Elliptic Curves, Group Schemes, and Mazur's Theorem

A thesis submitted by

Alexander B. Schwartz

to the

Department of Mathematics

in partial fulfillment of the honors requirements

for the degree of Bachelor of Arts

Harvard University

Cambridge, Massachusetts

April 5, 2004

Acknowledgements

I have benefited greatly from the help of many people. First and foremost, I would like to thank Professor Frank Calegari for his guidance and encouragement through every stage of the process. Without his extensive knowledge and incredible patience this paper would not have been possible. I would also like to thank Professor Noam Elkies for his prominent role in my mathematics education these past four years, as well as the rest of the Harvard Mathematics Department. Finally, I thank my parents for their support during the thesis process and always.

Abstract

This paper gives a proof of Mazur's Theorem, which classifies the possible torsion subgroups of rational elliptic curves. We begin with a reasonably comprehensive introduction to the theory of elliptic curves, including proofs of most of the relevant results. We proceed to review many additional topics in modern number theory and algebraic geometry, including group schemes, Néron models, and modular curves. Finally, we bring together all this material by giving a proof of Mazur's Theorem.

Contents

1 Introduction

The goal of this paper is to prove Mazur's Theorem, which completely classifies the possible torsion subgroups of rational elliptic curves. First proved in 1977, this result relies on many different methods in modern number theory and algebraic geometry. In another sense then, this paper seeks to review many different techniques relevant to these fields, using the proof of Mazur's Theorem as a road map.

Theorem 1.1 (Mazur). *Let $E/\mathbb{Q}$ be an elliptic curve. Then, as an abstract group, either $E_{\text{tors}}(\mathbb{Q}) \cong \mathbb{Z}/n\mathbb{Z}$ for $1 \leq n \leq 10$ or $n = 12$, or $E_{\text{tors}}(\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z}) \oplus (\mathbb{Z}/2n\mathbb{Z})$ for $1 \leq n \leq 4$.*

Proof. This follows immediately from proposition 4.5 and theorem 5.1. □

It is known that all 15 groups do arise for infinitely many rational elliptic curves. We will not discuss this fact further, but see [Kub, p. 217] for explicit parameterizations. In fact we will not deal with any of the small cases here. Rather, we will discuss Mazur's proof in [Ma1] that rational elliptic curves cannot have torsion points of prime order larger than 13. We make this choice because the former involves lengthy computations which are not particularly enlightening, whereas the latter serves as excellent motivation for the theory we will develop. We also mention that Mazur later gave a shorter but more advanced proof of the same result; see [Ma2] for details.

We begin with a review of the theory of elliptic curves, where we focus on those results which will be needed in the proof of Mazur's Theorem. Next we develop the theory of group schemes, and in particular we discuss Néron models for elliptic curves. We then discuss an important result about extensions of cyclotomic fields and briefly review the theory of modular curves, and we give a brief description of the computational methods used to settle the small cases of Mazur's Theorem. Finally, we conclude by giving a proof that no rational torsion points can have large prime order, a result which nicely ties together all the theory developed in this paper.

In terms of prerequisites, we assume that the reader has a graduate level understanding of most mathematical fields. In particular, we freely use without mention fundamental results from algebraic geometry, algebraic number theory, complex analysis, Galois theory, and linear algebra. Also, note that we only use the label "theorem" to describe substantial results when the proofs are not omitted.

2 Elliptic Curves

In this section we give an introduction to the theory of elliptic curves. We begin by studying their geometry, and then we focus our studies on the torsion points. After developing the general theory over arbitrary fields, we focus our studies in the second part on elliptic curves over finite fields, over the complex numbers, and over number fields. Throughout our primary reference is the excellent book by Silverman [Si1], although we cite other sources as needed.

Definition 2.1. *An* elliptic curve (E, O) *over a field* K *is a smooth, projective curve* E *of genus 1 along with a specified point* O*, all defined over* K*.*

In practise we will simply talk about the elliptic curve E/K, and O will be understood to be the base point. Further, as is standard practise we use the notation $E(K')$ to denote the points of E defined over K' for any field extension K' of K.

2.1 The Geometry of Elliptic Curves

Algebraic geometry has its most natural setting over algebraically closed fields. Thus, to study the geometry of elliptic curves, we assume throughout this section that K is an algebraically closed field (except as noted). We will make liberal use of the Riemann-Roch Theorem for curves, which we assume the reader is familiar with. For the statement and a proof see [Har, p. 295-296]. Also, if C/K is a curve and $D \in \mathrm{Div}(C)$ is a divisor, we use the notation $\mathscr{L}(D) = \{f \in K(C)^* : \mathrm{div}\, f \geq -D\} \cup \{0\}$, which is always a finite dimensional K-vector space.

One of the most important properties of an elliptic curve E is the natural group structure on the points of E obtained via the base point. We construct this group structure through a canonical bijection between the points of E and the abelian group $\mathrm{Pic}^0(E)$, as given in the following proposition.

Proposition 2.1. *Let* E/K *be an elliptic curve, and define a map* $\sigma : E \to \mathrm{Pic}^0(E)$ *by sending* P *to the class of* $(P) - (O)$*. Then* σ *is a bijection.*

Proof. It is immediately clear that σ is a well-defined map with image in $\mathrm{Pic}^0(E)$. Let $D \in \mathrm{Div}^0(E)$ be a representative for an arbitrary class in $\mathrm{Pic}^0(E)$, and consider $\mathscr{L}(D + (O))$. By the Riemann-Roch Theorem, this space is one-dimensional over K. Thus, there exists nonzero $f \in K(E)$ so that $\mathrm{div}\, f + D + (O) \geq 0$, where $\mathrm{div}\, f + D + (O)$ has degree one. Hence $\mathrm{div}\, f + D + (O) = (P)$ for some $P \in E$, and consequently $D \sim (P) - (O)$. This shows that σ is surjective. Now suppose that $\sigma(P) = \sigma(Q)$ for $P, Q \in E$. Then $(P) - (O) \sim (Q) - (O)$ in $\mathrm{Div}^0(E)$, that is $\mathrm{div}\, f = (P) - (Q)$ for some $f \in K(E)$. In particular $f \in \mathscr{L}((Q))$, and again by Riemann-Roch this space has dimension 1 over K. However, all the constant functions have divisors $\geq -(Q)$, and so f must be constant. Thus, for some $c \in K^*$, we have $(P) - (Q) = \mathrm{div}\, c = 0$. Hence $(P) = (Q)$, so σ is injective, and the proof is complete. □

In order to do explicit computations with elliptic curves, it is essential to have a representation as the zero locus of some polynomials. The next proposition solves this problem using Weierstrass equations.

Proposition 2.2. *Let* E/K *be an elliptic curve. Then there exist coordinate functions* $x, y \in K(E)$ *and constants* $a_1, a_2, a_3, a_4, a_6 \in K$ *such that the following condition holds. If* $f : E \to \mathbb{P}^2(K)$ *is the map given by* $P \mapsto [x(P) : y(P) : 1]$*, then* f *gives an isomorphism between* E *and the curve* $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$*. Conversely, every such equation gives an elliptic curve with base point* $[0 : 1 : 0]$ *whenever it is smooth.*

Proof. For any positive integer n, the Riemann-Roch Theorem gives that $\mathscr{L}(n(O))$ has dimension n over K. The constant functions make up a one-dimensional subspace, and so there exists $x, y \in K(E)$ with $\{1, x\}$ a basis for $\mathscr{L}(2(O))$ and $\{1, x, y\}$ a basis for $\mathscr{L}(3(O))$. In particular x has a pole of order exactly two at O, and y has a pole of order exactly three at O. Hence $\{1, x, y, x^2, xy, y^2, x^3\} \in \mathscr{L}(6(O))$, a six-dimensional vector-space. So there exists constants $c_1, \ldots, c_7 \in K$, not all zero, with $c_1 + c_2x + c_3y + c_4x^2 + c_5xy + c_6y^2 + c_7x^3 = 0$. Every term has a pole of different order at O except for the last two, and consequently $c_6c_7 \neq 0$. An obvious substitution gives the a_i, and the conditions on x and y imply that O maps to $[0 : 1 : 0]$. We note that the a_i are numbered as 6 minus the order of the pole of their associated term. Calling this curve C, we have a rational map $f : E \to C$. Because E is smooth f is a morphism. The map $x : E \to \mathbb{P}^1(K)$ has degree 2 because x has a pole of order 2 at O and no other poles, and therefore $[K(E) : K(x)] = 2$. Similarly $[K(E) : K(y)] = 3$, so $[K(E) : K(x, y)] = 1$. Therefore f has degree 1. If C is smooth then f is a degree one morphism between smooth curves, and then it must be an isomorphism. So we are done unless C is singular. A simple computation with Weierstrass equations shows that in this case there exists a rational map $g : C \to \mathbb{P}^1(K)$ or degree 1, and the composition $g \circ f$ gives a degree 1 morphism from E to $\mathbb{P}^1(K)$. Both these curves are smooth so $g \circ f$ is an isomorphism, but this is a contradiction because E has genus 1 and $\mathbb{P}^1(K)$ has genus 0. This completes the proof of the first statement.

Now take any smooth Weierstrass equation, and let E be the associated curve. Defining $O = [0 : 1 : 0]$, we see that (E, O) is an elliptic curve assuming E has genus 1. A tedious but entirely straightforward calculation reveals that the differential $\omega = dx/(2y + a_1x + a_3)$ has no zeros or poles on E. Hence $\operatorname{div} \omega = 0$, but a simple application of the Riemann-Roch Theorem shows that $\deg \operatorname{div} \omega' = 2g - 2$ for any differential ω'. So $2g - 2 = 0$ and E has genus 1, as desired. □

With minor alterations, this proof also holds when K is not algebraically closed. Thus, if E/K is an elliptic curve for any field K, then there exists a Weierstrass equation for E with coefficients in K.

Corollary 2.3. *If* $\operatorname{char} K \neq 2, 3$ *then* E *is given by an equation* $y^2 = x^3 + ax + b$ *for* $a, b \in K$.

Proof. This follows immediately from proposition 2.2 by simple algebra. □

Next, using Weierstrass equations we will classify the isomorphism classes of elliptic curves over K. Although the classification holds in all characteristics, we will only prove it here assuming $\operatorname{char} K \neq 2, 3$. See [Si1, p. 325-327] for the remaining cases. First we state a lemma, the proof of which we leave for the reader as an easy exercise.

Lemma 2.4. *Let* $y^2 = x^3 + ax + b$ *be a Weierstrass equation over* K. *Then the corresponding curve is nonsingular, and hence an elliptic curve, exactly when the discriminant* $\Delta = -16(4a^3 + 27b^2)$ *does not vanish.*

Proposition 2.5. *Assume* $\operatorname{char} K \neq 2, 3$, *and let* S *be the set of isomorphism classes of elliptic curves over* K. *Then there exists a bijection* $j : S \to K$, *defined as follows.*

If $y^2 = x^3 + ax + b$ is a representative of some class in S, then this class maps to $j = j(a,b) = 2^8 3^3 a^3/(4a^3 + 27b^2)$.

Proof. First we prove that this map is well-defined. By corollary 2.3, any isomorphism class always has a representative of the given form. Suppose that $y^2 = x^3 + ax + b$ and $y^2 = x^3 + a'x + b'$ are two representatives of the same class. By assumption there exist $x', y' \in K(x,y)$ mapping the first equation to the second. Degree considerations show that x' and y' must be linear in x and y, and straightforward algebra then shows that $(x', y') = (u^2 x, u^3 y)$ for some $u \in K$. One easily checks that j is invariant under this change of variables. By lemma 2.4, we see that $4a^3 + 27b^2$ cannot vanish. So indeed j gives a well-defined map from S to K, as claimed. For surjectivity, let $j_0 \in K$ be arbitrary. If $j_0 \neq 0, 1728$, then $y^2 = x^3 - (1/48 + 36/(j_0 - 1728))x + 1/864 + 2/(j_0 - 1728)$ has nonzero discriminant and $j = j_0$. Also $y^2 = x^3 + x$ has $j = 1728$, and $y^2 = x^3 + 1$ has $j = 0$. Thus j is surjective, as claimed. Finally, suppose that $y^2 = x^3 + ax + b$ and $y^2 = x^3 + a'x + b'$ both give the same value for j. Then $a^3/(4a^3 + 27b^2) = a'^3/(4a'^3 + 27b'^2)$, or $a^3 b'^2 = a'^3 b^2$. Considering what we just showed about elliptic curves with $j = 0, 1728$, it is clear that in any case there exists nonzero $u \in K$ with $a' = u^4 a$ and $b' = u^6 b$. Then $(x', y') = (u^2 x, u^3 y)$ gives an isomorphism between the two given curves, and they represent the same element of S. So j is injective, and the proof is complete. □

Definition 2.2. *If* $\operatorname{char} K \neq 2, 3$ *and E/K is an elliptic curve, then the quantity in K associated to E by proposition 2.5 is called the* j-invariant *of E.*

Having fully characterized elliptic curves over K, we now study maps between them. Recalling the definition of an elliptic curve, it is clear how to define such maps. For the following definition, we do not assume that K is algebraically closed.

Definition 2.3. *Let (E_1, O_1) and (E_2, O_2) be elliptic curves defined over a field K. Then an* isogeny *is a morphism of curves $f : E_1 \to E_2$ such that $f(O_1) = O_2$. If there exists a nonzero such map, then E_1 and E_2 are said to be* isogenous.

Although the group structure is not part of the definition of an elliptic curve, it is certainly central to their study. Thus, we might want to restrict our attention to isogenies which are also group homomorphisms. As the following shows, this is not necessary.

Proposition 2.6. *Let $f : E_1 \to E_2$ be an isogeny of elliptic curves. Then f is a homomorphism for the group structures on E_1 and E_2.*

Proof. For $i = 1, 2$ let $\sigma_i : E_i \to \operatorname{Pic}^0(E_i)$ be the bijection of proposition 2.1, which by definition is a group homomorphism. The result clearly holds if $f(E_1) = O_2$, so suppose that f is a finite map. Then $f_* : \operatorname{Pic}^0(E_1) \to \operatorname{Pic}^0(E_2)$ is a group homomorphism such that the following diagram is commutative:

$$\begin{array}{ccc} E_1 & \xrightarrow{\sigma_1} & \mathrm{Pic}^0(E_1) \\ \Big\downarrow f & & \Big\downarrow f_* \\ E_2 & \xrightarrow{\sigma_2} & \mathrm{Pic}^0(E_2) \end{array}$$

So σ_1, σ_2, and f_* are group homomorphisms, and σ_2 is injective. Thus f must also be a group homomorphism, as desired. □

We next prove a result which will be useful in developing our understanding of isogenies. Also, in the course of the proof we will describe an alternate construction of the group law using Weierstrass equations.

Proposition 2.7. *Let E/K be an elliptic curve, and let the maps $+ : E \times E \to E$ and $- : E \to E$ be given respectively by addition and negation under the group law on E. Then $+$ and $-$ are morphisms.*

Proof. By proposition 2.2 there exists a curve $C \subset \mathbb{P}^2(K)$ which is isomorphic to E and given by a Weierstrass equation. Further, the base point is given by $[0 : 1 : 0]$. Let $L \subset \mathbb{P}^2(K)$ be any line, given by $0 = f(x, y, z) = ax + by + cz$. Then L intersects C at exactly three points counting multiplicities, say $P_1, P_2, P_3 \in C$. Looking at the form of a general Weierstrass equation, it is clear that the line $z = 0$ intersects C with multiplicity three at $O = [0 : 1 : 0]$. Therefore $f/z \in K(C)$ has divisor $\sum_{i=1}^3 (P_i) - 3(O)$. So $\sum_{i=1}^3 ((P_i) - (O)) = 0$ in $\mathrm{Pic}^0(C)$, and consequently $\sum_{i=1}^3 P_i = 0$ in E exactly when the P_i lie on a line in $\mathbb{P}^2(K)$. Thus, to negate a point $P \in C$ we simply draw a line through P and O, and the third intersection of this line with C is $-P$. For our general Weierstrass equation this is the map $(x, y) \mapsto (x, -y - a_1x - a_3)$, which is certainly a morphism. Using similar ideas one can construct explicit rational functions for addition, showing that this map is a morphism as well. The details are tedious but not difficult. For the complete proof see [Si1, p. 68-69]. □

For two elliptic curves E_1 and E_2, let $\mathrm{Hom}(E_1, E_2)$ denote the set of all isogenies from E_1 to E_2. By proposition 2.7, this set has a natural structure as abelian group. Further, if $E_1 = E_2 = E$, then composition give a multiplicative structure to $\mathrm{Hom}(E_1, E_2) = \mathrm{End}(E)$. Distribution holds by proposition 2.6, and $\mathrm{End}(E)$ is in fact a ring (with identity). In particular there exists a ring homomorphism $[\cdot] : \mathbb{Z} \to \mathrm{End}(E)$. So, for each integer m we have a multiplication by m map $[m] : E \to E$. These maps will be essential in our later study of the torsion subgroups of an elliptic curve.

Let E be an elliptic curve. An important tool in the study of endomorphism rings is the map $\deg : \mathrm{End}(E) \to \mathbb{Z}$. The following proposition gives a fundamental result about this map. To prove it would require developing the theory of dual isogenies, which would take us too far afield.

Proposition 2.8. *Let E/K be an elliptic curve. Then the map* $\deg : \mathrm{End}(E) \to \mathbb{Z}$ *is a positive definite quadratic form.*

Proof. See [Si1, p. 88-89]. □

Corollary 2.9. *Let E/K be an elliptic curve. Then* $\deg[m] = m^2$ *for all integers* m.

Proof. The map [1] is the identity, so $\deg[1] = 1$. The result now follows by proposition 2.8. □

In the sequel we will only need corollary 2.9. Although the most natural proof uses proposition 2.8, there are alternate proofs as well. Using Weierstrass equations one can explicitly write down rational functions for $[m]$, giving a lengthy but elementary proof [Si1, p. 105]. Alternatively, the case $K = \mathbb{C}$ follows immediately from the results of section 2.4, and the Lefschetz Principle then implies the statement for all fields of characteristic zero [Si1, p. 164-165].

Finally, we conclude our study of the geometry of elliptic curves with a description of the possible isomorphism types for the endomorphism ring. This result will not be used again, so we omit the proof.

Proposition 2.10. *Let E/K be an elliptic curve. Then* $\mathrm{End}(E)$ *is either* $\mathbb{Z}$ *or an order in a quadratic imaginary field or a quaternion algebra.*

Proof. See [Si1, p. 100-102]. □

2.2 Torsion, the Tate Module, and the Weil Pairing

In this section we study the torsion subgroups of elliptic curves. These groups and their elements play a central role in the study of elliptic curves, and they are very useful for applications to number theory. For example, the torsion points on certain elliptic curves yield an explicit realization of class field theory for quadratic imaginary fields [Si2, ch. 2]. First, we begin with a lemma. We note that an isogeny is called separable just if the corresponding map is, and for the definition of a separable morphism see [Har, p. 300].

Lemma 2.11. *Let $E_1, E_2/K$ be elliptic curves with K algebraically closed, and let $f : E_1 \to E_2$ be a nonzero, separable isogeny. Then* $\ker f \subseteq E_1$ *is a finite subgroup of order* $\deg f$.

Proof. Because f is separable, we know that $f^{-1}(P)$ has $\deg f$ elements for all but finitely many $P \in E_2$. However $f^{-1}(P+Q) = f^{-1}(P) + Q'$ for any $Q' \in f^{-1}(Q)$, and $|f^{-1}(P)|$ is independent of P. Because K is infinite, this implies $|f^{-1}(P)| = \deg f$ for all $P \in E_2$. Hence $\ker f$ has $\deg f$ elements, and by proposition 2.6 it is a subgroup of E_1, as desired. □

Before proceeding with our study of torsion, we mention a sort of converse to lemma 2.11. This result will be necessary for the proof of Mazur's Theorem.

Proposition 2.12. *Let E/K be an elliptic curve, and let $H \subseteq E\left(\overline{K}\right)$ be any finite subgroup which is fixed under* $\mathrm{Gal}\left(\overline{K}/K\right)$. *Then there exists an elliptic curve E'/K and a separable isogeny $f : E \to E'$ defined over K so that* $\ker f = H$.

Proof. There are many approaches to proving this result, but all of them would require excessive space. For an approach using elementary algebraic geometry see [Si1, p. 107]. For a proof of the more general case, taking the quotient of any variety by a finite group of automorphisms, see [Mum, §7]. □

For any elliptic curve E/K and positive integer m, we write $E[m]$ to denote the points in $E\left(\overline{K}\right)$ of order dividing m. For the torsion points defined over K we write $E[m](K)$. Using the above result, we can now completely describe the isomorphism type of $E[m]$. Although we state the full result, we do not prove the case where $\operatorname{char} K$ divides m. This situation will not be necessary for our later work, and its proof requires the use of dual isogenies, among other things.

Proposition 2.13. *Let E/K be an elliptic curve, and let m be a positive integer. Write $m = p^e m'$ where $\operatorname{char} K = p$ and $(p, m') = 1$. If $\operatorname{char} K = 0$ then take $m' = m$. Then either $E[m] \cong (\mathbb{Z}/m'\mathbb{Z}) \oplus (\mathbb{Z}/m'\mathbb{Z})$ or $E[m] \cong (\mathbb{Z}/m\mathbb{Z}) \oplus (\mathbb{Z}/m'\mathbb{Z})$, and which isomorphism holds depends only on E.*

Proof. As mentioned, we will only give a proof for the case $e = 0$, that is p does not divide m. By corollary 2.9 the map $[m] : E \to E$ has degree m^2, and by our assumption $[m]$ must be separable. By lemma 2.11, we see that $E[m] = \operatorname{Ker}[m]$ has m^2 elements. Also then $E[d]$ has d^2 elements for all d dividing m, and the classification of finite, abelian groups shows that the only possibility is $E[m] \cong (\mathbb{Z}/m\mathbb{Z}) \oplus (\mathbb{Z}/m\mathbb{Z})$. This completes the proof for $e = 0$, and for the general result see [Si1, p. 89]. □

We let E_{tors} denote the full torsion subgroup of an elliptic curve E/K, and we let $E_{\text{tors}}(K)$ denote those points which are defined over K. In the following result, we use the notation $\mathbb{Z}_{(p)}$ for the elements of $\mathbb{Q}$ with denominators relatively prime to p.

Corollary 2.14. *Let E/K be an elliptic curve. If $\operatorname{char} K = 0$, then as an abstract group $E_{\text{tors}} \cong (\mathbb{Q}/\mathbb{Z}) \oplus (\mathbb{Q}/\mathbb{Z})$. If $\operatorname{char} K = p$, then either $E_{\text{tors}} \cong (\mathbb{Z}_{(p)}/\mathbb{Z}) \oplus (\mathbb{Z}_{(p)}/\mathbb{Z})$ or $E_{\text{tors}} \cong (\mathbb{Q}/\mathbb{Z}) \oplus (\mathbb{Z}_{(p)}/\mathbb{Z})$.*

Proof. Immediate from proposition 2.13. □

Let E/K be an elliptic curve, and let m be a positive integer. Recalling our geometric description of the group law using Weierstrass equations, it is clear that $[m] : E \to E$ is defined over K. Thus, for any $\sigma \in \operatorname{Gal}\left(\overline{K}/K\right)$ and $P \in E[m]$, we have $[m](\sigma(P)) = \sigma([m](P)) = \sigma(O) = O$. So $\operatorname{Gal}\left(\overline{K}/K\right)$ acts on $E[m]$. In particular, for each integer m not divisible by $\operatorname{char} K$ we have a Galois representation $\operatorname{Gal}\left(\overline{K}/K\right) \to \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$. We would also like to use elliptic curves to construct Galois representations over a ring of characteristic zero. To this end we make the following definition.

Definition 2.4. *Let E/K be an elliptic curve, and let p be a prime. We define the p-adic Tate module $T_p(E) = \varprojlim_n E[p^n]$, where the inverse limit is taken with respect to the map $[p] : E[p^{n+1}] \to E[p^n]$.*

Proposition 2.15. *Let E/K be an elliptic curve and p a prime. Then $T_p(E)$ is a $\mathbb{Z}_p$-module, and as such $T_p(E) \cong \mathbb{Z}_p \times \mathbb{Z}_p$ unless* $\operatorname{char} K = p$. *In this case either $T_p(E) = 0$ or $T_p(E) \cong \mathbb{Z}_p$.*

Proof. For any m the group $E[m]$ has the structure of a $(\mathbb{Z}/m\mathbb{Z})$-module, and thus $T_p(E)$ has the structure of a $\varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$ module. This is simply $\mathbb{Z}_p$, and now the result follows immediately from proposition 2.13. □

Thus, for any elliptic curve E/K and each prime p different from $\operatorname{char} K$, we obtain a Galois representation $\operatorname{Gal}\left(\overline{K}/K\right) \to \mathrm{GL}_2(\mathbb{Z}_p)$. Composing with the determinant we also obtain a map $\operatorname{Gal}\left(\overline{K}/K\right) \to \mathbb{Z}_p^*$. In order to study this latter representation we introduce the Weil pairing, which will also have numerous other applications. First though we need a lemma.

Lemma 2.16. *Let E/K be an elliptic curve, and let $D = \sum_i n_i(P_i) \in \operatorname{Div}(E)$ be arbitrary. Then D is principal if and only if $\sum_i n_i = 0$ and $\sum_i [n_i]P_i = 0$.*

Proof. If D is principal then clearly $\sum_i n_i = 0$. Assuming $D \in \operatorname{Div}^0(E)$, define $P = \sum_i [n_i]P_i$. The map $\operatorname{Div}^0(E) \to E$ given by $D \mapsto P$ is simply the inverse of the map from proposition 2.1. Thus its kernel consists exactly of the principal divisors, and the proof is complete. □

In the following μ_m denotes the set of m^{th} roots of unity. Also, in the proof we frequently use lemma 2.16 without explicit mention.

Proposition 2.17. *Let E/K be an elliptic curve, and let m a positive integer not divisible by* $\operatorname{char} K$. *Then there exists a canonical isomorphism of* $\operatorname{Gal}\left(\overline{K}/K\right)$*-modules $e_m : \bigwedge^2 E[m] \to \mu_m$.*

Proof. We will construct a bilinear, alternating map $e_m : E[m] \times E[m] \to \mu_m$. First let $P_1 \in E[m]$ be arbitrary, so there exists $f \in \overline{K}(E)$ with $\operatorname{div} f = m(P_1) - m(O)$. Take arbitrary $Q \in E[m^2]$ such that $[m]Q = P_1$, and find $g \in \overline{K}(E)$ which satisfies $\operatorname{div} g = \sum_{R \in E[m]}((Q+R)-(R))$. Then $f \circ [m]$ and g^m have divisor $\sum_{R \in E[m]}(m(Q+R)-m(R))$, and, multiplying f by a constant if necessary, we may assume that $f \circ [m] = g^m$. Fix some $P_2 \in E[m]$, and let $X \in E\left(\overline{K}\right)$ be arbitrary so that both $g(P_2 + X)$ and $g(X)$ are defined and nonzero. We define $e_m(P_1, P_2) = g(P_2 + X)/g(X)$. First, we have $g(P_2 + X)^m = f([m]P_2 + [m]X) = f([m]X) = g(X)^m$, and $e_m(P_1, P_2) \in \mu_m$. Thus $g(P_2 + X)/g(X) \in \mu_m$ for all but finitely many values of X, and this function must be independent of X. Further, the construction of g is defined up to a constant multiple, and we see that e_m is in fact a well-defined function from $E[m]^2$ to μ_m, as desired. We now prove various properties of e_m that will imply our desired result.

First we prove linearity. Let $P, Q_1, Q_2 \in E[m]$ be arbitrary, and let $f, g \in \overline{K}(E)$ be the functions corresponding to P. Then for appropriate $X \in E\left(\overline{K}\right)$ we have

$$\begin{aligned} e_m(P, Q_1 + Q_2) &= \frac{g(Q_1 + Q_2 + X)}{g(X)} = \left(\frac{g(Q_1 + (Q_2 + X))}{g(Q_2 + X)}\right)\left(\frac{g(Q_2 + X)}{g(X)}\right) \\ &= e_m(P, Q_1)e_m(P, Q_2). \end{aligned}$$

For linearity in the first factor, let $P_1, P_2, Q \in E[m]$ be arbitrary, and let f_1, f_2, f_3 and g_1, g_2, g_3 correspond to P_1, P_2, and $P_1 + P_2$ respectively. Take $h \in \overline{K}(E)$ with $\operatorname{div} h = (P_1+P_2)-(P_1)-(P_2)+(O)$, so that $f_3 = f_1 f_2 h^m$ after multiplying by a constant as necessary. Composing with $[m]$ we find $f_3 \circ [m] = (f_1 \circ [m])(f_2 \circ [m])(h \circ [m])^m$, or $g_3 = g_1 g_2 (h \circ [m])$. Again taking suitable $X \in E\left(\overline{K}\right)$ we obtain

$$\begin{aligned} e_m(P_1 + P_2, Q) &= \frac{g_3(Q+X)}{g_3(X)} = \frac{g_1(Q+X)g_2(Q+X)h([m]Q+[m]X)}{g_1(X)g_2(X)h([m]X)} \\ &= e_m(P_1, X)e_m(P_2, X), \end{aligned}$$

because $[m]Q = O$. Thus e_m is linear in both factors, and we next prove that it is alternating. By linearity, it is enough to show that $e_m(P, P) = 1$ for all $P \in E[m]$. Let $f, g \in \overline{K}(E)$ correspond to P, and consider the function $\prod_{i=0}^{m-1} f(X - [i]P)$. Its divisor is $\sum_{i=0}^{m-1}(([i+1]P) - ([i]P)) = 0$, so it must be constant. If $Q \in E[m^2]$ satisfies $[m]Q = P$, then $\prod_{i=0}^{m-1} g(X - [i]Q)^m = \prod_{i=0}^{m-1} f([m]X - [i]P)$ is constant, and so must be $\prod_{i=0}^{m-1} g(X - [i]Q)$. Evaluating at X and $X - Q$, we find $\prod_{i=0}^{m-1} g(X - [i]Q) = \prod_{i=1}^{m} g(X - [i]Q)$, or $g(X) = g(X - P)$. From this it follows that $e_m(P, P) = 1$, and finally we have shown that e_m induces a linear map $e_m : \bigwedge^2 E[m] \to \mu_m$. We will complete the proof by showing that e_m is bijective and Galois invariant.

Considering the order of each set, to show bijectivity it is enough to show surjectivity. Take $P \wedge Q$ which generates $\bigwedge^2 E[m]$ as an abelian group, and suppose that $e_m(P, Q)$ is a primitive ℓ^{th} root of unity for some ℓ dividing m. Then $e_m([\ell]P, Q) = 1$, and in fact $e_m(P', Q') = 1$ for all $Q' \in E[m]$ where $P' = [\ell]P$. Letting $f, g \in \overline{K}(E)$ correspond to P', this is $g(X + Q') = g(X)$ for all $Q' \in E[m]$. So there exists $h \in \overline{K}(E)$ with $g = h \circ [m]$, and consequently $f \circ [m] = g^m = (h \circ [m])^m$. The map $[m]$ is a nonzero morphism of smooth curves, so it must be surjective. Then f is a constant times h^m, and the divisor of h must be $(P') - (O)$. Hence $P' = O$ in E, that is $[\ell]P = O$. By the choice of P this implies $\ell = m$, and $e_m(P, Q)$ is a primitive m^{th} root of unity. So e_m is surjective and consequently bijective. Finally, take arbitrary $\sigma \in \operatorname{Gal}\left(\overline{K}/K\right)$, and let $P, Q \in E[m]$ be arbitrary with $f, g \in \bar{K}(E)$ corresponding to P. From the construction it is clear that f^σ and g^σ are the maps corresponding to $\sigma(P)$, and we find for appropriate $X \in E\left(\overline{K}\right)$ that $e_m(\sigma(P), \sigma(Q)) = g^\sigma(\sigma(X)+\sigma(Q))/g^\sigma(\sigma(X)) = \sigma(g(X+Q))/\sigma(g(X)) = \sigma(e_m(P, Q))$. This completes the proof. □

Using the Weil pairing e_m we can begin to limit the possibilities for the rational torsion of an elliptic curve.

Corollary 2.18. *Let $E/\mathbb{Q}$ be an elliptic curve. Then we have either $E_{\text{tors}}(\mathbb{Q}) \cong H$ or $E_{\text{tors}}(\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z}) \oplus H$ for some subgroup $H \subseteq \mathbb{Q}/\mathbb{Z}$.*

Proof. By corollary 2.14 it is enough to show that $E[m] \not\subset E_{\text{tors}}(\mathbb{Q})$ for all $m > 2$. Suppose that $E[m] \subseteq E_{\text{tors}}(\mathbb{Q})$ for some positive integer m. Then $\operatorname{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$ acts trivially on $E[m]$, and by proposition 2.17 it must also act trivially on μ_m. This implies $m \leq 2$, and the proof is complete. □

Of course, this result works equally well with $\mathbb{Q}$ replaced by $\mathbb{R}$. In fact, one can show that for any elliptic curve $E/\mathbb{R}$ either $E(\mathbb{R}) \cong \mathbb{R}/\mathbb{Z}$ or $E(\mathbb{R}) \cong (\mathbb{Z}/2\mathbb{Z}) \oplus (\mathbb{R}/\mathbb{Z})$. To do so here would take us too far afield, but see [Si2, p. 420] for a proof of this result.

2.3 Elliptic Curves over Finite Fields

In this section we will prove the Weil conjectures for elliptic curves. The general conjectures concern the number of points on varieties defined over finite fields, and their proof represents one of the major achievements of modern algebraic geometry; see [Har, app. C] for further information. Here we will only prove them in the case of elliptic curves, which does not require particularly advanced techniques. We will also forgo many other important topics in elliptic curves over finite fields, such as the Hasse invariant. The reader can consult [Si1, ch. 5] for further results. Before proving our main result, we need a couple of lemmas.

Lemma 2.19. *Let $E/\mathbb{F}_q$ be an elliptic curve with some embedding $E \subset \mathbb{P}^2(\mathbb{F}_q)$, and define $\phi : \mathbb{P}^2(\mathbb{F}_q) \to \mathbb{P}^2(\mathbb{F}_q)$ to be the map $[x : y : z] \mapsto [x^q : y^q : z^q]$. Then $\phi \in \mathrm{End}(E)$, and $1 - \phi$ is separable.*

Proof. Take the equation for E and raise all the coefficients to the q^{th} power. Then ϕ maps E to the curve defined this equation. However $\mathbb{F}_q$ is invariant under this map, and because E is defined over $\mathbb{F}_q$ we see that $\phi(E) = E$. Further, it is clearly a rational map which fixes the identity, and ϕ is an isogeny, as claimed. To show that $1 - \phi$ is separable would require developing the theory of invariant differentials, and thus we omit the proof here. See [Si1, p. 83-84] for a proof that in fact $m + n\phi$ is separable for integers m and n if and only if $(m, q) = 1$. □

The map ϕ in the above lemma is called the (q^{th}-power) Frobenius endomorphism of E. For the next result, recall from our work in section 2.2 that for any elliptic curve E/K and prime $p \neq \mathrm{char}\, K$ there exists a map $\mathrm{End}(E) \to \mathrm{End}(T_p(E))$. For arbitrary $\psi \in \mathrm{End}(E)$ we use the notation ψ_p for its image under this map. Also, from proposition 2.15, we can regard ψ_p as a 2×2 matrix with entries in $\mathbb{Z}_p$. Thus $\det \psi_p$ and $\mathrm{tr}\, \psi_p$ are well-defined quantities in $\mathbb{Z}_p$.

Lemma 2.20. *Let $E/\mathbb{F}_q$ be an elliptic curve, let $\psi : E \to E$ be any isogeny, and let p be any prime with $(p, q) = 1$. Then $\det \psi_p = \deg \psi$ and $\mathrm{tr}\, \psi_p = 1 + \deg \psi - \deg(1 - \psi)$.*

Proof. The proof of the first result uses the Weil pairing and dual isogenies, and we must therefore exclude it. See [Si1, p. 135]. For the second result, one simply notes that $\mathrm{tr}\, M = 1 + \det M - \det(1 - M)$ for any 2×2 matrix M with coefficients in any commutative ring with identity. □

Proposition 2.21. *Let $E/\mathbb{F}_q$ be an elliptic curve. Then there exists $\alpha \in \mathbb{C}$ with $|\alpha| = \sqrt{q}$ so that for all positive integers n the curve $E(\mathbb{F}_{q^n})$ contains exactly $q^n - \alpha^n - \bar{\alpha}^n + 1$ points.*

Proof. Let ϕ be the q^{th}-power Frobenius endomorphism of E, and let n be any positive integer. Then ϕ^n fixes exactly those points defined over $\mathbb{F}_q$, and by proposition 2.11 and lemma 2.19 the curve $E(\mathbb{F}_{q^n})$ contains $\deg(1-\phi^n)$ points. Now fix some prime $p \neq \operatorname{char} \mathbb{F}_q$. By lemma 2.20 the characteristic polynomial of ϕ_p has integer coefficients, and we may factor it over $\mathbb{C}$ as $(\lambda-\alpha)(\lambda-\beta)$. We evaluate the characteristic polynomial at any rational number a/b as $\det(a/b-\phi_p) = \det(a-b\phi_p)/b^2 = \deg(a-b\phi)/b^2 \geq 0$, and therefore $\beta = \bar{\alpha}$. Further $\alpha\bar{\alpha} = \det \phi_p = \deg \phi = q$, so $|\alpha| = \sqrt{q}$. Clearly $(\phi^n)_p = \phi_p^n$, and thus the characteristic polynomial of ϕ_p^n is given by $(\lambda-\alpha^n)(\lambda-\bar{\alpha}^n)$. Finally $\deg(1-\phi^n) = \det(1-\phi_p^n) = (1-\alpha^n)(1-\bar{\alpha}^n) = 1-\alpha^n-\bar{\alpha}^n+q^n$, and by the above this completes the proof. □

2.4 Elliptic Curves over $\mathbb{C}$

We begin with a review of the theory of doubly period functions on the complex plane. This area is frequently covered in graduate level complex analysis courses, so we omit the proofs here. For a complete exposition see for example [Ahl, ch. 7].

Proposition 2.22. *Let Λ be any lattice in the complex plane. There there exists an even meromorphic function $\wp(z)$ defined on all of $\mathbb{C}$ such that $\wp(z) = \wp(z+\omega)$ for all $\omega \in \Lambda$. Further $\wp$ is analytic on $\mathbb{C} \setminus \Lambda$, and it has a double pole with residue 0 at every point of Λ. Finally, for every $c \in \mathbb{C}$ the function $\wp(z) - c$ has exactly two zeros modulo Λ, counting multiplicities.*

Definition 2.5. *The function $\wp(z)$ described in proposition 2.22 is called the* Weierstrass $\wp$-function.

For the next proposition we use the notation $G_k(\Lambda) = \sum_{\omega \in \Lambda \setminus \{0\}} \omega^{-2k}$ for any lattice $\Lambda \subset \mathbb{C}$. Simple analytic arguments show that this sum converges for all integers $k > 1$.

Proposition 2.23. *The Weierstrass $\wp$-function associated to some lattice $\Lambda \subset \mathbb{C}$ satisfies the differential equation $\wp'(z)^2 = 4\wp(z)^3 - 60G_2(\Lambda)\wp(z) - 140G_3(\Lambda)$. Further, the cubic $4x^3 - 60G_2(\Lambda)x - 140G_3(\Lambda)$ has nonzero discriminant.*

We next recall a couple results about the space of all meromorphic functions $\mathbb{C}/\Lambda \to \mathbb{C}$.

Proposition 2.24. *Take arbitrary $n_1, \ldots, n_k \in \mathbb{Z}$ and $z_1, \ldots, z_k \in \mathbb{C}$. Then there exists a meromorphic function $\mathbb{C}/\Lambda \to \mathbb{C}$ with divisor $\sum_{i=1}^k n_i(z_i)$ if and only if $\sum_{i=1}^k n_i = 0$ and $\sum_{i=1}^k z_i \in \Lambda$.*

Proposition 2.25. *Let $\Lambda \subset \mathbb{C}$ be a lattice. Then any meromorphic $f : \mathbb{C}/\Lambda \to \mathbb{C}$ can be written as a rational function of $\wp$ and $\wp'$.*

From proposition 2.23 we see the connection between doubly periodic functions and elliptic curves. Because $\wp(z)$ and $\wp'(z)$ satisfy a Weierstrass equation, we might guess that they could be used to give an isomorphism between $\mathbb{C}/\Lambda$ and an elliptic curve over $\mathbb{C}$. This is indeed the case.

Proposition 2.26. *Let $\Lambda \subset \mathbb{C}$ be a lattice with associated Weierstrass function $\wp(z)$, and let $E/\mathbb{C}$ be the elliptic curve given by $y^2 = 4x^3 - 60G_2(\Lambda)x - 140G_3(\Lambda)$. Then the map $f : \mathbb{C}/\Lambda \to E$ given by $z \mapsto [\wp(z) : \wp'(z) : 1]$ is a group isomorphism.*

Proof. By proposition 2.23 the map f is well-defined. Now let $(x, y) \in E$ be arbitrary. By proposition 2.22 there exists $z \in \mathbb{C}/\Lambda$ with $\wp(z) = x$. That same proposition says that $\wp$ is even, and thus $\wp'$ is an odd function. So $\wp'(-z) = -\wp'(z)$. It is clear that $\wp'(z) = \pm y$, so taking $\pm z$ as appropriate we have found an element of $\mathbb{C}/\Lambda$ mapping to (x, y). One easily checks that the point at infinity also lies in the image, and therefore f is surjective. Finally, injectivity easily follows from the last statement in proposition 2.22, and f is bijective.

Now we verify that f is a group homomorphism. It is clear that $f(0) = O$, so let $z_1, z_2 \in \mathbb{C}$ be arbitrary. By proposition 2.24 there exists a meromorphic function $g : \mathbb{C}/\Lambda \to \mathbb{C}$ with $\operatorname{div} g = (z_1 + z_2) - (z_1) - (z_2) + (0)$, and by proposition 2.25 there exists a rational function $G(X, Y) \in \mathbb{C}(X, Y)$ with $g(z) = G(\wp(z), \wp'(z))$. Considering $G(x, y) \in \mathbb{C}(x, y) = \mathbb{C}(E)$, we now have $\operatorname{div} G = (f(z_1+z_2))-(f(z_1))-(f(z_2))+(f(0))$. By lemma 2.16 this implies $f(z_1 + z_2) = f(z_1) + f(z_2)$, and the proof is complete. □

In fact, the above map f is an isomorphism of complex Lie groups; that is f is also a complex analytic map. The usefulness of the above result comes from the fact that every complex elliptic curve has such a representation. This will follow immediately from the following result.

Proposition 2.27. *Let $a, b \in \mathbb{C}$ be arbitrary such that the cubic $4x^3 + ax + b$ has nonzero discriminant. Then there exists a (unique) lattice $\Lambda \subset \mathbb{C}$ such that $a = -60G_2(\Lambda)$ and $b = -140G_3(\Lambda)$.*

Proof. See [Ser, p. 89]. □

Corollary 2.28. *Let $E/\mathbb{C}$ be an elliptic curve. Then there exists a lattice $\Lambda \subset \mathbb{C}$ and a group isomorphism $f : \mathbb{C}/\Lambda \to E$.*

Proof. Immediate from propositions 2.26 and 2.27. □

The obvious remaining problem is to determine when two lattices $\Lambda_1, \Lambda_2 \subset \mathbb{C}$ correspond to isomorphic elliptic curves. Certainly if $\Lambda_2 = c\Lambda_1$ for nonzero $c \in \mathbb{C}$, then multiplication by c gives a group isomorphism $\mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$. We will see shortly that this is the only possibility, and non-homothetic lattices always give non-isomorphic elliptic curves. This follows from the following characterization of maps between complex tori of the form $\mathbb{C}/\Lambda$. The proof is entirely elementary but somewhat lengthy, and we skip the details here.

Proposition 2.29. *Let $E_1, E_2/\mathbb{C}$ be elliptic curves, and let $\Lambda_1, \Lambda_2 \subset \mathbb{C}$ be lattices such that $\mathbb{C}/\Lambda_i \cong E_i$ for $i = 1, 2$. Let $S = \{c \in \mathbb{C} : c\Lambda_1 \subseteq \Lambda_2\}$, and for each $c \in S$ let $f_c : E_1 \to E_2$ be the map induced by the multiplication by c map $\mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$. Then the association $c \mapsto f_c$ gives a bijection $S \to \operatorname{Hom}(E_1, E_2)$.*

Proof. See [Si1, p. 160]. □

Before completing out study of complex elliptic curves we mention a corollary of the above result which we be used in the proof of Mazur's Theorem.

Corollary 2.30. *Let $E/\mathbb{Q}$ be an elliptic curve, and let $f \in \operatorname{End} E$ be an endomorphism defined over $\mathbb{Q}$. Then f is scalar, that is $f = [m]$ for some $m \in \mathbb{Z}$.*

Proof. For any elliptic curve $E/\mathbb{C}$, proposition 2.29 shows that $\operatorname{End} E = \mathbb{Z}$ unless $E = \mathbb{C}/\Lambda$ where $\Lambda \subset \mathbb{C}$ is a lattice with $c\Lambda = \Lambda$ for some non-real $c \in \mathbb{C}$. Simple algebra shows that this can only occur if Λ is generated by $\{\tau_1, \tau_2\}$ with τ_1/τ_2 quadratic over $\mathbb{Q}$, and in this case $\operatorname{End} E \cong \mathcal{O}$ for some order $\mathcal{O}$ in an imaginary quadratic field.

Let $E/\mathbb{Q}$ be an elliptic curve, and suppose that there exists a non-scalar endomorphism of E defined over $\mathbb{Q}$. By the previous paragraph we obtain an action of $\mathcal{O}$ on $E/\mathbb{Q}$ for some order $\mathcal{O}$ in an imaginary quadratic field. This gives an action of $\mathcal{O}$ on $H^0(E/\mathbb{Q}, \Omega^1) \cong \mathbb{Q}$, and this action is faithful because $\mathbb{Z} \subset \mathcal{O}$ acts as $[m]^*\omega = m\omega$. So we have a faithful action of $\mathcal{O}$ on $\mathbb{Q}$, a contradiction because $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Q}$ has dimension greater than one. □

Let $\mathbb{H}$ denote the upper-half plane, that is $\mathbb{H} = \{z \in \mathbb{C} : \operatorname{Im} z > 0\}$. For any $\tau \in \mathbb{H}$ we obtain a lattice $\Lambda \subset \mathbb{C}$ generated by 1 and τ, and by proposition 2.26 this lattice corresponds to a complex elliptic curve. If we then consider the j-invariant of this elliptic curve, we obtain a map $j : \mathbb{H} \to \mathbb{C}$. We let $\mathrm{SL}_2(\mathbb{Z})$ act on $\mathbb{H}$ by $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)(z) = \frac{az+b}{cz+d}$. One easily checks that this is indeed an action. For any $\tau \in \mathbb{H}$ and $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{C})$ the lattice generated by $M(\tau)$ is homothetic to the lattice generated by $a\tau + b$ and $c\tau + d$. Because $ad - bc = 1$, this is also the lattice generated by 1 and τ, and consequently τ and $M(\tau)$ correspond to isomorphic elliptic curves. So j is invariant under $\mathrm{SL}_2(\mathbb{Z})$. We complete this section with the following result which summarizes the above work.

Proposition 2.31. *The map $j : \mathbb{H}/\mathrm{SL}_2(\mathbb{Z}) \to \mathbb{C}$ is bijective.*

Proof. By the above arguments j is a well-defined map. By proposition 2.5 and corollary 2.28 the map j is surjective. Further, we see that j is injective unless there exists $\tau_1, \tau_2 \in \mathbb{H}$ which are inequivalent modulo $\mathrm{SL}_2(\mathbb{Z})$ but yield isomorphic elliptic curves. By proposition 2.29, this means that the lattice generated by 1 and τ_1 is homothetic to the lattice generated by 1 and τ_2. However, one easily checks that this implies $\tau_1 \equiv \tau_2 \bmod \mathrm{SL}_2(\mathbb{Z})$, and the proof is complete. □

2.5 Reduction and Elliptic Curves over Number Fields

We complete our introduction to elliptic curves by considering them over number fields. The study of these objects pervades modern number theory, and many of the most important and deepest conjectures in modern mathematics concern points of elliptic curves defined over number fields. Of course we provide only the barest of introductions to this fascinating field.

One of the primary tools used to study elliptic curves consists of reducing modulo various primes. One takes a Weierstrass equation for the elliptic curve with integral

coefficients, and then reducing each coefficient modulo some prime ideal $\mathfrak{p}$ gives a cubic equation over the residue field of $\mathfrak{p}$. Unfortunately, these equations do not always define elliptic curves, as reducing sometimes gives cubics with vanishing discriminants. So we begin with a study of singular Weierstrass equations and the curves they define.

Proposition 2.32. *Let K be any algebraically closed field, and let $C \subset \mathbb{P}^2(K)$ be a singular curve defined by some Weierstrass equation with coefficients in K. Then C has exactly one singular point, which is either a node or a cusp. Further, there exists a natural group structure on the C_{ns}, the set of nonsingular points of C. If C has a node then as groups $C_{\text{ns}} \cong K^*$, and if C has a cusp then $C_{\text{ns}} \cong K^+$.*

Proof. Let C be given by $0 = f(x,y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6$, for $a_1, a_2, a_3, a_4, a_6 \in K$. One easily checks that the point at infinity is never singular, and, applying a linear shift as necessary, we may assume that the point $(0,0)$ is a singular point on C. Then $\{0,0,0\} = \{f(0,0), f_x(0,0), f_y(0,0)\} = \{-a_6, -a_4, a_3\}$. So C is given by $y^2 + a_1xy = x^3 + a_2x^2$, and from here it is a simple exercise to show that C has no other singular points. To determine the type of singularity at $(0,0)$, we recall that it is a node or cusp if the quadratic form $y^2 + a_1xy - a_2x^2$ has distinct or identical linear factors respectively. Clearly, both are possible. Finally, for the group structure on C_{ns} we refer the reader to [Si1, p. 61]. □

Definition 2.6. *Let E/K be an elliptic curve with K a number field. Let $\mathfrak{p}$ be any prime of K, and let $v : K^* \to \mathbb{Z}$ be the normalized valuation corresponding to $\mathfrak{p}$. A Weierstrass equation $f(x,y) = 0$ for E is said to be* minimal with respect to $\mathfrak{p}$ *if all the coefficients of f have nonnegative valuation and $v(\Delta) \geq 0$ is minimal, where Δ is the discriminant of $f(x,y)$. Let $g(x,y)$ be given by reducing the coefficients of f modulo $\mathfrak{p}$, so that g has coefficients in the residue field of $\mathfrak{p}$. Then E is said to have* good reduction at $\mathfrak{p}$ *if g defines an elliptic curve; otherwise E has* bad reduction at $\mathfrak{p}$. *If the singular curve defined by g has a node then the reduction is called* multiplicative *or* semi-stable*, and if the curve has a cusp then the reduction is called* additive *or* unstable.

In the above definition we used the notion of a discriminant for a general Weierstrass equation, while in section 2.1 we only considered the discriminant of equations of the form $y^2 = x^3 + ax + b$. For the more general definition and the fact that $v(a_1), \ldots, v(a_6) \geq 0$ implies $v(\Delta) \geq 0$ see [Si1, p. 46]. For a proof that the above concepts are well-defined, that distinct minimal Weierstrass equations always give the same type of reduction, see [Si1, p. 180]. The choice of the terms additive reduction and multiplicative reduction follows immediately from proposition 2.32. The terms stable, semi-stable, and unstable come from considerations in the theory of moduli spaces. See [F-M] for a detailed explanation. Another explanation comes from the fact that additive reduction will become either multiplicative reduction or good reduction over an appropriate extension field, as the following result shows. Although we are concerned here with number fields, the result is most naturally stated in the context of local fields. It should be clear how to interpret the various types of reduction in this context.

Proposition 2.33. *Let $E/\mathbb{Q}_p$ be an elliptic curve for some prime p, and suppose that E has additive reduction at the maximal ideal of $\mathbb{Z}_p$. Then there exists an extension field $K/\mathbb{Q}_p$ with ring of integers $\mathcal{O}$ so that E/K has either good or multiplicative reduction at the maximal ideal of $\mathcal{O}$. Furthermore, one can choose K to have absolute ramification index at most six over $\mathbb{Q}_p$.*

Proof. See [B-S, §2]. □

In working with elliptic curves over number fields, it is very useful to have many ways of determining the reduction type at a particular prime. This need is satisfied by a powerful result called the Criterion of Néron-Ogg-Shafarevich. To state the full result would require defining a notion of ramification for Tate modules. Instead we only give one of its statements and also one of its corollaries, which are all that we will need for proving Mazur's Theorem. In the following we use the notation $K(E[m])$ for the field generated over K by the points of order m. Equivalently, this is the extension field of K fixed by the same subgroup of $\mathrm{Gal}\left(\overline{K}/K\right)$ that acts trivially on $E[m]$, which in particular must be a Galois extension.

Proposition 2.34 (Néron-Ogg-Shafarevich). *Let E/K be an elliptic curve with K a number field, let $\mathfrak{p}$ be any finite place of K, and let m be any positive integer not divisible by $\mathfrak{p}$. If K has good reduction at $\mathfrak{p}$, then $K(E[m])$ is unramified at $\mathfrak{p}$, and, if $K(E[m])$ is unramified at $\mathfrak{p}$ for infinitely many positive integer m, then K has good reduction at $\mathfrak{p}$.*

Proof. This result follows from studying elliptic curves over local fields. The proof is not complicated, but going through the details would require developing a lot of extra theory. See [Si1, p. 178] for the first implication and [Si1, p. 184] for the second. □

Corollary 2.35. *Let $E_1, E_2/K$ be elliptic curves with K a number field, and suppose that there exists an isogeny $f : E_1 \to E_2$ defined over K. Then E_1 has good reduction at any given prime of K if and only if E_2 does.*

Proof. Let $\mathfrak{p}$ be any prime of K, and let $m > 1$ be any integer relatively prime to $\deg f$ and not divisible by $\mathfrak{p}$. Then f restricted to $E_1[m]$ is injective, and we obtain a bijective map $f : E_1[m] \to E_2[m]$. Because f is defined over K we see that this is an isomorphism of $\mathrm{Gal}\left(\overline{K}/K\right)$-modules, and consequently $K(E_1[m])$ is unramified over $\mathfrak{p}$ if and only if $K(E_2[m])$ is. This equivalence holds for infinitely many positive integer m, and by proposition 2.34 we see that E_1 has good reduction at K if and only if E_2 does, as desired. □

We now consider the group structure of elliptic curves defined over number fields. The most important result in this area is the Mordell-Weil Theorem. Its proof is far too lengthy to be included here, but fortunately it will not be used in the sequel. However, no introduction to elliptic curves over number fields would be complete without at least stating this important result.

Proposition 2.36 (Mordell-Weil). *Let E/K be an elliptic curve with K a number field. Then $E(K)$ is a finitely generated group.*

Proof. See [Si1, ch. 8]. □

Using this result along with our conclusions based on the Weil pairing, we can further restrict the possible structure of $E_{\text{tors}}(\mathbb{Q})$.

Corollary 2.37. *Let $E/\mathbb{Q}$ be an elliptic curve. Then either $E_{\text{tors}}(\mathbb{Q}) \cong \mathbb{Z}/n\mathbb{Z}$ or $E_{\text{tors}}(\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z}) \oplus (\mathbb{Z}/2n\mathbb{Z})$ for some positive integer n.*

Proof. This follows immediately from corollary 2.18 and proposition 2.36. □

Given that elliptic curves over number fields are finitely generated, the torsion-free part is always of the form $\mathbb{Z}^r$ for some nonnegative integer r; we call r the rank of the elliptic curve. Unfortunately, the proof of the Mordell-Weil Theorem is not effective, and in fact there is no known procedure guaranteed to compute the rank of any elliptic curve, even if we restrict to the case $K = \mathbb{Q}$. However, there are many important conjectures which connect the rank to various properties of analytic functions associated to elliptic curves, and if true they would provide an effective procedure for calculating the rank. The details are beyond the scope of the current paper, but the interested reader can consult [Si1, p. 360-363].

Beyond looking at points defined over given number fields, another natural question concerns finding integral points. The following result, which is a corollary to a theorem of Siegel, solves a generalization of this problem. If K is any number field and S is any set of places including all the infinite places, we use the notation R_S for the set of elements of K which have nonnegative valuation with respect to all the primes not in S.

Proposition 2.38 (Siegel). *Let E/K be an elliptic curve with K a number field, and let $x \in K(E)$ be a coordinate function on E. Let S be any finite set of places of K, including all the infinite places. Then there are only finitely many points $P \in E(K)$ with $x(P) \in R_S$.*

Proof. See [Si1, p. 248]. □

Finally, we complete our introduction to elliptic curves with Shafarevich's Theorem. We will use this result directly in our later work, and it is a fitting conclusion as it combines most of the elements of this section. Also, for future applications of this result, we note that every elliptic curve E over a number field K has good reduction at all but finitely many places. To see this simply write down any Weierstrass equation for E with coefficients in R, and then E has good reductions at all primes not dividing the discriminant of this equation.

Proposition 2.39 (Shafarevich). *Let K be a number field, and let S be a finite set of places of K including all the infinite places. Then, up to isomorphism over K, there are only finitely many elliptic curves defined over K with good reduction at all primes not in S.*

Proof. The full proof depends on details we omitted above, such as using the discriminant of a minimal Weierstrass equation to determine the reduction type. We give an quick outline though, and refer the reader to [Si1, p. 264] for a complete proof. Roughly, suppose we have an elliptic curve E/K with good reduction outside S. Then E has a Weierstrass equation of the form $y^2 = x^3 + ax + b$ with $a, b \in R_S$. Furthermore, the given conditions greatly restrict the possible values for the discriminant of this Weierstrass equation, and, considering the formula for the discriminant, one can write down another elliptic curve and a correspondence between pairs (a, b) and solutions to this curve with coordinate in R_S. By proposition 2.38 this latter elliptic curve can only have finitely many points defined over R_S, and the conclusion follows. □

3 Group Schemes and the Néron Model

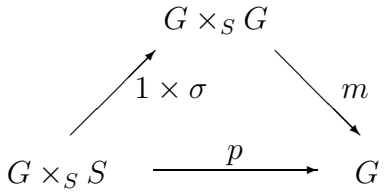
In this section we study group schemes, which play a prominent role in both modern algebraic geometry and number theory. We begin with definitions and basic results, and then we consider the group schemes most relevant to our present concerns, namely the Néron models of elliptic curves. Finally, we mention a couple of results on group schemes which will be needed for the proof of Mazur's Theorem. We assume the reader is already familiar with basic scheme theory, as developed in [Har] for example.

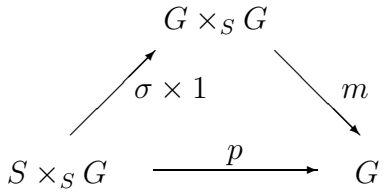
3.1 Definitions and Basic Results

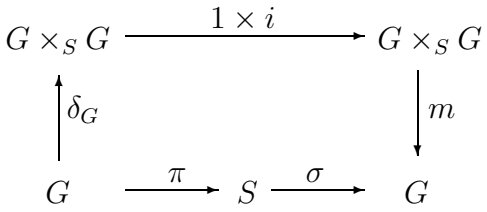
There are many distinct approaches to defining group schemes, although of course ultimately they are all equivalent. Here we adopt an somewhat explicit approach, although we still phrase the group laws in terms of maps rather than actions on individual elements. An alternative approach defines group schemes as representable, covariant functors form the category of schemes to the category of groups. In the proof of Mazur's Theorem we will only encounter commutative group schemes, but we develop the theory in full generality because it requires no extra effort. The material in this section is based on the introductions to group schemes presented in [Si2], [Tat], [Voi], and [Wat].

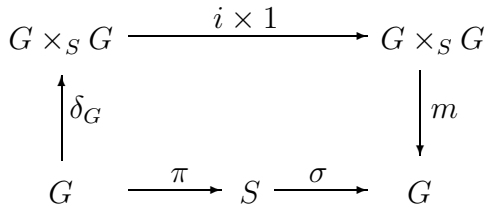
Definition 3.1. *An* S-group scheme *consists of an* S*-scheme* $\pi : G \to S$ *along with three* S*-morphisms, the* unit map $\sigma : S \to G$*, the* inverse map $i : G \to G$*, and the* multiplication map $m : G \times_S G \to G$*, such that the following five diagrams commute. In the below* p *denotes projection, and* $\delta_G : G \to G \times_S G$ *denotes the diagonal morphism.*

$$\begin{array}{ccc} G \times_S G \times_S G & \xrightarrow{m \times 1} & G \times_S G \\ \downarrow{\scriptstyle 1 \times m} & & \downarrow{\scriptstyle m} \\ G \times_S G & \xrightarrow{m} & G \end{array}$$









The name S-group scheme is particularly suitable, as such an object G gives a scheme for defining a group on the T-valued points of G for any other S-scheme T. As usual we have $G(T) = \mathrm{Hom}(T, G)$, the set of all morphisms in the category of S-schemes, and the multiplication map $m_T : G(T) \times G(T) \to G(T)$ is computed in the obvious way as $m_T(f_1, f_2) = m \circ (f_1 \times_S f_2) : T \to G \times_S G \to G$. One can easily check that the axioms for an S-group scheme force $G(T)$ to be a group.

We now give two examples of $\mathbb{Z}$-group schemes, the additive and the multiplicative. Technically they are $(\operatorname{Spec}\mathbb{Z})$-group schemes, but here and elsewhere we sometimes omit the Spec for notational ease. It will always be clear from context what is intended. So consider $\operatorname{Spec}\mathbb{Z}[x]$, and define multiplication $\operatorname{Spec}\mathbb{Z}[x] \times_{\mathbb{Z}} \operatorname{Spec}\mathbb{Z}[x] \to \operatorname{Spec}\mathbb{Z}[x]$ as the dual of the map $\mathbb{Z}[x] \to \mathbb{Z}[x] \otimes_{\mathbb{Z}} \mathbb{Z}[x] \cong \mathbb{Z}[x_1, x_2]$ given by $x \mapsto x_1 + x_2$. This latter map, which always exists by duality in the case of affine group schemes, is called comultiplication. Similarly, the counit map $\mathbb{Z}[x] \to \mathbb{Z}$ is induced by $x \mapsto 0$, and for the coinverse map we take $x \mapsto -x$. To show that these definition make $\operatorname{Spec}\mathbb{Z}[x]$ a group scheme, one simply shows that the diagrams dual to those in definition 3.1 are commutative. The group scheme $\operatorname{Spec}\mathbb{Z}[x]$ is denoted $\mathbb{G}_a$, and it is so called because for any ring R we have $\mathbb{G}_a(R) = \mathbb{G}_a(\operatorname{Spec} R) \cong R^+$, the abelian group underlying R. One can similarly define a $\mathbb{Z}$-group scheme $\mathbb{G}_m$ so that $\mathbb{G}_m(R) \cong R^\times$ for any ring R. In this case $\mathbb{G}_m$ is dual to the ring $\mathbb{Z}[x, x^{-1}]$ with comultiplication $x \mapsto x_1 x_2$, counit $x \mapsto 1$, and coinverse $x \mapsto x^{-1}$.

Repeating the above paragraph verbatim except replacing each occurrence of $\mathbb{Z}$ with an arbitrary commutative ring with identity R, we obtain R-group scheme analogs of the additive and multiplicative groups schemes, which we denote $(\mathbb{G}_a)_R$ and $(\mathbb{G}_m)_R$. However, for any R-algebra A, one easily checks that $(\mathbb{G}_a)_R(A) \cong \mathbb{G}_a(A)$ and $(\mathbb{G}_m)_R(A) \cong \mathbb{G}_m(A)$ as groups. Hence $(\mathbb{G}_a)_R$ and $(\mathbb{G}_m)_R$ are in some sense the same as $\mathbb{G}_a$ and $\mathbb{G}_m$. To formalize this we introduce the concept of a base change. If T and U are S-schemes, we use the notation U_T for the base change of U from S to T, which is given by $U \times_S T$. Clearly U_T is a T-scheme. Any other T-scheme V is also canonically an S-scheme, and we recall that $U_T(V) = U_S(V)$.

Proposition 3.1. *Let G be an S-group scheme, and let T be an S-scheme. Then G_T is a T-group scheme, and for any T-scheme U we have $G_T(U) \cong G(U)$ as groups.*

Proof. Using cumbersome but entirely elementary methods from category theory one can construct the multiplication, unit, and inverse maps for G_T and verify that they satisfy the required properties. Alternatively, the proof comes almost immediately using the functorial definition of a group scheme. See [Tat] for details. □

Using proposition 3.1, we can now explain our observations that $(\mathbb{G}_a)_R(A) \cong \mathbb{G}_a(A)$ and $(\mathbb{G}_m)_R(A) \cong \mathbb{G}_m(A)$ for any commutative ring with identity R and R-algebra A. Every scheme S is uniquely a $(\operatorname{Spec}\mathbb{Z})$-scheme, and the group schemes $(\mathbb{G}_a)_R$ and $(\mathbb{G}_m)_R$ are simply the canonical base changes from $\operatorname{Spec}\mathbb{Z}$ to $\operatorname{Spec} R$.

So far we have developed the theory of arbitrary group schemes, but all our examples have been restricted to affine schemes. In the sequel, we will only be interested in the affine case, and, to simplify matters, for the remainder of this section we assume that all schemes are affine. Recall though that all finite schemes over affine bases schemes are automatically themselves affine [Har, p. 91]. Given this simplifying assumption, we can freely work with the comultiplication, counit, and coinverse maps. We also assume that all rings are commutative with identity and locally noetherian. The former is pretty much always true of rings one considers in algebraic geometry, and the latter will be useful for simplifying many of the definitions. In particular, we note that the below definitions implicitly rely on results using our assumptions and are no longer valid without them.

Definition 3.2. *A* finite flat group scheme of order n *is a* $(\operatorname{Spec} R)$*-group scheme* $\operatorname{Spec} A$ *where A is a locally free R-algebra of rank n.*

We note that finite is a technical term which is stronger than simply requiring the fiber over each point to be finite. A scheme satisfying this latter property is called quasi-finite.

Our first two examples, namely $\mathbb{G}_a$ and $\mathbb{G}_m$, are clearly not finite flat group schemes. To give an example of a finite flat group scheme we construct the constant R-group scheme Γ_R for any finite group Γ. By proposition 3.1 it is enough to restrict to the case $R = \mathbb{Z}$. First, recall that for any finite set X the constant $\mathbb{Z}$-scheme $X_{\mathbb{Z}}$ is the disjoint union $\coprod_{x\in X}(\operatorname{Spec}\mathbb{Z})_x$ of copies of $\operatorname{Spec}\mathbb{Z}$ indexed by X. Further, we know that for any $\mathbb{Z}$-scheme S we have $X_{\mathbb{Z}}(S) = \prod_{i\in I} X$, where I is the set of connected components of S. In light of this, we cannot hope to construct a group scheme $\Gamma_{\mathbb{Z}}$ with $\Gamma_{\mathbb{Z}}(S) \cong \Gamma$ for all schemes S. The best we can hope for is that this holds whenever S is non-empty and connected, and we indeed achieve this goal. Fix a finite group Γ, and let R be the ring $\prod_{\gamma\in\Gamma}\mathbb{Z}_\gamma$. For each $\gamma \in \Gamma$ let e_γ denote the element of R which vanishes on every component except $\mathbb{Z}_\gamma$, where it is given by 1. Then the e_γ form a system of orthogonal idempotents in R. Define comultiplication by $e_\gamma \mapsto \sum_{\gamma_1\gamma_2=\gamma} e_{\gamma_1} e_{\gamma_2}$, define counit by $e_1 \mapsto 1$ and $e_\gamma \mapsto 0$ for $\gamma \neq 1$, and define coinverse by $e_\gamma \mapsto e_{\gamma^{-1}}$. One may easily check that these make $\Gamma_{\mathbb{Z}} = \operatorname{Spec} R$ into a group scheme, and it is clearly finite flat with order the same as that of Γ.

Next we would like to define the notion of a closed subgroup scheme, but we will need a preliminary definition.

Definition 3.3. *Let $G = \operatorname{Spec} A$ be an R-group scheme, and let $I \subset A$ be the kernel of the counit map $A \to R$. Then I is called the* augmentation ideal.

Definition 3.4. *Let $G = \operatorname{Spec} A$ be a group scheme. A closed subgroup scheme of G is a group scheme $H = \operatorname{Spec} A/J$, where J is an ideal in A contained in the augmentation ideal and where the multiplication, identity, and inverse morphisms on H are induced by those on G.*

As an example of these definitions we construct the group scheme μ_n, which has the property that for any ring R the group $\mu_n(R)$ consists of the n^{th} roots of unity in R. As one might expect, we will see that μ_n is a closed subgroup scheme of $\mathbb{G}_m$. First, recall that $\mathbb{G}_m$ is given by $\operatorname{Spec} \mathbb{Z}[x, x^{-1}]$. The counit map is induced by $x \mapsto 1$, and thus the augmentation ideal consists of all polynomials $\sum_{i=-a}^{b} c_i x^i$ with $\sum_{i=-a}^{b} c_i = 0$. In particular, fixing any positive integer n, the ideal $(x^n - 1) \subset \mathbb{Z}[x, x^{-1}]$ is contained in the augmentation ideal. We define $\mu_n = \operatorname{Spec} \mathbb{Z}[x, x^{-1}]/(x^n - 1)$. It is an easy exercise to check that multiplication, unit, and inverse maps on $\mathbb{G}_m$ induce maps on μ_n, and one easily verifies that $\mu_n(R)$ has the previously described form. Finally, we note that μ_n is a finite flat group scheme of order n.

In a typical development of the theory of group schemes, one would next consider kernels and cokernels, quotient group schemes, and other notions analogous to those in group theory. However, in most cases the obvious approaches do not work, just as the naive definition of the cokernel of a map of sheaves only gives a presheaf. Beyond what we have developed so far and the results of section 3.3, the only additional notion we will need in the sequel is that of a map between group schemes. Thus we conclude our review of the basic properties of group schemes with the following definition.

Definition 3.5. *Let G and H be S-group schemes with multiplication maps m_G and m_H respectively. A* homomorphism of S-group schemes *is a map $f : G \to H$ such that f is a morphism of S-schemes and such that the following diagram commutes.*

$$\begin{array}{ccc} G \times_S G & \xrightarrow{m_G} & G \\ \downarrow{\scriptstyle f \times f} & & \downarrow{\scriptstyle f} \\ H \times_S H & \xrightarrow{m_H} & H \end{array}$$

3.2 The Néron Model

This section is primarily based on [Si2, ch. 4]. Any elliptic curve is both a group and a variety, and therefore a scheme. Thus one might expect that all elliptic curves are group schemes. If E/K is an elliptic curve, then indeed E may be given the structure of a K-group scheme. However, this does not yield any new information about E, because $\operatorname{Spec} K$ consists of a single point and the group scheme is essentially just E. If instead we take a Weierstrass equation for E over a commutative ring with identity R, so that E is defined over the field of fractions of R, then a group scheme structure on E would provide lots of new information. Primarily, the fibers of this hypothetical

group scheme lying over the non-generic points of $\operatorname{Spec} R$ would give information on the reduction of E modulo the various prime ideals of R. It is the search for such a group scheme that occupies us in this section.

Let R be a commutative ring with identity with field of fractions K, and let E/K be an elliptic curve given by a Weierstrass equations with coefficients in R. This equation defines a subscheme $S \subset \mathbb{P}^2(R)$, and elementary results on projective schemes shows that $S(R) = E(K)$. The group law extends to a rational map $S \times_R S \to S$, but in general this map is not a morphism. Indeed, recall from section 2.5 that reducing an elliptic curve modulo a prime ideal might yield a curve with a singular point. However, the group law yields a valid morphism on the non-singular part of this curve, and, in the present context, the group law gives a morphism $T \times_R T \to T$, where T denotes the scheme obtained by removing all the singular points on the non-generic fibers of S. We do not prove this result here and cite it only for illustrative purposes. So T is our candidate group scheme, but, while $S(R) = E(K)$, it is possible that $T(R) \neq E(K)$. In our hope that there exists a group scheme $\mathcal{E}$ with $\mathcal{E}(R) = E(K)$, we make the following definition. The term smooth group scheme simply means a group scheme where the underlying scheme is smooth.

Definition 3.6. *Let R be a Dedekind domain with field of fractions K, and let E/K be an elliptic curve. A* Néron model for E/K *is a smooth R-group scheme $\mathcal{E}$ with $\mathcal{E}(R) = E(K)$ that satisfies the* Néron mapping property*. That is, for any smooth R-scheme S with generic fiber C/K and for any K-rational map $\phi_K : C \to E$ there exists a unique R-scheme morphism $\phi_R : S \to \mathcal{E}$ which reduces to ϕ_K on the generic fibers.*

We note that this definition is somewhat redundant, as the Néron mapping property implies $\mathcal{E}(R) = E(K)$. For illustrative purposes though it is useful to explicitly state this as part of the definition. Now, if an elliptic curve has a Néron model, then the fiber of this model over a nonzero prime ideal $\mathfrak{p}$ gives a nonsingular group variety defined over the residue field of $\mathfrak{p}$. This is certainly a very useful property, and we will make heavy use of it in the proof of Mazur's Theorem. The obvious problem now is to determine which elliptic curves have Néron models, and luckily the answer is all of them.

Proposition 3.2. *Let R be a Dedekind domain with field of fractions K, and let E/K be an elliptic curve. Then there exists an R-group scheme $\mathcal{E}$ which is a Néron model for E/K. Further, the group scheme $\mathcal{E}$ is unique up to isomorphism.*

Proof. The proof of this important result is highly technical, and space constraints prevent us from covering the details in the present work. The reader is referred to [Si2, p. 325-338] for the complete proof. However, we can summarize the method of constructing $\mathcal{E}$. There is a general method of "blowing-up" singularities which can be applied to the singular point on the curve at a prime of bad reduction. This method may create new singularities, but after a finite number of applications the process will necessarily terminate to give an R-scheme S that has $S(R) = E(K)$ and many other nice properties. This object is called a proper regular model for E/K, and there exists

a minimal such model. The Néron model is then constructed as the largest subscheme of a minimal proper regular model for E/K which is smooth over R. Finally, the last statement to be proven follows easily from the Néron mapping property. □

Besides their existence, the other central result concerning Néron models describes the structure of their special fibers. Let R be a Dedekind domain with field of fractions K, and let $\mathcal{E}$ be a Néron model over R for the elliptic curve E/K. As mentioned before, the fiber of $\mathcal{E}$ over any nonzero prime ideal $\mathfrak{p} \subset R$ gives a nonsingular group variety defined over the residue field $k_\mathfrak{p}$. Rather than record the full Kodaira-Néron classification, we quote a simpler version that will be sufficient for use in proving Mazur's Theorem. We note that by definition the special fiber over $\mathfrak{p}$ is simply $\mathcal{E}(k_\mathfrak{p})$, and we use the notation $\mathcal{E}(k_\mathfrak{p})^0$ for the connected component of the identity.

Proposition 3.3 (Kodaira-Néron). *Let R be a Dedekind domain with field of fractions K, let $\mathcal{E}$ be a Néron model over R for an elliptic curve E/K, and let $\mathfrak{p} \subset R$ be any nonzero prime ideal with residue field $k_\mathfrak{p}$. If E has stable reduction at $\mathfrak{p}$, then $\mathcal{E}(k_\mathfrak{p}) = \mathcal{E}(k_\mathfrak{p})^0$ is an elliptic curve. If E has semi-stable reduction at $\mathfrak{p}$, then there exists an extension k of $k_\mathfrak{p}$ of degree at most two so that $\mathcal{E}(k)^0 \cong k^*$ and $\mathcal{E}(k)/\mathcal{E}(k)^0 \cong \mathbb{Z}/n\mathbb{Z}$ for some positive integer n. If E has unstable reduction at $\mathfrak{p}$, then $\mathcal{E}(k_\mathfrak{p})^0 \cong k_\mathfrak{p}^+$, and $\mathcal{E}(k_\mathfrak{p})/\mathcal{E}(k_\mathfrak{p})^0$ is a finite group of order at most four.*

Proof. We note that all values for n do occur in the case of semi-stable reduction, and all five groups of order at most four occur in the case of unstable reduction. Also, the reason we may need a quadratic extension in the case of multiplicative reduction is that the relevant theory only applies if the tangent lines to the node have slope defined over k. As usual, the proof is far too lengthy to be included here, but we do mention that it is a primarily straightforward application of intersection theory. For the complete proof see [Si2, p. 361-379]. □

3.3 Further Results on Group Schemes

In this section we collect a couple of results on group schemes which will be needed in the proof of Mazur's Theorem. In both cases the proofs are far too complicated to be included here, and instead we must be satisfied with references to other papers. We note that an abelian (or commutative) group scheme is defined in the obvious way using a commutative diagram.

Proposition 3.4 (Raynaud). *Let p be an odd prime, and let $\mathcal{O}$ be the ring of integers in a field $K/\mathbb{Q}_p$ of absolute ramification less than $p-1$. Let G be a commutative, finite flat $\mathcal{O}$-group scheme of order a power p. The G is uniquely determined up to isomorphism by the isomorphism type of its generic fiber.*

Proof. See [Tat, p. 152]. □

Proposition 3.5. *Let T be an open subscheme of* $\operatorname{Spec}\mathbb{Z}$ *over which 2 is invertible, let A be an abelian T-group scheme, and let p be any prime giving a closed point of T. Then the specialization map $A(T)_{\text{tors}} \to A(\mathbb{F}_p)$ is injective.*

Proof. This follows from a result in [O-T]. See [Ma1, p. 160] for the details of the implication. □

4 Additional Topics

In this section we review a couple of topics not yet covered which are relevant to the proof of Mazur's Theorem. First we discuss Herbrand's Theorem, which concerns unramified extensions of cyclotomic fields, and then we give a brief introduction to the theory of modular curves. We conclude with a quick look at the computational methods used to settle the small cases of Mazur's Theorem, and in particular we reduce to the problem of showing that rational torsion points on elliptic curves cannot have large prime order.

4.1 Extensions of Cyclotomic Fields

Cyclotomic fields are central to number theory, and as such they have been studied extensively for centuries. We record here only those results which will be need for proving Mazur's Theorem.

Let $\mathbb{Q}(\mu_p)$ be the p^{th} cyclotomic field, for p an odd prime, and let K be its Hilbert class field. Let Y' be the maximal quotient of $\text{Gal}(K/\mathbb{Q}(\mu_p))$ where every element has order a power of p, and let Y be the subgroup of Y' generated by elements of order p. In particular, we see that Y is the trivial group whenever p is a regular prime. Now, the group $\text{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$ acts on $\text{Gal}(K/\mathbb{Q}(\mu_p))$ by conjugation in $\text{Gal}(K/\mathbb{Q})$, and via projection $\text{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$ acts on Y as well. Let ζ be any primitive p^{th} root of unity, and let $\sigma \in \text{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$ be arbitrary. Then $\sigma(\zeta) = \zeta^d$ for some $d \in (\mathbb{Z}/p\mathbb{Z})^*$, and d does not depend on the choice of ζ. So there exists a canonical isomorphism $\text{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q}) \to (\mathbb{Z}/p\mathbb{Z})^*$, and we obtain an action of $(\mathbb{Z}/p\mathbb{Z})^*$ on Y. Now, for any integer j, we define $Y^{(j)}$ to be the subgroup of Y on which $a \in (\mathbb{Z}/p\mathbb{Z})^*$ acts as multiplication by a^j. We can now state Herbrand's Theorem.

Proposition 4.1 (Herbrand). *Using the notation from above, let $1 < j < p-1$ be an odd integer. If $Y^{(j)}$ is non-trivial, then the Bernoulli number B_{p-j} has numerator divisible by p.*

Proof. As usual, the proof is beyond the scope of this paper. See [Ma1, p. 52-54] for details. □

4.2 Modular Curves

Recall from proposition 2.31 that we have a bijection $j : \mathbb{H}/\text{SL}_2(\mathbb{Z}) \to \mathbb{C}$, where $\mathbb{H}$ is the upper-half plane and $\text{SL}_2(\mathbb{Z})$ acts as described in section 2.4. The Riemann surface $\mathbb{H}/\text{SL}_2(\mathbb{Z})$ is the simplest example of a modular curve, an object ubiquitous in modern mathematics. We will discuss here only those modular curves used in the proof of Mazur's Theorem, and even in this specific case we must omit proofs. For a

good introduction to the more general theory see [Roh], and for the scheme theoretic perspective see [Del]. Another valuable reference is [Shi].

Fix any positive integer N, and define $\Gamma_0(N) = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}) : c \equiv 0 \bmod N \right\}$. Now let $\tau \in \mathbb{H}$ and $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)$ be arbitrary. Because $M \in \mathrm{SL}_2(\mathbb{Z})$ we know that $M(\tau) \in \mathbb{H}$ corresponds to the same complex elliptic curve as τ. However, the restrictions on $\Gamma_0(N)$ imply that more structure is preserved by this action. So, let Λ be the lattice generated by 1 and τ, and let Λ' be the lattice generated by 1 and $\tau' = M(\tau) = (a\tau + b)/(c\tau + d)$. Then we have an isomorphism $f : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$ given by $z \mapsto z/(c\tau + d)$. We compute that $1/N - f(d/N) = (c/N)\tau/(c\tau + d) \in \Lambda'$ because N divides c. Thus $f(d/N) = 1/N$ in $\mathbb{C}/\Lambda'$, and f preserves the subgroup of order N generated by $1/N$. Thus the points of $\mathbb{H}/\Gamma_0(N)$ correspond to pairs $(E, \mathbb{Z}/N\mathbb{Z})$ where $E/\mathbb{C}$ is an elliptic curve with a fixed subgroup $\mathbb{Z}/N\mathbb{Z} \subset E(\mathbb{C})$.

The above characterization of the points of $\mathbb{H}/\Gamma_0(N)$ shows their immediate usefulness to analyzing elliptic curves. In the case $N = 1$, where $\Gamma_0(N) = \mathrm{SL}_2(\mathbb{Z})$, we have the bijection $j : \mathbb{H}/\Gamma_0(1) \to \mathbb{C}$. We would like a similar structure theorem on the space $\mathbb{H}/\Gamma_0(N)$ for general N, and this is provided by the result we shall state shortly. First though, we need to briefly describe the space $\mathbb{H}^*$. This is defined as $\mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})$, and the action of $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ on $[x : y] \in \mathbb{P}^1(\mathbb{Q})$ is given by $[x : y] \mapsto [ax + by : cx + dy]$. One easily checks that $\mathbb{P}^1(\mathbb{Q})/\mathrm{SL}_2(\mathbb{Z})$ consists of a single point, and one can show that j extends to a bijection $\mathbb{H}^*/\mathrm{SL}_2(\mathbb{Z}) \to \mathbb{P}^1(\mathbb{C})$, where the point $\mathbb{P}^1(\mathbb{Q})/\mathrm{SL}_2(\mathbb{Z})$ maps to the point at infinity.

Proposition 4.2. *Let N be a positive integer. There exists a smooth projective curve $X_0(N)/\mathbb{Q}$ and a bijection $j_{N,0} : \mathbb{H}^*/\Gamma_0(N) \to X_0(N)(\mathbb{C})$ with the following property. Let $\tau \in \mathbb{H}/\Gamma_0(N)$, and let $K = \mathbb{Q}(j_{N,0}(\tau))$. Then τ correspond to a pair (E, C) where E/K is an elliptic curve and $C \subset E$ is a cyclic subgroup of order N also defined over K.*

Proof. See [Shi, §6.7]. □

The curves $X_0(N)$ are modular curves. Not only does the above result give $\mathbb{H}^*/\Gamma_0(N)$ the structure of a smooth projective rational curve, but it also shows how to determine the field of definition of a pair (E, C) corresponding to any point $\tau \in \mathbb{H}^*/\Gamma_0(N)$. Based on this observation one can study the scheme theoretic properties of $X_0(N)$ viewed as a moduli space.

We can only give a brief introduction. If S is a scheme, then the S-valued points of $X_0(N)$ correspond to pairs (E, C) with C a cyclic subgroup or order N in an elliptic curve E, where both E and C are defined over S. For S corresponding to a finite extension of $\mathbb{Q}$ this is explained by proposition 4.2. The other important idea we will need to prove Mazur's Theorem is a modular interpretation for the points of $X_0(N)$ corresponding to $\mathbb{P}^1(\mathbb{Q}) \subset \mathbb{H}^*$. Whenever N is an odd prime one can easily check that $\mathbb{P}^1(\mathbb{Q})/\Gamma_0(N)$ consists of two points, which are sometimes called 0 and ∞. These points, the cusps of $X_0(N)$, in some sense correspond to curves defined by singular Weierstrass equations. To fix ideas, let $E/\mathbb{Q}$ be an elliptic curve with multiplicative reduction at some prime p, let $\mathcal{E}$ be a Néron model for E over $\mathbb{Z}$, and let $C \subseteq E_{\mathrm{tors}}(\mathbb{Q})$ be a cyclic subgroup of order N. Then $\mathcal{E}(\mathbb{F}_p)$ is not an elliptic curve, and instead

it corresponds to one of the cusps. If $C \subset \mathcal{E}(\mathbb{F}_p)^0$ then it corresponds to 0, while if $C \not\subset \mathcal{E}(\mathbb{F}_p)^0$ then it corresponds to ∞.

We conclude this section with a result of Mazur which will be play an essential role in the proof of his Theorem. Conveniently (and not coincidentally), both proofs are given in the same paper [Ma1]. Of all the results in the present paper for which we omit the proofs, the following is by far the most substantive. Indeed, it is in some sense the heart of Mazur's proof of his Theorem.

Proposition 4.3 (Mazur). *Let N be an odd prime. There exists an abelian variety J and a surjective morphism $X_0(N) \to J$ such that $J(\mathbb{Q})$ is a torsion group. Further, if the point $0 - \infty \in X_0(N)$ maps to the identity in J, then $N \leq 13$.*

Proof. See [Ma1, p. 148-150]. We will also give a brief, non-rigorous explanation of the second part here. The morphism $X_0(N) \to J$ factors through the Jacobian, and it turns out that if $0 - \infty$ goes to zero in J then is must go to zero in the Jacobian. From this one concludes $(0) - (\infty)$ must be a principal divisor, and therefore $\mathscr{L}((\infty))$ has dimension at least two. This contradicts the Riemann-Roch Theorem whenever the genus is greater than zero. However, it is well-known that for N prime the curve $X_0(N)$ only has genus zero for $N \leq 7$ or $N = 13$, from which the desired result follows. □

4.3 Computations for Small Cases

In this section we briefly describe the computational methods used to classify the possible p-parts of the rational torsion of an elliptic curve for small primes p. We begin by mentioning a result that is quite useful for computing the torsion subgroup of any explicit rational elliptic curve.

Proposition 4.4 (Nagell-Lutz). *Let $E/\mathbb{Q}$ be an elliptic curve given by a Weierstrass equation $y^2 = x^3 + ax + b$ with $a, b \in \mathbb{Z}$, and let $(x, y) \in E(\mathbb{Q})$ be a nonzero torsion point. Then $x, y \in \mathbb{Z}$, and either $y = 0$ or y^2 divides $4a^3 + 27b^2$.*

Proof. In a treatment on elliptic curves over local fields, one proves that torsion points on elliptic curves satisfy a similar integrality condition, although it is not quite as strict. In particular, points of order a power of p in an elliptic curve over $\mathbb{Q}_p$ do not necessarily have coordinates in $\mathbb{Z}_p$, but one can give reasonable lower bounds on the valuations of these coordinates. The given result is proven by putting together all these local integrality conditions. See [Si1, p. 221] for details. □

In particular, the above gives a computational procedure to effectively determine the torsion subgroup of any given rational elliptic curve. However, to prove results about all rational elliptic curves, more advanced techniques are required. Essentially, one can perform computations using the modular curves described in section 4.2, although the proofs are usually not straightforward. Many of the curves arising in this context have relatively high genus, and one often searches for quotients or other related curves of lower genus to work with. Even so the proofs can be incredibly complicated. For example, showing that no elliptic curve has a rational point of order

25 requires a 71-decent on a curve of genus 4. Beyond these vague generalities though, we must be content to simply quote the conclusions of the involved computations performed by Kubert and many others.

Proposition 4.5 (Kubert). *Suppose that Mazur's Theorem is false. Then there exists an elliptic curve $E/\mathbb{Q}$ so that $E_{\text{tors}}(\mathbb{Q})$ contains a point of prime order $p \geq 23$.*

Proof. See [Kub]. □

5 Proof of Mazur's Theorem

In this section we prove the following result of Mazur, which coupled with proposition 4.5 gives a complete proof of Mazur's Theorem.

Theorem 5.1 (Mazur). *Let $E/\mathbb{Q}$ be an elliptic curve, and suppose that $P \in E_{\text{tors}}(\mathbb{Q})$ is a point of prime order p. Then $p \leq 13$.*

Proof. This follows immediately from lemmas 5.2 and 5.7. □

The proof presented here is very similar to that given in [Ma1, p. 156-160], except that we explain some of the parts in more detail. First we reduce the problem to showing that a certain field extension is unramified. We then study the properties of a constant group scheme sitting inside a Néron model, and we complete the proof by using the conclusions of this study to show that the desired field extension is indeed unramified. The heart of the proof lies in lemma 5.5, which in turn relies primarily on proposition 4.3.

5.1 Reducing to a Question of Ramification

Lemma 5.2. *Let $E/\mathbb{Q}$ be an elliptic curve with a point $P \in E_{\text{tors}}(\mathbb{Q})$ of order p, an odd prime. Then E is rationally isogenous to an elliptic curve $E'/\mathbb{Q}$ with a point of order p so that $\mathbb{Q}(E'[p])$ is a ramified extension of $\mathbb{Q}(\mu_p)$.*

Proof. Recall, from proposition 2.17, that there exists an isomorphism of Galois modules $e_p : \bigwedge^2 E[m] \to \mu_p$. We define a map $E[m] \to \mu_p$ by $Q \mapsto e_p(P, Q)$, and, because $P \in E(\mathbb{Q})$, this gives a short exact sequence of $\text{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$-modules $0 \to \mathbb{Z}/p\mathbb{Z} \to E[p] \to \mu_p \to 0$. Let $K = \mathbb{Q}(E[p])$, which we know must contain $\mathbb{Q}(\mu_p)$. Now, the action of $\text{Gal}(K/\mathbb{Q})$ on $E[p]$ is faithful, and from our exact sequence we have an embedding $\text{Gal}(K/\mathbb{Q}) \to \text{GL}_2(\mathbb{Z}/p\mathbb{Z})$ of the form $\left(\begin{smallmatrix} 1 & * \\ 0 & \chi \end{smallmatrix}\right)$, where $\chi : \text{Gal}(K/\mathbb{Q}) \to \text{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$ is the cyclotomic character. It is clear that there are only two possibilities, namely that the image of $\text{Gal}(K/\mathbb{Q})$ consists of all matrices of the given form or only those of the form $\left(\begin{smallmatrix} 1 & 0 \\ 0 & \chi \end{smallmatrix}\right)$. Further, our short exact sequence of Galois modules is split if and only if we are in the latter situation.

Now suppose, for contradiction, that any rational elliptic curve isogenous to E and with a point of order p always contains a Galois submodule isomorphic to μ_p; this is, suppose that the associated short exact sequence of Galois modules always

splits. Take $E = E_1$, and by proposition 2.12 there exists an elliptic curve $E_2/\mathbb{Q}$ and a rational isogeny $E_1 \to E_2$ with kernel μ_p. Then the image of the Galois submodule $\mathbb{Z}/p\mathbb{Z}$ gives a point of order p in E_2, and by assumption E_2 must also have a cyclic subgroup isomorphic to μ_p. Continuing in this fashion we obtain a sequence of rational isogenies $E_1 \to E_2 \to \cdots$, where each isogeny has kernel μ_p. By corollary 2.35, we see that all the E_i have good reduction at the same set of primes in $\mathbb{Q}$, and by proposition 2.39 we see that $E_i \cong E_j$ for some $i < j$. So composing our isogenies gives a rational endomorphism $f : E_i \to E_i$, and, if $P \in E_i(\mathbb{Q})$ is a point of order p, then by construction $P \notin \operatorname{Ker} f$. However $\deg f$ is a power of p, and therefore f is a non-scalar endomorphism defined over $\mathbb{Q}$, a contradiction by proposition 2.30.

By the previous paragraph there exists an elliptic curve $E'/\mathbb{Q}$ isogenous to E and containing a point of order p so that the associated short exact sequence of Galois modules does not split. Letting K denote $\mathbb{Q}(E'[p])$, the above shows that there exists an isomorphism $\operatorname{Gal}(K/\mathbb{Q}) \to G$, where G is the subgroup of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ consisting of all matrices of the form $\left(\begin{smallmatrix} 1 & k \\ 0 & a \end{smallmatrix}\right)$ with $a \neq 0$. Further, we see that $\operatorname{Gal}(K/\mathbb{Q}(\mu_p))$ corresponds to those matrices with bottom-right entry equal to 1. Now, take arbitrary $a \in (\mathbb{Z}/p\mathbb{Z})^* \cong \operatorname{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$, so that $\left(\begin{smallmatrix} 1 & 0 \\ 0 & a \end{smallmatrix}\right)$ is a representative of the coset corresponding to our element in $\operatorname{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$. Then conjugating $\left(\begin{smallmatrix} 1 & k \\ 0 & 1 \end{smallmatrix}\right)$ by $\left(\begin{smallmatrix} 1 & 0 \\ 0 & a \end{smallmatrix}\right)$ gives $\left(\begin{smallmatrix} 1 & k/a \\ 0 & 1 \end{smallmatrix}\right)$. Suppose, for contradiction, that K is unramified over $\mathbb{Q}(\mu_p)$. Then K is contained in the Hilbert class field of $\mathbb{Q}(\mu_p)$. Because $a \in (\mathbb{Z}/p\mathbb{Z})^*$ acts on $\operatorname{Gal}(K/\mathbb{Q}(\mu_p))$ as multiplication by a^{-1}, in the notation of section 4.1 we see that $Y^{(-1)}$ is nontrivial. Applying proposition 4.1 with $j = p - 2$, we see that the Bernoulli number B_2 must have numerator divisible by p. However $B_2 = 1/6$, giving the desired contradiction. Therefore K is in fact a ramified extension of $\mathbb{Q}(\mu_p)$, and the proof is complete. □

5.2 Analyzing $\mathbb{Z}/p\mathbb{Z} \subset \mathcal{E}$

Throughout this section we fix an elliptic curve $E/\mathbb{Q}$ with $P \in E_{\mathrm{tors}}(\mathbb{Q})$ a point of prime order $p > 13$. Let $\mathcal{E}$ be a Néron model for E over $\mathbb{Z}$, and let $\mathbb{Z}/p\mathbb{Z} \subset \mathcal{E}$ be the constant, finite flat subgroup scheme generated by P. In light of proposition 3.4, we see that P indeed generates $\mathbb{Z}/p\mathbb{Z}$ as a group scheme because we are working in a context of ramification $e = 1 < p - 1$. Also, here and in the next section we use the notation $\cdot^0$ to denote the connected component of the identity.

Lemma 5.3. *The elliptic curve E has either good or multiplicative reduction at all primes q.*

Proof. Suppose, for contradiction, that E has additive reduction at q. By proposition 3.3, we see that $\mathcal{E}(\mathbb{F}_q)^0$ has index at most four in $\mathcal{E}(\mathbb{F}_q)$. Therefore we obtain $\mathbb{Z}/p\mathbb{Z}(\mathbb{F}_q) \subseteq \mathcal{E}(\mathbb{F}_q)^0 \cong \mathbb{F}_q^+$. This is a contradiction unless $q = p$, so suppose that this is the case. By proposition 2.33 there exists an extension field $K/\mathbb{Q}_p$ of absolute ramification index at most six so that E/K has either good or multiplicative reduction at the maximal ideal of $\mathcal{O}$, the ring of integers of K. Let $\mathcal{E}'$ be a Néron model for E over $\mathcal{O}$, and let $\mathcal{E}_{\mathcal{O}}$ denote $\mathcal{E} \times_{\operatorname{Spec} \mathbb{Z}} \operatorname{Spec} \mathcal{O}$, the base change of $\mathcal{E}$ from $\mathbb{Z}$ to $\mathcal{O}$. By the Néron mapping property there exists a morphism $f : \mathcal{E}_{\mathcal{O}} \to \mathcal{E}'$ which is an isomorphism on

the generic fibers. However, as is easily shown, there are no nontrivial maps from an additive group to a multiplicative group or an elliptic curve over given field, and consequently f must be trivial on the special fibers. Let $G \subset \mathcal{E}'$ be the closed subgroup scheme generated by $f(\mathbb{Z}/p\mathbb{Z}(K))$, that is generated by the copy of $\mathbb{Z}/p\mathbb{Z}$ sitting in the generic fiber of $\mathcal{E}'$. Then f restricts to a morphism $g : (\mathbb{Z}/p\mathbb{Z})_{\mathcal{O}} \to G$ which is an isomorphism on generic fibers, and because f is trivial on the special fibers we see that g is not an isomorphism. Now G is quasi-finite by construction, and because it is closed it is finite. Because it sits inside a Néron model it must also be flat, and finally then g is a morphism of commutative, finite flat group schemes of order p which is an isomorphism on generic fibers. However K has absolute ramification index at most $6 < p - 1$ over $\mathbb{Q}_p$, and by proposition 3.4 we see that g must be an isomorphism, a contradiction. □

Lemma 5.4. *The elliptic curve E has bad reduction at 2 and 3.*

Proof. If E has good reduction at some prime q, then $\mathcal{E}(\mathbb{F}_q)$ is an elliptic curve, which by proposition 2.21 has at most $q+2\sqrt{q}+1$ points. We must have $\mathbb{Z}/p\mathbb{Z}(\mathbb{F}_q) \subseteq \mathcal{E}(\mathbb{F}_q)$, and consequently $p \leq q + 2\sqrt{q} + 1$. This is a contradiction for $q < 7$, completing the proof. □

Lemma 5.5. *If E has bad reduction at a prime q, then $\mathbb{Z}/p\mathbb{Z}(\mathbb{F}_q) \not\subset \mathcal{E}(\mathbb{F}_q)^0$.*

Proof. By lemma 5.3, we see that E has multiplicative reduction at q. The field $\mathbb{F}_{q^2}$ contains every quadratic extension of $\mathbb{F}_q$, and by proposition 3.3 we see that $\mathcal{E}(\mathbb{F}_{q^2})^0 \cong \mathbb{F}_{q^2}^*$, a cyclic group of order $q^2 - 1$. So $\mathbb{Z}/p\mathbb{Z}(\mathbb{F}_q) \subseteq \mathcal{E}(\mathbb{F}_q)^0$ can only occur if p divides $q^2 - 1$. In particular, this inclusion does not hold if $q \in \{2, 3, p\}$.

Now suppose, for contradiction, that $\mathbb{Z}/p\mathbb{Z}(\mathbb{F}_q) \subseteq \mathcal{E}(\mathbb{F}_q)^0$. By the previous paragraph we may assume that $q \notin \{2, 3, p\}$. Let S be the scheme $\operatorname{Spec} \mathbb{Z}[1/2p]$, and let x be the S-valued point of $X_0(p)$ determined by the pair $(E_S, (\mathbb{Z}/p\mathbb{Z})_S)$, that is $x = j_{N,0}(E_S, (\mathbb{Z}/p\mathbb{Z})_S)$ via proposition 4.2. Recall that E has multiplicative reduction at 3 and $\mathbb{Z}/p\mathbb{Z}(\mathbb{F}_3) \not\subset \mathcal{E}(\mathbb{F}_3)^0$. From our discussion in section 4.2 of the modular interpretations for the cusps of $X_0(p)$, we see that the value of x lying over 3 is ∞, while the value of x lying over q is 0. Now let $f : X_0(N)(S) \to J(S)$ be the map induced by that in proposition 4.3, where $J(S) = J(\mathbb{Q})$ is a torsion group. By proposition 3.5 the map $J(S) \to J(\mathbb{F}_\ell)$ is injective for $\ell = 3, q$, and we may now conclude that $f(x(\mathbb{F}_3)) = f(x(\mathbb{F}_q))$. This equation is not quite precise, since the two sides lie in different rings, but because the various reduction maps are injective we can make sense of it by identifying rational points with their images. So we have shown $f(0) = f(\infty)$, and $f(0 - \infty)$ is the identity in J. By proposition 4.3 we see that $p \leq 13$, giving the desired contradiction. □

5.3 Completing the Proof

Lemma 5.6. *Let $X/\mathbb{Q}$ be a scheme, and let X' be the scheme $X/\mathbb{Q}_p$ for some prime p. Then $X\left(\overline{\mathbb{Q}}\right)$ is unramified at p if and only if $X'\left(\overline{\mathbb{Q}}_p\right)$ is.*

Proof. Fix any embedding $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_q$, and from this we obtain an injective homomorphism $\mathrm{Gal}\left(\overline{\mathbb{Q}}_q/\mathbb{Q}_q\right) \to \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$ and an injective morphism $X \to X'$. Using the former map we get an action of $\mathrm{Gal}\left(\overline{\mathbb{Q}}_q/\mathbb{Q}_q\right)$ on X; this group clearly acts on X' as well, and by construction these actions commute with latter map. To put it more concisely, localization commutes with Galois action, and our desired result now follows immediately. □

Lemma 5.7. *Let $E/\mathbb{Q}$ be an elliptic curve with $P \in E_{\mathrm{tors}}(\mathbb{Q})$ a point of prime order $p > 13$. Then $\mathbb{Q}(E[p])$ is an unramified extension of $\mathbb{Q}(\mu_p)$.*

Proof. Define $K = \mathbb{Q}(E[p])$. By proposition 2.34, we see that K is unramified at all primes of $\mathbb{Q}(\mu_p)$ lying over rational primes of good reduction for E, except possibly those primes lying over p. Now let q be a prime of bad reduction, and let $\mathcal{E}$ be the Néron model of E over $\mathbb{Z}_q$. We claim that $\mathcal{E}^0[p]$ is nontrivial. By lemma 5.3 we know that E has multiplicative reduction at q, and thus $\mathcal{E}^0$ is given by $\mathbb{G}_m$ over $\overline{\mathbb{F}}_q$, which has points of all orders relatively prime to q. The case $p = q$ is a little trickier, but reasoning with Tate curves shows that $\mu_p \subseteq \mathcal{E}^0$, which proves our claim in this case as well; see [Si2, ch. 5] for an introduction to Tate curves. Now consider the short exact sequence of groups $0 \to \mathcal{E}^0\left(\overline{\mathbb{Q}}_q\right) \to \mathcal{E}\left(\overline{\mathbb{Q}}_q\right) \to \mathcal{E}\left(\overline{\mathbb{Q}}_q\right)/\mathcal{E}^0\left(\overline{\mathbb{Q}}_q\right) \to 0$. By lemma 5.5 and our claim, the restriction of this exact sequence to $E[p]$ must split. By the reasoning in the proof of lemma 5.2, we see that $\mathbb{Q}_q(E[p])$ is unramified over $\mathbb{Q}_q(\mu_p)$ at all primes lying over q, and by lemma 5.6 we conclude that $\mathbb{Q}(E[p])$ is unramified over $\mathbb{Q}(\mu_p)$ at all primes lying over q. Finally, we will show that this extension is unramified over the primes lying over p whenever E has good reduction at p. Suppose this is the case, and consider the short exact sequence of $\mathbb{Z}_p$-group schemes $0 \to \mathbb{Z}/p\mathbb{Z} \to E[p] \to \mu_p \to 0$. Over $\overline{\mathbb{F}}_p$ the group $\mathbb{Z}/p\mathbb{Z}$ is completely disconnected, while μ_p collapses to a point. Applying the "connected component of the identity" functor shows that $E[p]^0 = \mu_p$, and this exact sequence must also split. As before we conclude that $\mathbb{Q}(E[p])$ is unramified over $\mathbb{Q}(\mu_p)$ at all primes lying over p, and the proof is complete. □

6 Conclusion

In this course of this paper we have accomplished many things. We have learned a good deal about elliptic curves, and we have discussed many areas that can be used to solve difficult problems in number theory. In proving Mazur's Theorem, we have seen an example of how all these previous results may be applied, and we have also demonstrated a fairly interesting result. There are two obvious avenues for further work.

First, one could more fully understand many of the topic only briefly considered here. Most notably, the theory of modular curves is a fascinating subject to which we only gave the barest of introductions. A further study of these curves and related objects, such as modular functions and automorphic forms, would be quite rewarding. One might explore further topics in elliptic curves or perhaps study abelian varieties, a generalization of elliptic curves to higher dimensional varieties. Finally, one might

study any of the numerous other topic touched on in this paper, such as Herbrand's Theorem or Néron models.

The second direction for future work is a study of the generalizations of Mazur's Theorem. The most obvious consideration is to classify the possible group structures for $E_{\text{tors}}(K)$, with K a specific or perhaps general class of number fields. For the primary paper discussing this problem see [Mer]. Finally, one might study the more advanced techniques used for the shorter proof of Mazur's Theorem in [Ma2].

References

[Ahl] L. Ahlfors. *Complex Analysis*. McGraw-Hill, Inc., 1979.

[B-S] Z. Borevich and I. Shafarevich. *Number Theory*. Academic Press, 1966.

[Del] P. Deligne. Formes modulaires et représentations ℓ-adiques. In *Séminaire Bourbaki, exposé 355, Lecture Notes in Mathematics 179*, pages 139–172. Springer-Verlag, 1971.

[F-M] J. Fogerty and D. Mumford. *Geometric Invariant Theory*. Springer-Verlag, 1982.

[Har] R. Hartshorne. *Algebraic Geometry*. Springer-Verlag, 1977.

[Kub] D. Kubert. Universal bounds on the torsion of elliptic curves. *Proc. London Math. Soc. (3)* **33**(1976), 193–237.

[Ma1] B. Mazur. Modular curves and the Eisenstein ideal. *IHES Publ. Math.* **47**(1977), 33–186.

[Ma2] B. Mazur. Rational isogenies of prime degree. *Invent. Math.* **44**(1978), 129–162.

[Mer] L. Merel. Bornes pour la torsion des courbes elliptiques sur les corps de nombres. *Invent. Math.* **124**(1996), 437–449.

[Mum] D. Mumford. *Abelian Varieties*. Oxford Univ. Press, 1974.

[O-T] F. Oort and J. Tate. Group schemes of prime order. *Ann. Sci. École Norm. Sup. (4)* **3**(1970), 1–21.

[Roh] D. Rohrlich. Modular curves, Hecke correspondences, and L-functions. In *Modular Forms and Fermat's Last Theorem*, pages 41–100. Springer, 1997.

[Ser] J.-P. Serre. *A Course in Arithmetic*. Springer, 1973.

[Shi] G. Shimura. *Introduction to the Arithmetic Theory of Automorphic Functions*. Princeton Univ. Press, 1971.

[Si1] J. Silverman. *The Arithmetic of Elliptic Curves*. Springer-Verlag, 1986.

[Si2] J. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*. Springer-Verlag, 1994.

[Tat] J. Tate. Finite flat group schemes. In *Modular Forms and Fermat's Last Theorem*, pages 121–154. Springer, 1997.

[Voi] J. Voight. Introduction to Finite Group Schemes. Lecture notes for a course taught at Berkeley, available at http://math.berkeley.edu/∼jvoight/notes/.

[Wat] W. Waterhouse. *Introduction to Affine Group Schemes*. Springer-Verlag, 1979.