, and let E/K be an elliptic curve. Our goal is to analyze $E_{\text{tors}}(K)$, and, motivated by the fruitful algebraic number theoretic interaction between global and local fields, we now turn to analyzing elliptic curves over the latter.

Throughout this section, let v be a normalized non-Archimedean valuation of K, let $|\cdot|_v$ be the corresponding absolute value, let K_v be the associated completion, let $\mathcal{O}_v$ be the ring of integers of K_v, let π be a uniformizer of $\mathcal{O}_v$, let $\mathfrak{m}_v = \pi\mathcal{O}_v$ be the maximal ideal of $\mathcal{O}_v$, and let $k_v = \mathcal{O}_v/\mathfrak{m}_v$ be the residue field.

3.1 Reduction Modulo $\mathfrak{m}_v$

Let E/K_v be an elliptic curve. We would like to reduce this to an elliptic curve $\widetilde{E}/k_v$ via the usual quotient map $\mathcal{O}_v \longrightarrow k_v$, yet E/K_v has points with coordinates in K_v, not necessarily $\mathcal{O}_v$. We describe how to reduce these points modulo $\mathfrak{m}_v$ below.

Definition 3.1. Let P be in $\mathbb{P}^n(K_v)$, and let $P = [x_0, \dots, x_n]$ be homogeneous coordinates for P lying in K_v. We may scale $[x_0, \dots, x_n]$ by powers of π such that every x_i lies in $\mathcal{O}_v$ and at least one x_i lies in $\mathcal{O}_v^\times$—namely, multiply $[x_0, \dots, x_n]$ by the $-\min\{x_0, \dots, x_n\}$-th power of π. Then $[\widetilde{x}_0, \dots, \widetilde{x}_n]$ lies in $\mathbb{P}^n(k_v)$, where $\widetilde{x}_i$ is the reduction of x_i modulo $\mathfrak{m}_v$.

The *reduction modulo* $\mathfrak{m}_v$ *map* $\mathbb{P}^n(K_v) \xrightarrow{q} \mathbb{P}^n(k_v)$ is given by sending P to $[\widetilde{x}_0, \dots, \widetilde{x}_n]$. To see this is well-defined, let $[x_0', \dots, x_n']$ be another such representative of P, and let $[\widetilde{x}_0', \dots, \widetilde{x}_n']$ be the corresponding reduced point. Since there exists some λ in K_v satisfying $x_i' = \lambda x_i$ for all i, we see $\widetilde{x}_i' = \widetilde{\mu}\widetilde{x}_i$, where $\widetilde{\mu}$ is the reduction of $\lambda\pi^{-\operatorname{ord}_v \lambda} \in \mathcal{O}_v^\times$ modulo $\mathfrak{m}_v$.

Let $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ be a Weierstrass equation for E/K_v. The image of $E(K_v)$ under the reduction modulo $\mathfrak{m}_v$ map $\mathbb{P}^2(K_v) \xrightarrow{q} \mathbb{P}^2(k_v)$ obviously satisfies the reduced equation $y^2 + \widetilde{a}_1xy + \widetilde{a}_3y = x^3 + \widetilde{a}_2x^2 + \widetilde{a}_4x + \widetilde{a}_6$. If the Weierstrass equation defined by this equation is smooth, it indeed provides an elliptic curve E'/k_v. However, there could be many Weierstrass equations for E/K_v, so one must discern which ones reflect the essential properties of E/K_v after reducing modulo $\mathfrak{m}_v$.

Definition 3.2. Let E/K_v be an elliptic curve, and let $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ be a Weierstrass equation for E. If all the a_i lie in $\mathcal{O}_v$ and $v(\Delta)$ is minimal while upholding this condition, we say this is a *minimal equation for* E.

We begin by checking this definition is not vacuous.

Proposition 3.3. *Let E/K_v be an elliptic curve. Then E has a minimal equation.*

Proof. Let $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ be a Weierstrass equation for E/K_v. Proposition 2.21 indicates the substitution $(x, y) \mapsto (u^{-2}x, u^{-3}y)$ yields another Weierstrass equation for E/K_v with a_i replaced by u^ia_i, so taking $u = \pi^N$ for sufficiently high N yields a Weierstrass equation with coefficients in $\mathcal{O}_v$. Now note that since Δ is a polynomial in the a_i, so Δ is in $\mathcal{O}_v$ if the a_i are. Thus $v(\Delta)$ is non-negative, and we may apply well-ordering to show minimal equations exist. □

Minimal equations are precisely the Weierstrass equations that preserve nice properties when reduced modulo $\mathfrak{m}_v$. Before elaborating, we clarify which of the changes of variables outlined in Proposition 2.16 preserve minimality.

Proposition 3.4. *Let E/K_v be an elliptic curve.*

(a) A minimal equation is unique up to change of coordinates in the form

$$x = u^2x' + r \qquad y = u^3y' + su^2x' + t \qquad \text{for some } u \text{ in } \mathcal{O}_v^\times \text{ and } r, s, t \text{ in } \mathcal{O}_v.$$

(b) As a converse, any substitution used to obtain a minimal equation from a Weierstrass equation with coefficients in R is in above form, except the restriction on u is relaxed to $u \in \mathcal{O}_v$.

Proof. This is a routine calculation using Proposition 2.21 and basic properties of valuations—see Proposition VII.1.3 in [Sil09]. □

Returning to our original plan, we use minimal equations to define elliptic curves reduced modulo $\mathfrak{m}_v$.

Definition 3.5. Let E/K_v be an elliptic curve. We denote the Weierstrass equation obtained from reducing a minimal equation for E modulo $\mathfrak{m}_v$ by $\widetilde{E}/k_v$.

Remark 3.6. This $\widetilde{E}/k_v$ is not necessarily smooth, so it may not define an elliptic curve over k_v. We will restrict to the $\widetilde{E}/k_v$ smooth case, but as in Remark 2.14 the singular case also entails a rich theory. For reference, see Chapter VII in [Sil09].

In a manner reminiscent of the short exact sequence $0 \longrightarrow \mathfrak{m}_v \longrightarrow \mathcal{O}_v \longrightarrow k_v \longrightarrow 0$, we obtain a similar short exact sequence of elliptic curves.

Theorem 3.7. *Let E/K_v be an elliptic curve such that $\widetilde{E}(k_v)$ is smooth.*

(a) Then the reduction modulo $\mathfrak{m}_v$ map induces a surjective group homomorphism $E(K_v) \xrightarrow{q} \widetilde{E}(k_v)$.

(b) The kernel $\ker q$ is independent of the minimal equation chosen for defining $\widetilde{E}/k_v$. We denote it by $E_1(K_v)$. Altogether we obtain a short exact sequence

$$0 \longrightarrow E_1(K_v) \longrightarrow E(K_v) \longrightarrow \widetilde{E}(k_v) \longrightarrow 0.$$

Proof. See Proposition VII.2.1 in [Sil09]. □

Remark 3.8. The suggestive notation $E_1(K_v)$ indeed generalizes to $E_n(K_v)$ for arbitrary non-negative integers n—see Exercise VII.7.4 in [Sil09].

3.2 Elliptic Curve Formal Groups

In the previous subsection, we reduced the study of $E(K_v)$ to that of $E_1(K_v)$ and $\widetilde{E}(k_v)$. The latter is finite since k_v is a finite field, so now we turn to $E_1(K_v)$.

Since K_v is a non-Archimedean local field, it is amenable to analytic arguments. Here, they manifest as formal power series expansions of group operations. Let us take a brief abstract excursion into formal groups.

Definition 3.9. Let A be a commutative ring. A *formal group over A* is a power series $F(X, Y)$ in two variables with coefficients in A satisfying

(a) $F(X, 0) = X$ and $F(0, Y) = Y$.

(b) There exists a unique power series $i(T)$ in one variable with coefficients in A satisfying $F(T, i(T)) = 0$.

(c) $F(X, F(Y, Z)) = F(F(X, Y), Z)$.

(d) $F(X, Y) = F(Y, X)$.

(e) $F(X, Y) = X + Y \mod (X^2, XY, Y^2)$.

We denote formal groups by F/A.

Remark 3.10. Pretending that $F(X, Y)$ gives a binary operation $A \times A \xrightarrow{F} A$, note that (a)–(d) in Definition 3.9 precisely state that F provides a commutative group structure, while (e) says that to first order F simply corresponds to the usual ring addition.

Example 3.11. Let E/K_v be an elliptic curve. We aim to construct a formal group over K_v corresponding to elliptic curve addition. Since power series expansions happen best around the origin and the identity element, we first make a change of variables that sends O to $(0,0)$. More specifically, we set $z = -x/y$ and $w = -1/y$, transforming the defining Weierstrass equation to

$$w = z^3 + a_1zw + a_2z^2w + a_3w^2 + a_4zw^2 + a_6w^3.$$

Notice this is a polynomial expression for w in terms of w and z. By inductively substituting the right hand side, we obtain a formal power series of w in z. Thus we may use z to parametrize our formal group.

By using explicit polynomial formulas for the elliptic curve group operation, we can construct two formal power series $F(z_1, z_2)$ and $i(z)$ that correspond to the elliptic curve group operations. For detailed calculations of this procedure, see IV.1 in [Sil09].

Let A be a commutative ring. The collection of formal groups over A forms a category once we define appropriate morphisms.

Definition 3.12. Let F/A and G/A be formal groups. A *homomorphism from F to G over R* is a power series $f(T)$ in one variable with coefficients in R such that $f(F(X,Y)) = G(f(X), f(Y))$.

Remark 3.13. From here, one defines endomorphisms and isomorphisms of formal groups as usual. Once again pretending that F and G provide commutative group structures, if we additionally pretend that $f(T)$ creates a map $A \xrightarrow{f} A$, then Definition 3.12 indicates f induces a group homomorphism between the groups provided by F and G.

Example 3.14. Let F/A be a formal group, and let m be an integer. We can inductively define a power series $f_m(T)$ by setting

$$f_0(T) = 0 \qquad f_{m+1}(T) = F(f_m(T), T) \qquad f_{m-1}(T) = F(f_m(T), i(T)).$$

These f_m are formal group endomorphisms of F/A. They are analogous to multiplication by m endomorphisms of abelian groups. In fact, if m is a unit in A, then f_m is a formal group isomorphism—see Proposition IV.2.3 in [Sil09]. This reflects the following fact: let $\operatorname{End} A$ be the endomorphism ring of the additive group of A, and let $\operatorname{Aut} A$ be the corresponding automorphism group. Then if $A \longrightarrow \operatorname{End} A$ sends a to the multiplication by a map, the units $A^\times$ are mapped to $\operatorname{Aut} A$.

In Remarks 3.10 and 3.13, we commented that formal groups and their morphisms could ostensibly form groups if only they formed actual maps between sets. The metric properties of K_v allow us to do just that—here we can evaluate the power series described in Examples 3.11 and 3.14 on $\mathfrak{m}_v$.

Definition 3.15. Let E/K_v be an elliptic curve, and let F/K_v be its corresponding formal group law as described in Example 3.11. Then the *group associated to F/K_v*, denoted by $\widehat{E}(\mathfrak{m}_v)$, is the group given as follows. The underlying set of $\widehat{E}(\mathfrak{m}_v)$ is $\mathfrak{m}_v$, the binary operation $\mathfrak{m}_v \times \mathfrak{m}_v \longrightarrow \mathfrak{m}_v$ maps (z_1, z_2) to $F(z_1, z_2)$, and the inverse map $\mathfrak{m}_v \longrightarrow \mathfrak{m}_v$ takes z to $i(z)$.

We now relate this to our original discussion of $E_1(K_v)$.

Proposition 3.16. *Let E/K_v be an elliptic curve given by a minimal equation, and let $\widehat{E}(\mathfrak{m}_v)$ be the group described in Definition 3.15. Then $E_1(K_v)$ and $\widehat{E}(\mathfrak{m}_v)$ are isomorphic via the map*

$$\widehat{E}(\mathfrak{m}_v) \longrightarrow E_1(K_v) \quad \textit{that sends} \quad z \mapsto \left(\frac{z}{w(z)}, -\frac{1}{w(z)}\right).$$

Proof. See Proposition VII.2.2 in [Sil09]. □

Therefore we may use formal group methods to study $E_1(K_v)$ and by extension $E(K_v)$.

3.3 Torsion Points

First, we start with a lemma concerning the torsion of $\widehat{E}(\mathfrak{m}_v)$.

Lemma 3.17. *Let E/K_v be an elliptic curve, and let $\widehat{E}(\mathfrak{m}_v)$ be the group given in Definition 3.15. Let $p = \operatorname{char} k_v$. Then every torsion element in $\widehat{E}(\mathfrak{m}_v)$ has order a power of p.*

Proof. As an immediate reduction, we may multiply torsion elements by powers of p to show it is enough to prove there are no nontrivial torsion elements with order relatively prime to p. Let m be a positive integer prime to p. Then m is not in $\mathfrak{m}_v$, so it is a unit in $\mathcal{O}_v$. Now multiplication by m is precisely the group endomorphism induced by f_m from Example 3.14, and because f_m was a formal group isomorphism, multiplication by m is an actual group isomorphism. Thus it has trivial kernel, making $\widehat{E}(\mathfrak{m}_v)[m] = 0$. □

We immediately use Lemma 3.17 along with our short exact sequence from Theorem 3.7 to obtain the following result.

Theorem 3.18. *Let E/K_v be an elliptic curve, let m be a positive integer not divisible by $p = \operatorname{char} k_v$, and suppose $\widetilde{E}/k_v$ is smooth. Then the reduction map $E(K_v)[m] \xrightarrow{q} \widetilde{E}(k_v)[m]$ on m-torsion is injective.*

Proof. Since Proposition 3.16 and Lemma 3.17 indicate $E_1(K_v)$ has no nontrivial m-torsion, the m-torsion of $E(K_v)$ trivially intersects $E_1(K_v)$. From here, the short exact sequence provided in Theorem 3.7 indicates the m-torsion of $E(K_v)$ embeds into $\widetilde{E}(k_v)$. □

Theorem 3.18 serves as a power tool to calculate $E_{\text{tors}}(K)$. The canonical embedding $K \longrightarrow K_v$ allows one to embed $E(K) \longrightarrow E(K_v)$, and this injection preserves m-torsion points. Then by choosing various valuations v and explicitly calculating the reduced curves $\widetilde{E}(k_v)$, one obtains an upper bound for $E_{\text{tors}}(K)$ using these injections.

Next, we seek a way to provide lower bounds for $E_{\text{tors}}(K_v)$, which will similarly provide lower bounds for $E_{\text{tors}}(K)$. The following result for general number fields achieves this by narrowing the possibilities for p^n-torsion of $\widehat{E}(\mathfrak{m}_v)$.

Lemma 3.19. *Let E/K_v be an elliptic curve, and let $\widehat{E}(\mathfrak{m}_v)$ be the group given in Definition 3.15. Let $p = \operatorname{char} k_v$. If z is a nontrivial torsion element of order p^n in $\widehat{E}(\mathfrak{m}_v)$, then $v(z) \leq v(p)/(p^n - p^{n-1})$.*

Proof. See Theorem IV.6.1 in [Sil09]. □

Proposition 3.20. *Let E/K_v be an elliptic curve with Weierstrass coordinates given by a minimal equation for E, and let P be a nontrivial torsion point in $E(K)$ of order m.*

(a) If m is not a power of $p = \operatorname{char} k_v$, then the coordinates of P lie in $\mathcal{O}_v$.

(b) Let $r = \left\lfloor \dfrac{v(p)}{p^n - p^{n-1}} \right\rfloor$. If $m = p^n$ for some $n \geq 1$, then $v(x(P)) \geq -2r$ and $v(y(P)) \geq -3r$.

Proof. Let $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ be the Weierstrass coordinates defining E/K_v, which is minimal by hypothesis. If either $x(P)$ or $y(P)$ lies in $\mathcal{O}_v$, then the other must as well since $\mathcal{O}_v$ is integrally closed.

Therefore we may consider the case where both coordinates of P have negative valuation. Taking v of both sides of the Weierstrass coordinates yields

$$\begin{aligned} &\min\{2v(y(P)), v(a_1) + v(x(P)) + v(y(P))\} \\ =&\min\{2v(y(P)), v(a_1) + v(x(P)) + v(y(P)), v(a_3) + v(y(P))\} \\ \leq&\min\{3v(x(P)), v(a_2) + 2v(x(P)), v(a_4) + v(x(P)), v(x(P))\} = 3v(x(P)) \end{aligned}$$

where strict inequality can only occur if $2v(y(P)) = v(a_1)+v(x(P))+v(y(P))$. If this indeed occurred, we would have $v(a_1)+v(x(P))+v(y(P)) < 3v(x(P))$ and $v(y(P)) = v(a_1)+v(x(P))$. Because $v(a_1) \geq 0$, we see $v(y(P)) \geq v(x(P))$. But we also have $v(y(P))-v(x(P)) < v(x(P))-v(a_1) < 0$, a contradiction. Finally, if $2v(y(P)) > v(a_1)+v(x(P))+v(y(P))$, then we see $v(y(P)) > v(a_1)+v(x(P)) \geq v(x(P))$. But then our equality becomes $v(y(P)) \leq v(a_1)+v(y(P)) = 2v(x(P)) < v(x(P))$, a contradiction, so the only possibility is that the above equality takes the form $2v(y(P)) = 3v(x(P))$.

We may write this integer as $-6s$ for some positive integer s. The inverse $E_1(K_v) \longrightarrow \widehat{E}(\mathfrak{m}_v)$ of the map described in Proposition 3.16 sends $P \mapsto -x(P)/y(P)$, which lands in $\mathfrak{m}_v$ because $s = v(-x(P)/y(P))$. Lemma 3.17 and the isomorphism given by Proposition 3.16 indicate P must have order a power of p, finishing the proof of (a). Lastly, Lemma 3.19 indicates $s \leq v(p)/(p^n - p^{n-1})$, concluding the proof of (b). □

APPLICATIONS TO GLOBAL THEORY

Let $E/\mathbb{Q}$ be an elliptic curve. We can deduce from Proposition 3.20 the following theorem of Lutz and Nagell, which gives a finite set of possibilities for the elements of $E_{\text{tors}}(\mathbb{Q})$.

Theorem 4.1 (Lutz–Nagell)**.** *Let $E/\mathbb{Q}$ be an elliptic curve given by an equation of the form $y^2 = x^3+Ax+B$, where A and B are integers. If P is a nontrivial torsion point, then its coordinates are both integral. Furthermore, either $y(P) = 0$ or $y(P)^2$ divides $4A^3 + 27B^2$.*

Proof. See Corollary VIII.7.2 in [Sil09]. Proposition 3.20 provides most of the work, and the divisibility statement $y(P)^2 \mid 4A^3 + 27B^2$ is done via the polynomial calculations using Group Law Algorithm III.2.3 in [Sil09]. □

Recall from §1 that Mazur's torsion theorem provides a finite set of groups to which $E_{\text{tors}}(\mathbb{Q})$ may be isomorphic.

Theorem 4.2 (Mazur [Maz77])**.** *Let $E/\mathbb{Q}$ be an elliptic curve. Then $E_{tors}(\mathbb{Q})$ is isomorphic to one of the following:*

(i) $\mathbb{Z}/n\mathbb{Z}$ *for* $1 \leq n \leq 10$ *or* $n = 12$

(ii) $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}$ *for* $1 \leq n \leq 4$.

We shall utilize results from §3 to show that each of the above 15 groups are indeed achieved as $E_{\text{tors}}(\mathbb{Q})$ for some appropriate $E/\mathbb{Q}$. We outline our strategy for calculations as follows. Given Weierstrass coordinate functions for $E/\mathbb{Q}$, we calculate the discriminant Δ. For any prime number p, consider the corresponding elliptic curve $E/\mathbb{Q}_p$ obtained by viewing the Weierstrass coordinates for $E/\mathbb{Q}$ as given over $\mathbb{Q}_p$. This $E/\mathbb{Q}_p$ still has discriminant Δ, so of course these Weierstrass coordinates are minimal if $v(\Delta) = 0$, that is, p does not divide Δ. For such p, we may reduce modulo p to the elliptic curve $\widetilde{E}/\mathbb{F}_p$ given by Definition 3.5, which we can calculate in finite time, and apply Theorem 3.18 to bound $E_{\text{tors}}(\mathbb{Q})$ above.

To obtain a lower bound, we make use of the transformations given by Propositions 2.8 and 2.9 to transform $E/\mathbb{Q}$ to a Weierstrass equation $E'/\mathbb{Q}$ of the form given in Theorem 4.1 if need be. From here, the geometric definition of the group structure shows that nontrivial 2-torsion points P are precisely those with $y(P) = 0$, and we systematically check for torsion elements using the possibilities given by Theorem 4.1.

Example 4.3. Consider the Weierstrass equation $E/\mathbb{Q}$ given by $y^2 = x^3 - 2$. It has $\Delta = -2^6 3^3$. We calculate $\#\widetilde{E}/\mathbb{F}_5 = 6$, which implies there is only nontrivial 2-, 3-, and 5-torsion, and $\#\widetilde{E}/\mathbb{F}_7 = 7$, which implies there is only nontrivial 7-torsion. Altogether $E(\mathbb{Q})$ has no nontrivial torsion, which makes $E_{\text{tors}}(\mathbb{Q}) \cong \mathbb{Z}/1\mathbb{Z}$.

Example 4.4. Let $E/\mathbb{Q}$ be given by $y^2 = x^3+8$, which has discriminant $\Delta = -2^{10}3^3$. The value $\#\widetilde{E}/\mathbb{F}_5 = 6$ implies there is only nontrivial 2-, 3-, 5-, and 6-torsion, while $\#\widetilde{E}/\mathbb{F}_{13} = 16$ implies there is only nontrivial 2-, 4-, 8-, 13-, and 16-torsion. Altogether there can only be 2-torsion, and $\#\widetilde{E}/\mathbb{F}_5 = 6$ implies the 2-torsion is at most $\mathbb{Z}/2\mathbb{Z}$. We indeed have the 2-torsion point $(-2, 0)$ in $E(\mathbb{Q})$, so $E_{\text{tors}}(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$.

Example 4.5. Consider the Weierstrass equation $E/\mathbb{Q}$ given by $y^2 = x^3 + 4$. It has $\Delta = -2^8 3^3$. We calculate $\#\widetilde{E}/\mathbb{F}_5 = 6$, which implies there is only nontrivial 2-, 3-, 5-, and 6-torsion, and $\#\widetilde{E}/\mathbb{F}_7 = 3$, which implies there is only nontrivial 3- and 7-torsion. Altogether $E(\mathbb{Q})$ only has nontrivial 3-torsion, and $\#\widetilde{E}/\mathbb{F}_7 = 3$ implies it is at most $\mathbb{Z}/3\mathbb{Z}$. We indeed find a nontrivial torsion point $(0, 2)$, so we have $E_{\text{tors}}(\mathbb{Q}) \cong \mathbb{Z}/3\mathbb{Z}$.

Example 4.6. Let $E/\mathbb{Q}$ be given by $y^2 = x^3+4x$, which has discriminant $\Delta = -2^{12}$. The value $\#\widetilde{E}/\mathbb{F}_3 = 4$ implies there is only nontrivial 2-, 3-, and 4-torsion, while $\#\widetilde{E}/\mathbb{F}_5 = 8$ implies there is only nontrivial 2-, 4-, 5-, and 8-torsion. Altogether there can only be 2- and 4-torsion. We can find all the nontrivial torsion by inspection—they are $\{(2, 4), (2, -4), (0, 0)\}$, and only $(0, 0)$ is 2-torsion. Therefore the only possibility for this group is $E_{\text{tors}}(\mathbb{Q}) \cong \mathbb{Z}/4\mathbb{Z}$.

Example 4.7. Consider the Weierstrass equation $E/\mathbb{Q}$ given by $y^2 - y = x^3 - x$. It has $\Delta = -11$. We calculate $\#\widetilde{E}/\mathbb{F}_2 = 5$, which implies there is only nontrivial 2- and 5-torsion, and $\#\widetilde{E}/\mathbb{F}_3 = 5$, which implies there is only nontrivial 3- and 5-torsion. Altogether $E(\mathbb{Q})$ only has nontrivial 5-torsion, and $\#\widetilde{E}/\mathbb{F}_7 = 5$ implies it is at most $\mathbb{Z}/5\mathbb{Z}$. Changing coordinates to the isomorphic over $\mathbb{Q}$ Weierstrass equation $E'/\mathbb{Q}$, we get $4A^3 + 27B^2 = 2^8 3^{12} 11$. Testing points, we indeed find a nontrivial torsion point $(-12, 108)$, so we have $E_{\text{tors}}(\mathbb{Q}) \cong \mathbb{Z}/5\mathbb{Z}$.

Example 4.8. Let $E/\mathbb{Q}$ be given by $y^2 = x^3+1$, which has discriminant $\Delta = -2^4 3^3$. The value $\#\widetilde{E}/\mathbb{F}_5 = 6$ implies there is only nontrivial 2-, 3-, 5-, and 6-torsion, while $\#\widetilde{E}/\mathbb{F}_7 = 12$ implies there is only nontrivial 2-, 3-, 4-, 6-, 7-, and 12-torsion. Altogether there can only be 2-, 3-, and 6-torsion. We indeed have a 2-torsion point $(0, -1)$, and we also have another nontrivial torsion point $(-1, 0)$. The count $\#\widetilde{E}/\mathbb{F}_5 = 6$ then implies the 2-torsion is at most $\mathbb{Z}/2\mathbb{Z}$, so $(-1, 0)$ must be either 3- or 6-torsion. This forces $E_{\text{tors}}(\mathbb{Q}) \cong \mathbb{Z}/6\mathbb{Z}$.

Example 4.9. Consider the Weierstrass equation $E/\mathbb{Q}$ given by $y^2 = x^3 - 43 + 166$. It has $\Delta = -2^{19}13$. We calculate $\#\widetilde{E}/\mathbb{F}_3 = 7$, which implies there is only nontrivial 3-, and 7-torsion, and $\#\widetilde{E}/\mathbb{F}_5 = 7$, which implies there is only nontrivial 5- and 7-torsion. Altogether $E(\mathbb{Q})$ only has nontrivial 7-torsion, and $\#\widetilde{E}/\mathbb{F}_3 = 7$ implies it is at most $\mathbb{Z}/7\mathbb{Z}$. Testing points, we indeed find a nontrivial torsion point $(3, 8)$, so we have $E_{\text{tors}}(\mathbb{Q}) \cong \mathbb{Z}/7\mathbb{Z}$.

Example 4.10. Let $E/\mathbb{Q}$ be given by $y^2 + 7xy = x^3 + 16x$, which has discriminant $\Delta = 2^8 3^4 17$. The value $\#\widetilde{E}/\mathbb{F}_5 = 8$ implies there is only nontrivial 2-, 4-, 5-, and 8-torsion, while $\#\widetilde{E}/\mathbb{F}_7 = 8$ implies there is only nontrivial 2-, 4-, 7-, and 8-torsion. Altogether there can only be 2-, 4-, and 8-torsion. Furthermore, $\#\widetilde{E}/\mathbb{F}_5 = 8$ indicates the 4-torsion is at most $\mathbb{Z}/4\mathbb{Z}$. We find the torsion points $\{(0, 0), (-2, 4), (-2, 10), (8, 16)\}$ by inspection, so $\#E_{\text{tors}}(\mathbb{Q}) \geq 5$ and hence $E_{\text{tors}}(\mathbb{Q}) \cong \mathbb{Z}/8\mathbb{Z}$.

Example 4.11. Consider the Weierstrass equation $E/\mathbb{Q}$ given by $y^2 + xy + y = x^3 - x^2 - 14x + 29$. It has $\Delta = -2^9 3^5$. We calculate $\#\widetilde{E}/\mathbb{F}_5 = 9$, which implies there is only nontrivial 3-, 5-, and 9-torsion, and $\#\widetilde{E}/\mathbb{F}_7 = 9$, which implies there is only nontrivial 3-, 7-, and 9-torsion. Altogether $E(\mathbb{Q})$ only has nontrivial 3- and 9-torsion. Switching to the Weierstrass equation $E'/\mathbb{Q}$, which has $4A^3 + 27B^2 = 2^{17} 3^{17}$, we find the nontrivial torsion points $\{(27, 864), (-117, 1296), (99, 648)\}$. Thus $\#E_{\text{tors}}(\mathbb{Q}) \geq 4$, and Mazur's torsion theorem informs us $E_{\text{tors}}(\mathbb{Q}) \ncong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. So we see $E_{\text{tors}}(\mathbb{Q}) \cong \mathbb{Z}/9\mathbb{Z}$ is the only possibility.

Example 4.12. Let $E/\mathbb{Q}$ be given by $y^2 + xy = x^3 - 45x + 81$, which has discriminant $\Delta = 2^{10} 3^5 11$. The value $\#\widetilde{E}/\mathbb{F}_7 = 10$ implies there is only nontrivial 2-, 5-, 7-, and 10-torsion, while $\#\widetilde{E}/\mathbb{F}_{13} = 10$ implies there is only nontrivial 2-, 5-, 10-, 13-torsion. Altogether there can only be 2-, 5- and 10-torsion.

Furthermore, $\#\widetilde{E}/\mathbb{F}_7 = 10$ indicates the 2-torsion is at most $\mathbb{Z}/2\mathbb{Z}$ and the 5-torsion is at most $\mathbb{Z}/5\mathbb{Z}$. Turning to the Weierstrass equation $E'/\mathbb{Q}$ with $4A^3 + 27B^2 = -2^{18}3^{17}11$, we find the 2-torsion point $(75, 0)$. We also obtain a nontrivial non 5-torsion point $(219, 1296)$. Therefore $E_{\text{tors}}(\mathbb{Q}) \cong \mathbb{Z}/10\mathbb{Z}$.

Example 4.13. Consider the Weierstrass equation $E/\mathbb{Q}$ given by $y^2 + 43xy - 210y = x^3 - 210x^2$. It has $\Delta = 2^{12}3^65^37^413$. We calculate $\#\widetilde{E}/\mathbb{F}_{11} = 12$, which implies there is only nontrivial 2-, 3-, 4-, 6-, 11-, and 12-torsion, and $\#\widetilde{E}/\mathbb{F}_{13} = 12$, which implies there is only nontrivial 2-, 3-, 4-, 6-, 12-, and 13-torsion. Altogether $E(\mathbb{Q})$ only has nontrivial 2-, 3-, 4-, 6-, and 12-torsion. Switching to the Weierstrass equation $E'/\mathbb{Q}$, which has $4A^3+27B^2 = -2^{20}3^{18}5^37^413$, we find the only nontrivial 2-torsion point is $(3531, 0)$. Checking for more torsion yields $\{(10587, 952560), (4107, 77760), (1515, 163296), (3027, 22680), (-4533, 508032)\}$. Thus $\#E_{\text{tors}}(\mathbb{Q}) \geq 7$. So Mazur's torsion theorem informs us $E_{\text{tors}}(\mathbb{Q}) \cong \mathbb{Z}/12\mathbb{Z}$ is the only possibility.

Example 4.14. Let $E/\mathbb{Q}$ be given by $y^2 = x^3-4x$, which has discriminant $\Delta = 2^{12}$. The value $\#\widetilde{E}/\mathbb{F}_3 = 4$ implies there is only nontrivial 2-, 3-, and 4-torsion, while $\#\widetilde{E}/\mathbb{F}_5 = 4$ implies there is only nontrivial 2-, 3-, 4-, 5-torsion. Altogether there can only be 2- and 4-torsion. Furthermore, $\#\widetilde{E}/\mathbb{F}_3 = 4$ indicates the torsion subgroup has order at most 4. We immediately find the nontrivial 2-torsion points $\{(0, 0), (2, 0), (-2, 0)\}$, which makes $E_{\text{tors}}(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Example 4.15. Consider the Weierstrass equation $E/\mathbb{Q}$ given by $y^2 = x^3 + 2x^2 - 3x$. It has $\Delta = 2^83^2$. We calculate $\#\widetilde{E}/\mathbb{F}_5 = 8$, which implies there is only nontrivial 2-, 4-, 5-, 8-torsion, and $\#\widetilde{E}/\mathbb{F}_7 = 8$, which implies there is only nontrivial 2-, 4-, 7-, 8-torsion. Altogether $E(\mathbb{Q})$ only has nontrivial 2-, 4-, and 8-torsion. The count $\#\widetilde{E}/\mathbb{F}_7 = 8$ indicates $\#E_{\text{tors}}(\mathbb{Q}) \leq 8$. We find the nontrivial 2-torsion points $\{(0, 0), (1, 0), (-3, 0)\}$, and we also find another torsion point $(-1, 2)$. Thus $\#E_{\text{tors}}(\mathbb{Q}) \geq 5$, so we must have $E_{\text{tors}}(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.

Example 4.16. Let $E/\mathbb{Q}$ be given by $y^2 + 5xy - 6y = x^3 - 3x^2$, which has discriminant $\Delta = 2^23^65^2$. The value $\#\widetilde{E}/\mathbb{F}_7 = 12$ implies there is only nontrivial 2-, 3-, 4-, 6-, 7-, and 12-torsion, while $\#\widetilde{E}/\mathbb{F}_{11} = 12$ implies there is only nontrivial 2-, 3-, 4-, 6-, 11-, and 12-torsion. Altogether there can only be 2-, 3-, 4-, 6-, and 12-torsion. Furthermore, $\#\widetilde{E}/\mathbb{F}_7 = 12$ indicates the torsion subgroup has order at most 12. We turn to the Weierstrass equation $E'/\mathbb{Q}$, which has $4A^3 + 27B^2 = -2^{10}3^{18}5^2$. We immediately find the nontrivial 2-torsion points $\{(-177, 0), (66, 0), (111, 0)\}$, and we also find a 3-torsion point $(-69, 1620)$. Therefore the torsion subgroup must be $E_{\text{tors}}(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$.

Example 4.17. Consider the Weierstrass equation $E/\mathbb{Q}$ given by $y^2+17xy-120y = x^3-60x^2$. It has $\Delta = 2^83^85^47^2$. We calculate $\#\widetilde{E}/\mathbb{F}_{11} = 16$, which implies there is only nontrivial 2-, 4-, 8-, 11-, and 16-torsion, and $\#\widetilde{E}/\mathbb{F}_{13} = 16$, which implies there is only nontrivial 2-, 4-, 8-, 13-, and 16-torsion. Altogether $E(\mathbb{Q})$ only has nontrivial 2-, 4-, and 8-torsion, because Mazur's torsion theorem rules out 16-torsion. Our count $\#\widetilde{E}/\mathbb{F}_{13} = 16$ implies $\#E_{\text{tors}}(\mathbb{Q}) \leq 16$. Switching to the Weierstrass equation $E'/\mathbb{Q}$ has $4A^3 + 27B^2 = -2^{16}3^{20}5^47^2$, we first find the 2-torsion points $\{(282, 0), (-1293, 0), (1011, 0)\}$. Afterwards, we also find other nontrivial torsion points $\{(1227, 22680), (147, 12960), (2307, 97200), (-285, 27216), (-933, 29160)\}$ via checking the possibilities outlined by Lutz-Nagell. So $\#E_{\text{tors}}(\mathbb{Q}) \geq 9$, which forces $\#E_{\text{tors}}(\mathbb{Q}) = 16$. The only such possibility for $E_{\text{tors}}(\mathbb{Q})$ is $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$.

REFERENCES

[Abr95] Dan Abramovich. Formal finiteness and the torsion conjecture on elliptic curves. A footnote to a paper: "Rational torsion of prime order in elliptic curves over number fields" [Astérisque No. 228 (1995), 3, 81–100; MR1330929 (96c:11058)] by S. Kamienny and B. Mazur. *Astérisque*, (228):3, 5–17, 1995. Columbia University Number Theory Seminar (New York, 1992).

[Cas67] J. W. S. Cassels. Global fields. In *Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965)*, pages 42–84. Thompson, Washington, D.C., 1967.

[Fal83] G. Faltings. Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. *Invent. Math.*, 73(3):349–366, 1983.

[Frö67] A. Fröhlich. Local fields. In *Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965)*, pages 1–41. Thompson, Washington, D.C., 1967.

[Kam92] S. Kamienny. Torsion points on elliptic curves and q-coefficients of modular forms. *Invent. Math.*, 109(2):221–229, 1992.

[Kem93] George R. Kempf. *Algebraic varieties*, volume 172 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 1993.

[KM95] S. Kamienny and B. Mazur. Rational torsion of prime order in elliptic curves over number fields. *Astérisque*, (228):3, 81–100, 1995. With an appendix by A. Granville, Columbia University Number Theory Seminar (New York, 1992).

[Maz77] B. Mazur. Modular curves and the Eisenstein ideal. *Inst. Hautes Études Sci. Publ. Math.*, (47):33–186 (1978), 1977.

[Mer96] Loïc Merel. Bornes pour la torsion des courbes elliptiques sur les corps de nombres. *Invent. Math.*, 124(1-3):437–449, 1996.

[Mor22] Louis J. Mordell. On the rational solutions of the indeterminate equations of the third and fourth degrees. *Mathematical Proceedings of the Cambridge Philosophical Society*, 21:179–192, 1922.

[Sil09] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.

[Wei29] André Weil. L'arithmétique sur les courbes algébriques. *Acta Math.*, 52(1):281–315, 1929.