RATIONAL POINTS ON MODULAR CURVES: A DIOPHANTINE APPLICATION OF ALGEBRAIC GEOMETRY

Hanson Hao

A thesis submitted to the Department of Mathematics in partial fulfillment of the requirements for the undergraduate honors program

Stanford University
June 2023

Abstract

Elliptic curves over $\mathbf{Q}$ are objects of fundamental arithmetic interest. In 1971, Ogg conjectured a relationship between the genera of the modular curves $X_1(N)$ and the possible groups that can appear as the torsion group $E(\mathbf{Q})_{\text{tors}}$ of such elliptic curves, setting off a program of work that culminated with Mazur's full classification in 1978 [18]. Our goal in this thesis is to give a detailed exposition of the key exceptional case $N = 13$ worked out by Mazur and Tate [19], prefaced by developing the scheme-theoretic background on relative elliptic curves and modular curves necessary for this goal.

Contents

1 Introduction

The main subject of this thesis is the arithmetic of elliptic curves. Recall that classically (i.e. over a field k), an elliptic curve is given by a smooth genus 1 curve E/k with a chosen point $0 \in E(k)$, and the pointed set of rational points $E(k)$ can be naturally equipped with the structure of an abelian group. For k a number field, the study of the structure of this group begins with the following famous theorem, proved by Mordell in 1922 for $k = \mathbf{Q}$:

Theorem 1.0.1. If E is an elliptic curve over a number field k, then $E(k)$ is a finitely generated abelian group.

Given Mordell's Theorem, one natural question is to ask for the possible groups that could occur as the torsion group $E(\mathbf{Q})_{\text{tors}}$ for elliptic curves E over $\mathbf{Q}$. To approach this question, one builds certain *modular curves* $Y_1(N)$ over $\mathbf{Q}$, where the $\mathbf{Q}$-points of $Y_1(N)$ correspond to pairs (E, P), where E is an elliptic curve over $\mathbf{Q}$ equipped with a point $P \in E(\mathbf{Q})$ of exact order N. In other words, if $Y_1(N)(\mathbf{Q})$ is nonempty then there is some elliptic curve E with $E(\mathbf{Q})_{\text{tors}}$ containing $\mathbf{Z}/N\mathbf{Z}$ as a subgroup, and conversely if $Y_1(N)(\mathbf{Q})$ is empty then $E(\mathbf{Q})_{\text{tors}}$ can never contain $\mathbf{Z}/N\mathbf{Z}$.

To understand the rational points of $Y_1(N)$, one builds its *compactification* $X_1(N)$, which is a geometrically connected smooth projective curve over $\mathbf{Q}$, so we can speak of its genus. It turns out that $g(X_1(N))$ is 0 exactly when $4 \leq N \leq 10$ or $N = 12$ (we need to exclude $N = 1, 2, 3$ due to the presence of nontrivial automorphisms preserving some pairs (E, P), so the moduli problem that would give rise to $Y_1(N)$ is not representable). For such N, $X_1(N) \cong \mathbf{P}^1_{\mathbf{Q}}$ because $X_1(N)(\mathbf{Q}) \neq \emptyset$ (via a "degenerate N-gon" over $\mathbf{Q}$), so $Y_1(N)$ has many rational points. Following [16, Table 3], here are some parameterizations for elliptic curves E over any field k with $\text{char}(k) \nmid N$, where $E(k)$ contains a point with exact order N:

- For $N = 4$: let E_t be the elliptic curve given by the Weierstrass equation

$$y^2 + xy - ty = x^3 - tx^2,$$

  subject to the condition that the discriminant $\Delta(t) = t^4(1 + 16t)$ is nonzero. Then $(0, 0)$ has exact order 4 in $E_t(k)$.

- For $N = 5$: let E_t be the elliptic curve given by the Weierstrass equation

$$y^2 + (1 - t)xy - ty = x^3 - tx^2,$$

  subject to the condition that the discriminant $\Delta(t) = -t^5(t^2 - 11t - 1)$ is nonzero. Then $(0, 0)$ has exact order 5 in $E_t(k)$.

- For $N = 10$: let E_t be the elliptic curve given by the Weierstrass equation

$$y^2 + (1 + c(t))xy - b(t)y = x^3 - b(t)x^2$$

where $c(t) = t(t-1)(2t-1)/(t^2-3t+1)$ and $b(t) = t^3(t-1)(2t-1)/(t^2-3t+1)^2$, subject to the conditions that $t^2-3t+1 \neq 0$ (so $c(t)$ and $b(t)$ make sense) and the discriminant $\Delta(t)$ is nonzero. Then $(0,0)$ has exact order 10 in $E_t(k)$.

Note that the condition $\Delta(t) \neq 0$ entails that the product $t^{10}(t-1)^{10}(2t-1)^5(4t^2-2t-1)$ of $\mathbf{Q}$-irreducible polynomials is nonzero.

On the other hand, for N such that $g(X_1(N)) > 0$, we may not have many rational points on $X_1(N)$ at all, and consequently $Y_1(N)(\mathbf{Q})$ might be empty (in the case that all of the rational points of $X_1(N)$ lie in the complement of $Y_1(N)$). For $N = 11$, where $g(X_1(11)) = 1$, this is indeed the case: work of Billing and Mahler [2] shows that $X_1(11)$ can be explicitly described as the elliptic curve $y^2 - y = x^3 - x^2$, which only has 5 rational points, none of which lie on $Y_1(11)$ (there are 5 non-isomorphic "degenerate" objects over $\mathbf{Q}$, so these account for the $\mathbf{Q}$-points). This result led Ogg to conjecture [22] that $Y_1(N)(\mathbf{Q})$ is empty if $g(X_1(N)) > 0$. After proving this conjecture for N a prime greater than 13 and several small exceptional values of N (e.g. 13, 18, 25), the final classification was given by Mazur [18]:

Theorem 1.0.2 (Mazur [18])**.** The torsion group $E(\mathbf{Q})_{\text{tors}}$ of an elliptic curve $E/\mathbf{Q}$ is isomorphic to one of the following groups:

- $\mathbf{Z}/N\mathbf{Z}$ for $1 \leq N \leq 10$ or $N = 12$.
- $\mathbf{Z}/N\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ for $N = 2, 4, 6, 8$.

A proof of this theorem is well beyond the scope of this thesis, so instead we will focus on the proof of Ogg's conjecture in the key exceptional case $N = 13$, which is due to Mazur and Tate [19]. As we will see, this is the smallest N for which $X_1(N)$ has genus greater than 1, which makes determining $X_1(13)(\mathbf{Q})$ unamenable to direct computation (as is possible in the case $N = 11$).

We have tried to give complete proofs for all results in this thesis, providing references when we need to use certain facts without proof. We will assume the basic theory of algebraic geometry as in [13], as well as the classical theory of elliptic curves as in [26]. In Section 5, we will also need some notions from algebraic number theory and class field theory.

As for the content of this thesis, Section 2 describes the theory of relative elliptic curves, where the base scheme is no longer constrained to be the spectrum of a field. In this general setting, we will discuss the commutative group scheme structure of relative elliptic curves, as well as what we need to do in order to describe such curves with Weierstrass equations. In Section 3, we use the groundwork from Section 2 to build the moduli space $Y_1(N)$ as a scheme over $\mathbf{Z}[1/N]$, and then we discuss some of its geometric properties. In Section 4, we use analytic input to deduce more geometric properties of $Y_1(N)_{\mathbf{Q}}$ and its compactification $X_1(N)_{\mathbf{Q}}$. These two sections culminate in the genus formula (Proposition 4.2.12) for the

curve $X_1(N)_{\mathbf{Q}}$. Finally, Section 5 contains the core of this thesis, which is the aforementioned result of Mazur and Tate that no elliptic curve over $\mathbf{Q}$ has a rational point of exact order 13. Our exposition follows their paper [19], but we provide many extra details and explanations in order to make their arguments more accessible to a novice algebraic geometer.

In Appendix A, we have provided proofs of some useful results from algebraic geometry that are used in the main exposition, but would otherwise distract from the flow of the core arguments. The reader is advised to simply accept these results on faith during a first reading, and come back to their proofs later.

Acknowledgements

This thesis would not have been completed without the support and guidance of my advisor, Dr. Brian Conrad. I thank him for introducing me to the topics of this thesis (and to algebraic geometry more generally), for his patience while I struggled to learn the below material over the past year, and for his thorough and detailed comments on earlier drafts. I especially thank him for sharing his profound knowledge of mathematics with me through explanations that display both an intuitive understanding and the "morally correct" viewpoint. I have learned a lot from him.

I also thank my friend Wenqi Li for many helpful conversations regarding this thesis and for being a steadfast companion, in mathematical matters or otherwise. Finally, I thank my family, and especially my father, for all of the support they have given me over my four years at (and away from) Stanford.

2 Relative Elliptic Curves

In this section, we develop the theory of elliptic curves over locally Noetherian base schemes. We follow the discussion from Chapter 2 of [15], as well as from [6]. We will also freely invoke the theory of elliptic curves over a perfect (e.g. algebraically closed) field, as in [26].

Definition 2.0.1. Let S be a locally Noetherian scheme. A proper smooth S-scheme E is a *(relative) elliptic curve* over S if it has 1-dimensional geometrically connected fibers all of genus 1, as well as a given section $e : S \to E$.

Note that the section e is part of the data of the elliptic curve E. We might like to think of this relative situation as a family of elliptic curves $E_s/k(s)$, parameterized by $s \in S$.

Remark 2.0.2. The section e is a closed immersion, since if $f : E \to S$ is the structure map, then $\mathrm{id} = f \circ e$ is a closed immersion and f is separated.

2.1 The Group Law

In this section, we give the construction of a commutative group law on E. When S is the spectrum of a field k, the group law is given in the language of Weil divisors: given $P, Q \in E(k)$, $P+Q$ is the unique $R \in E(k)$ such that $P+Q \sim R+e$ as divisors on E. Equivalently, R is the unique k-point such that $\mathscr{I}_P^{-1} \otimes \mathscr{I}_Q^{-1} \cong \mathscr{I}_R^{-1} \otimes \mathscr{I}_e^{-1}$ as $\mathcal{O}_E$-modules, where $\mathscr{I}_x$ is the invertible sheaf corresponding to a point $x \in E(k)$.

On the other hand, in the relative case, we need to include input from the base S, since $\mathrm{Pic}(S)$ might not be trivial. This is done via the following theorem:

Theorem 2.1.1 ([15, 2.1.2, Abel's Theorem])**.** For any invertible sheaf $\mathcal{L}$ on E such that $\deg_{E_s}(\mathcal{L}_s) = 1$ for all $s \in S$, there is a unique $P \in E(S)$ and some $\mathscr{N} \in \mathrm{Pic}(S)$ such that $\mathcal{L} \cong \mathscr{I}_P^{-1} \otimes f^*(\mathscr{N})$. For such P, we write $\mathcal{L} \approx \mathscr{I}_P^{-1}$.

For an S-scheme T, we now use this theorem to build a commutative group structure on $E(T)$ functorial in T; that defines the desired group law on E by Yoneda's Lemma. Given $P, Q \in E(T) = E_T(T)$, the invertible sheaf $\mathscr{I}_P^{-1} \otimes \mathscr{I}_Q^{-1} \otimes \mathscr{I}_{e_T}$ on E_T has fiberwise degree $1+1-1=1$, so we may find a *unique* $R \in E_T(T)$ such that $\mathscr{I}_P^{-1} \otimes \mathscr{I}_Q^{-1} \otimes \mathscr{I}_{e_T} \approx \mathscr{I}_R^{-1}$. We define $P+Q$ to be R. For $S = \mathrm{Spec}(k)$ where k is a field, this is the classical procedure.

Clearly $P+Q = Q+P$. To check that the binary operation "+" is associative, we note that $(P+Q)+R$ and $P+(Q+R)$ are both described by the unique $R' \in E_T(T)$ such that

$$\mathscr{I}_P^{-1} \otimes \mathscr{I}_Q^{-1} \otimes \mathscr{I}_R^{-1} \otimes \mathscr{I}_{e_T}^2 \approx \mathscr{I}_{R'}^{-1}$$

where the left side has fiberwise degree $1+1+1-2=1$.

The section e_T is the identity in $E(T)$ since we trivially have $\mathscr{I}_P^{-1} \otimes \mathscr{I}_{e_T}^{-1} \otimes \mathscr{I}_{e_T} \approx \mathscr{I}_P^{-1}$, so $P + e_T = P$. To see that we have inverses, note that $\mathscr{I}_P \otimes \mathscr{I}_{e_T}^{-1} \otimes \mathscr{I}_{e_T}^{-1}$ has fiberwise degree 1, so there is a unique $P' \in E_T(T)$ such that $\mathscr{I}_P \otimes \mathscr{I}_{e_T}^{-1} \otimes \mathscr{I}_{e_T}^{-1} \approx \mathscr{I}_{P'}^{-1}$, in which case the above construction shows that $P + P' = e_T$. This gives a commutative group structure on $E(T)$. This is functorial in T, since the formation of the invertible ideal sheaves $\mathscr{I}_P$ is naturally compatible with base change.

We will also need the following uniqueness and naturality properties of the group law:

Theorem 2.1.2 ([15, 2.5.1])**.** If (E, e) is an elliptic curve over S, then the group law described above is the *unique* structure of an S-group scheme on E for which e is the identity section. Moreover, if (E', e') is another elliptic curve over S, then any S-morphism $f : E \to E'$ such that $f(e) = e'$ automatically respects the (uniquely determined) group laws on E and E' (i.e. f is a homomorphism of S-group schemes).

2.2 Relative Weierstrass Equations

From the theory of elliptic curves over a field, we know that such curves correspond to Weierstrass cubic equations with nonzero (invertible) discriminant and vice-versa.

We now prove that *affine-locally* on the base, any elliptic curve $E \to S$ is given by a smooth relative Weierstrass equation in $\mathbf{P}^2$ over the base. In other words:

Theorem 2.2.1. Affine-locally on $S = \mathrm{Spec}(A)$, E is given by (the projectivization of) a Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{2.2.1}$$

inside $\mathbf{P}^2_S$, where: $a_i \in A$, the above equation has discriminant in $A^\times$, and the closed immersion $E \hookrightarrow \mathbf{P}^2_S$ sends the identity section e to $[0,1,0] \in \mathbf{P}^2(S)$.

We first claim that we may reduce to the case where S is local. Indeed, if we have $s \in S$ and an $\mathcal{O}_{S,s}$-scheme isomorphism $E \otimes_S \mathcal{O}_{S,s} \cong C \otimes_S \mathcal{O}_{S,s}$, where C is the closed subscheme of $\mathbf{P}^2_S$ given by (2.2.1), then by "spreading out", this isomorphism arises from a U-isomorphism $E \otimes_S U \cong C \otimes_S U$, where $U \subseteq S$ is an affine open neighborhood of s (see [17, Ex. 3.2.5] for a more precise statement). The property of being a unit can also be checked on stalks, so the statement about the discriminant also reduces to the local case. Hence from now on, we may and do assume $S = \mathrm{Spec}(A)$ with A local Noetherian.

By [15, 1.2.2], we know that the ideal sheaf $\mathscr{I}_e$ of the closed subscheme $e(S)$ is invertible. So pick a small enough affine open neighborhood $U = \mathrm{Spec}(B)$ of the closed point of $e(S)$ such that $\mathscr{I}_e$ is trivial over U. Since S is the spectrum of a local ring, U must then contain all of $e(S)$. Hence $\mathscr{I}_e|_U = t\mathcal{O}_U$ for some non-zero-divisor $t \in B$, and $\mathscr{I}_e|_{E-e(S)} = \mathcal{O}_{E-e(S)}$.

We will now need some facts about the pushforwards of the powers $\mathscr{I}_e^{-n}$ for $n \geq 1$.

Proposition 2.2.2. For $n \geq 1$, $f_*(\mathscr{I}_e^{-n})$ is locally free of rank n and its formation commutes with base change.

Proof. For any $s \in S$, the $k(s)$-vector spaces $H^1(E_s, \mathscr{I}_{e(s)}^{-n})$ and $H^0(E_s, \mathscr{I}_{e(s)}^{n} \otimes \Omega^1_{E_s/k(s)})$ have the same dimension by Serre duality. But since we are in the genus-1 situation on fibers, we have $\deg(\mathscr{I}_{e(s)}^{n} \otimes \Omega^1_{E_s/k(s)}) = -n + (2 \cdot 1 - 2) < 0$, implying by Riemann-Roch that $H^0(E_s, \mathscr{I}_{e(s)}^{n} \otimes \Omega^1_{E_s/k(s)}) = 0$. Hence $H^1(E_s, \mathscr{I}_{e(s)}^{-n}) = 0$, so the cohomology and base change theorem [10, 7.7.5] implies $R^1f_*(\mathscr{I}_e^{-n})(s) = 0$ since the fibral base change map

$$\varphi^1_s : R^1f_*(\mathscr{I}_e^{-n})(s) \to H^1(E_s, \mathscr{I}_{e(s)}^{-n})$$

is trivially surjective and therefore an isomorphism (note that $\mathscr{I}_e^{-n}$ is flat over S since it is locally free over E and $f : E \to S$ is smooth). Hence the fibral base change map φ^0_s in degree 0 is also surjective and thus an isomorphism, so $f_*(\mathscr{I}_e^{-n})$ is locally free with formation commuting with base change since the fibral base change map in degree -1 is trivially surjective.

To determine the rank, we may pass to (geometric) fibers. Our task is to compute $h^0(E, \mathcal{O}_E(ne))$ for an elliptic curve (E, e) over a field k, where $\mathcal{O}_E(ne) = \mathscr{I}_e^{-n}$. But $h^1(E, \mathcal{O}_E(ne)) = 0$ by Serre duality since $\deg(\Omega^1_{E/k}(-ne)) = (2 \cdot 1 - 2) - n < 0$, so by Riemann-Roch, we have $h^0(E, \mathcal{O}_E(ne)) = n$. □

Since $f_*(\mathscr{I}_e^{-n})$ is a locally free sheaf of finite rank over the *local ring* $S = \mathrm{Spec}(A)$, it must in fact be *free* of rank n.

Proposition 2.2.3. The natural map $\mathcal{O}_S \to f_*(\mathscr{I}_e^{-1})$ is an isomorphism.

Proof. On fibers, the map $\mathcal{O}_S \to f_*(\mathscr{I}_e^{-1})$ becomes $k(s) \to H^0(E_s, \mathcal{O}_{E_s}(e(s)))$, and we saw in the proof of Proposition 2.2.2 that the right side has dimension 1 over $k(s)$. The map is clearly injective (interpreting it in the context of rational functions on an elliptic curve over a field), so is an isomorphism. To prove that $\mathcal{O}_S \to f_*(\mathscr{I}_e^{-1})$ is an isomorphism, it suffices to check that the stalk map $\mathcal{O}_{S,s} \to (f_*\mathscr{I}_e^{-1})_s$ is an isomorphism for any $s \in S$. This is a map of *finite free* $\mathcal{O}_{S,s}$-modules (of rank 1) that reduces to the above isomorphism after passing to the residue field $k(s)$, so the stalk map is a surjection, hence an isomorphism. □

This shows that $f_*(\mathscr{I}_e^{-1})$ has an $\mathcal{O}_S$-basis $\{1\}$. Now, for each $n \geq 1$, consider the exact sequence

$$0 \to \mathscr{I}_e^{-n} \to \mathscr{I}_e^{-n-1} \to \mathscr{I}_e^{-n-1}/\mathscr{I}_e^{-n} \to 0.$$

This stays exact upon applying the pushforward f_*, since in the proof of Proposition 2.2.2 we saw that $R^1 f_*(\mathscr{I}_e^{-n})$ vanishes. Moreover, since e is a section to f and $\mathscr{I}_e^{-n-1}/\mathscr{I}_e^{-n}$ (being killed by $\mathscr{I}_e$) is supported on $e(S) \subseteq E$, we can identify

$$f_*(\mathscr{I}_e^{-n-1}/\mathscr{I}_e^{-n}) \cong f_* e_* e^*(\mathscr{I}_e^{-n-1}) = e^*(\mathscr{I}_e^{-n-1})$$

with $\mathscr{I}_e^{-n-1}/\mathscr{I}_e^{-n}$, where the first $\mathscr{I}_e^{-n-1}/\mathscr{I}_e^{-n}$ inside the pushforward f_* is considered as a sheaf of $\mathcal{O}_E$-modules and the second standalone $\mathscr{I}_e^{-n-1}/\mathscr{I}_e^{-n}$ is considered as a sheaf of $\mathcal{O}_S$-modules. So after applying f_*, we have a short exact sequence

$$0 \to f_*(\mathscr{I}_e^{-n}) \to f_*(\mathscr{I}_e^{-n-1}) \to \mathscr{I}_e^{-n-1}/\mathscr{I}_e^{-n} \to 0 \tag{2.2.2}$$

of $\mathcal{O}_S$-modules. The first two terms are free of ranks n and $n+1$, and the third term is free of rank 1, since it isomorphic to $\mathcal{O}_S$ via multiplication by t^{n+1} (recall that the non-zero-divisor t is chosen so that $\mathscr{I}_e = t\mathcal{O}_U$ on an affine open neighborhood $U = \mathrm{Spec}(B)$ of $e(S)$). Write θ_n for the surjective composite map

$$f_*(\mathscr{I}_e^{-n-1}) \to \mathscr{I}_e^{-n-1}/\mathscr{I}_e^{-n} \xrightarrow[\sim]{\cdot t^{n+1}} \mathcal{O}_S.$$

Let's look at the global sections of the sheaves in (2.2.2). Note that since S is affine, the global sections functor is exact. This means that, beginning with $n = 1$, we can write:

- $f_*(\mathscr{I}_e^{-1})$ is free on $\{1\}$.
- $f_*(\mathscr{I}_e^{-2})$ is free on global sections $\{1, x\}$, where $\theta_1(x) = 1$.
- $f_*(\mathscr{I}_e^{-3})$ is free on global sections $\{1, x, y\}$, where $\theta_2(y) = 1$.

The idea is that on U around $e(S)$, x has a t-adic expansion t^{-2} + (higher order terms) in terms of t, and similarly y has a t-adic expansion t^{-3} + (higher order terms), where B has t-adic completion $A[\![t]\!]$. Continuing on, we see that

- $f_*(\mathscr{I}_e^{-4})$ is free on $\{1, x, y, x^2\}$, since $\theta_3(x^2) = 1$.
- $f_*(\mathscr{I}_e^{-5})$ is free on $\{1, x, y, x^2, xy\}$, since $\theta_4(xy) = 1$.
- $f_*(\mathscr{I}_e^{-6})$ is free on $\{1, x, y, x^2, xy, x^3\}$ and on $\{1, x, y, x^2, xy, y^2\}$, since $\theta_5(x^3)$ and $\theta_5(y^2)$ both equal 1.

We conclude that $\theta_5(x^3 - y^2) = 0$, which implies that $x^3 - y^2$ is a global section of $f_*(\mathscr{I}_e^{-5})$. Using the above basis of $f_*(\mathscr{I}_e^{-5})$, there is a unique equation

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

with the $a_i \in A$, as in (2.2.1).

Recall that on the affine open U around $e(S)$, we have $\mathscr{I}_e^{-3}|_U = t^{-3}\mathcal{O}_U$, and away from $e(S)$, we have $\mathscr{I}_e^{-3}|_{E-e(S)} = \mathcal{O}_{E-e(S)}$. Then by looking at the "t-adic expansions" of x and y (i.e. the maps θ_n defined earlier), we see that $t^3x|_U \in t\mathcal{O}_U$ and $t^3y|_U \in 1 + t\mathcal{O}(U)$. By shrinking U if necessary, we can arrange that $t^3y|_U \in \mathcal{O}(U)^\times$. Indeed, $t^3y|_U$ is a unit in the residue field at the unique closed point $e(s)$ of $e(S) \cong \mathrm{Spec}(B/tB)$ (its reduction mod t is already 1), so it is a unit on some affine open around $e(s)$ (necessarily containing all of $e(S)$), which we can take to be U. Hence y generates $\mathscr{I}_e^{-3}|_U$, and clearly 1 generates $\mathscr{I}_e^{-3}|_{E-e(S)}$, so by the universal property of projective space, we can use the invertible sheaf $\mathscr{I}_e^{-3}$ and its generating global sections $\{x, y, 1\}$ to define an S-map $\psi : E \to \mathbf{P}^2_S$, given on $E - e(S)$ by $(x, y) \in \mathcal{O}_E(E - e(s))^2$.

By the construction of ψ, the global section

$$W(X, Y, Z) := Y^2Z + a_1XYZ + a_3YZ^2 - (X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3)$$

of $\mathcal{O}(3)$ on $\mathbf{P}^2_S$ pulls back to $y^2 + a_1xy + a_3y - (x^3 + a_2x^2 + a_4x + a_6) = 0$ in $\mathscr{I}_e^{-9}(E)$, so the natural map of graded rings

$$A[X, Y, Z] \twoheadrightarrow \bigoplus_{n\geq 0} \Gamma(E, (\mathscr{I}_e^{-3})^{\otimes n})$$

has W in its kernel. In particular, ψ factors through the closed subscheme $C \subseteq \mathbf{P}^2_S$ given by the projectivization of the Weierstrass equation (2.2.1).

We now show that $\psi : E \to C$ is an isomorphism. First, E is flat over S because it is smooth, and C is flat over S because the Weierstrass polynomial is monic in both x and y. Then via the "fibral isomorphism criterion" [12, IV.17.9.5], to show ψ is an isomorphism, it suffices to check this for the maps $\psi_{\bar{s}} : E_{\bar{s}} \to C_{\bar{s}}$ between geometric fibers over each

geometric point $\overline{s}$ of S. Hence, now $S = \mathrm{Spec}(k)$ for an algebraically closed field k. Since $\mathscr{I}_e^{-3} = \mathcal{O}_E(3e)$ has $\{1, x, y\}$ a basis of its global sections, by [13, IV.3.1, IV.3.2] we conclude that ψ is a closed immersion into C (more precisely, a closed immersion $E \to \mathbf{P}^2$ whose image must be contained in C). But a closed immersion between integral proper curves must be an isomorphism, so ψ is an isomorphism.

Note that the discriminant of our Weierstrass equation must be a unit, since this can be checked on fibers, where we use the theory over an algebraically closed field again [26, III.1.4(a)].

To complete the proof of Theorem 2.2.1, it remains to show that ψ sends $e(S)$ to $[0, 1, 0]$ as S-points. We saw earlier that $t^3 y|_U$ is a *unit* in $\mathcal{O}(U)$, so the restrictions $x|_U \in \mathscr{I}_e^{-2}|_U$ and $1|_U \in \mathcal{O}(U)$ are multiples of $y|_U$ by elements of $\mathscr{I}_e(U) = t\mathcal{O}(U)$. Thus, $x|_U = b_0 y|_U$ and $1|_U = b_2 y|_U$ for $b_0, b_2 \in \mathscr{I}_e(U)$. Then $\psi(U) \in D_+(Y) \subseteq \mathbf{P}^2_S$ with $\psi : U \to D_+(Y) \cong \mathbf{A}^2_S$ given by $(b_0, b_1) \in B^2$. By design, b_0 and b_2 in $\mathscr{I}_e(U) = tB$ have vanishing image in the coordinate ring of $e(S) \cong \mathrm{Spec}(B/tB)$. Hence the isomorphism ψ carries $e(S)$ to $[0, 1, 0]$ as S-points of $\mathbf{P}^2$.

Remark 2.2.4. The closed subscheme $E \subseteq \mathbf{P}^2_R$ given by any smooth Weierstrass equation $\mathcal{W}$ as in (2.2.1) always has $\{1, x, y\}$ in $\Gamma(W, \mathscr{I}_e^{-3})$ as generators of the sheaf $\mathscr{I}_e^{-3}$, where $\{1, x\}$ forms a basis of $f_*(\mathscr{I}_e^{-2})$, $\{1, x, y\}$ forms a basis of $f_*(\mathscr{I}_e^{-3})$, and $t = y/x \in \mathscr{I}_e(U)$ is a basis of $\mathscr{I}_e|_U$ for an open U around $e(S)$. This gives a converse to Theorem 2.2.1, up to keeping track of the unit leading coefficients of the t-adic expansions of x and y.

Example 2.2.5. To show that the statement of Theorem 2.2.1 really is only Zariski-local on the base in general, we give an example of a relative elliptic curve with no smooth global Weierstrass model in $\mathbf{P}^2$ over the base. To do this, we need the following theorem:

Theorem 2.2.6 ([28, 1.7])**.** Let E be an elliptic curve over an imaginary quadratic number field K. If E has a global minimal Weierstrass model then E cannot have everywhere good reduction.

In other words, if E did have everywhere good reduction, then it cannot be expressed as the K-fiber of a smooth global Weierstrass model over $\mathcal{O}_K$ (this would be a global minimal Weierstrass model, since its discriminant Δ_E would be a unit). The discussion in [4, Section 4] gives an example of an elliptic curve E over the imaginary quadratic field $\mathbf{Q}(\sqrt{-259})$ with everywhere good reduction. Explicitly, E is given by the Weierstrass equation

$$y^2 = x^3 - 3A(A^3 - 1728)u^2 x - 2(A^3 - 1728)^2 u^3,$$

where $A = 16$ and $u = 222 + 36\sqrt{-259}$.

In fact, by [4, 1.2], as we vary over all imaginary quadratic fields K, there are infinitely many admitting an elliptic curve E/K with everywhere good reduction.

2.3 Multiplication by N

To complete our general discussion about relative elliptic curves, we need a fact concerning the multiplication-by-N map $[N]$, where N is a nonzero integer. By commutativity of the group law, for an elliptic curve $E \to S$, $[N] : E \to E$ is an S-homomorphism. We want to prove the following:

Proposition 2.3.1. The map $[N] : E \to E$ is finite locally free of rank N^2. If N is invertible on the base S, then $[N]$ is even étale.

The first part is the same as saying $[N]$ is finite flat, since S is locally Noetherian.

Proof. First, E is proper over S, so the S-map $[N]$ is proper. We next wish to show that $[N]$ is quasi-finite, so then it is finite. It suffices for this to be checked on fibers over points $s \in S$, and even geometric fibers. But from the classical theory [26, III.6.2], $[N]_{\overline{s}} : E_{\overline{s}} \to E_{\overline{s}}$ has finite fibers.

We now want to prove that $[N]$ is flat. Since E is flat over S, we can use the "fibral flatness criterion" [11, 11.3.11] to reduce to verifying the flatness between fibers, and even geometric fibers, over S. Since $[N]_{\overline{s}}$ is a nonconstant map between smooth connected curves over an algebraically closed field, it must be surjective, so it induces injections of stalks. But the stalks of $E_{\overline{s}}$ are all regular local rings of dimension at most 1, hence fields or discrete valuation rings. Since injections $R_1 \hookrightarrow R_2$ of discrete valuation rings are flat (as R_2 is torsion-free over R_1), we have the desired flatness of $[N]_{\overline{s}}$. To conclude that the rank is N^2, we can just look at the rank on the generic fibers over geometric points of S, which is N^2 by the classical theory.

It remains to prove that if N is invertible on the base, then $[N]$ is étale. We have a "fibral étaleness criterion" [12, 17.8.2] in a similar manner as above, so it suffices to check étaleness of each $[N]_{\overline{s}}$, where N is invertible in $k(\overline{s})$. Thus, now $S = \mathrm{Spec}(k)$ for an algebraically closed field k with $\mathrm{char}(k) \nmid N$. We claim that we only need to check étaleness at the identity $e \in E(k)$. Indeed, for any point $p \in E(k)$, the diagram

$$\begin{array}{ccc} E & \xrightarrow{-p} & E \\ \downarrow{\scriptstyle [N]} & & \downarrow{\scriptstyle [N]} \\ E & \xrightarrow{-Np} & E \end{array}$$

commutes, where the two horizontal arrows are isomorphisms (translation by a point). Thus, the left vertical arrow is étale at p if the right vertical arrow is étale at e. Since k is algebraically closed, and the étale locus is open, étaleness at $E(k)$ is therefore sufficient.

Now, because we are working with smooth schemes over a field, and $[N](e) = e$, it suffices to show that the tangent map $d[N](e) : T_{E/k,e} \to T_{E/k,e}$ is injective [17, 4.3.27]. By Lemma A.1, this map is simply multiplication by the integer N on tangent vectors. But N is invertible in k by assumption, so such a map of k-vector spaces is injective. □

Note that Proposition 2.3.1 implies that the S-group scheme $E[N] \coloneqq \ker([N]) \cong S \times_E E$ (the fiber product with $e : S \to E$ and $[N] : E \to E$) is finite locally free over S, and if N is invertible on S, $E[N]$ is even finite étale over S.

3 Algebraic Theory of Modular Curves

In this section, we work out parts of the theory of modular curves via algebraic approaches. For the rest of this section, $N \geq 4$ is an integer.

3.1 Some Definitions

We first need to define what we mean by an "exact order N point" on an elliptic curve E over a $\mathbf{Z}[1/N]$-scheme S. We adopt the definition and equivalent conditions of [15, Lemma 1.4.4].

Definition 3.1.1. Suppose N is invertible on S. We say $P \in E(S)$ has *exact order* N if it is N-torsion (i.e. $NP = e$ in $E(S)$) and the induced point $P_{\overline{s}} \in E(\overline{s})$ has exact order N (in the classical sense) for every geometric point $\overline{s}$ of S.

Beware that this is the "wrong" definition if N is not invertible on S. With Definition 3.1.1, we can make the following definition:

Definition 3.1.2. The functor F_N from the category of $\mathbf{Z}[1/N]$-schemes to the category of sets is:

$$F_N(S) = \{(E, P) : E/S \text{ is an elliptic curve, } P \in E(S) \text{ of exact order } N\}/\text{isomorphism}.$$

We will prove that F_N is representable, with universal object that is an elliptic curve in "Tate normal form" (defined in Definition 3.1.3) equipped with a point $(0, 0)$ of exact order N. Even if N is not invertible on S, this is still true; we impose invertibility to ensure good behavior of the representing object $Y_1(N)$. For instance, we'll need invertibility to ensure that it is smooth over $\mathbf{Z}[1/N]$ (see Proposition 3.3.1), along with many other important properties.

The Tate normal form of an elliptic curve will help us build the modular curves $Y_1(N)$.

Definition 3.1.3. A *Tate normal form* for an elliptic curve $E \to S = \mathrm{Spec}(R)$ is a (global) smooth Weierstrass model of the form

$$y^2 + axy + by = x^3 + bx^2 \tag{3.1.1}$$

with $a, b \in R$.

Note that the equation (3.1.1) has discriminant

$$\Delta(a,b) = b^3(-a^4 + a^3 - 8a^2b + 36ab - 16b^2 - 27b), \tag{3.1.2}$$

so b must be a unit (since one can check this on fibers). Moreover, $(0,0) = [0,0,1]$ is a section on the curve (3.1.1) that is everywhere disjoint from the identity $[0,1,0]$.

3.2 Tate Normal Form and $Y_1(N)$

We now prove some facts concerning the Tate normal form.

Lemma 3.2.1. The Tate normal form admits no non-trivial change of Weierstrass coordinates $(x,y) \mapsto (x',y')$ preserving $(0,0)$.

Proof. We adapt the proof of [26, III.3.1(b)]. By Remark 2.2.4, we see that $\{1,x\}$ and $\{1,x'\}$ both form bases of $f_*(\mathscr{I}_e^{-2})$, and $\{1,x,y\}$ and $\{1,x',y'\}$ both form bases of $f_*(\mathscr{I}_e^{-3})$. Since $S = \mathrm{Spec}(R)$, there are elements $u_1, u_2 \in R$ and $r, s_2, t \in R$ such that $x = u_1x' + r$ and $y = u_2y' + s_2x' + t$. Moreover, u_1 is a unit because $\mathcal{O}_S = f_*(\mathscr{I}_e^{-1})$ (Proposition 2.2.3) and $f_*(\mathscr{I}_e^{-2})/f_*(\mathscr{I}_e^{-1}) \cong \mathscr{I}_e^{-2}/\mathscr{I}_e^{-1}$ from (2.2.2) has both $\{x\}$ and $\{x'\}$ as an R-basis. Similarly, u_2 is a unit.

Upon substituting the expressions $x = u_1x' + r$ and $y = u_2y' + s_2x' + t$ into (3.1.1), we get an equation

$$(u_2y' + s_2x' + t)^2 + a(u_1x' + r)(u_2y' + s_2x' + t) + b(u_2y' + s_2x' + t) = (u_1x' + r)^3 + b(u_1x' + r)^2, \tag{3.2.1}$$

and since $E \subseteq \mathbf{P}^2_S$ is defined by a Weierstrass equation $\mathcal{W}'$ in terms of x' and y', we must have $u_1^3 = u_2^2$. Indeed, otherwise we can subtract $u_1^3\mathcal{W}'$ from (3.2.1) to get a nontrivial R-linear combination of $\{1, x', y', (x')^2, x'y', (y')^2\}$ that equals 0 on E, contradicting the fact that this set forms a basis for $f_*(\mathscr{I}_e^{-6})$.

Define $u \coloneqq u_2/u_1$ and $s \coloneqq s_2/u^2$, so $u^2 = u_1$ and $u^3 = u_2$. Hence $x = u^2x' + r$ and $y = u^3y' + su^2x' + t$. Now, since $(0,0)$ is preserved by the coordinate transformation, r and t must be 0. Then upon substituting u^2x' for x and $u^3y' + su^2x'$ for y in (3.1.1), we rearrange to get

$$(y')^2 + \frac{a+2s}{u}x'y' + \frac{b}{u^3}y' = (x')^3 + \frac{b - sa - s^2}{u^2}(x')^2 - \frac{sb}{u^4}x'.$$

Since the Tate normal form in terms of x' and y' is such that $a_4 = 0$ (in the notation of (2.2.1)), we must have $sb/u^4 = 0$. But b and u are both units, so $s = 0$. Also $a_2 = a_3$ for Tate normal forms, so $b/u^3 = b/u^2$, giving $u = 1$. Hence $x = x'$ and $y = y'$. □

Given this uniqueness, it is natural to try to describe when a relative elliptic curve actually does have a Tate normal form. It turns out that in the case we ultimately care the most about, this always happens:

Proposition 3.2.2. If E is an elliptic curve over a ring R, and $P \in E(R)$ is a point which is not 2 or 3-torsion on any fiber, then E has a unique Tate normal form with $P = (0, 0)$.

Proof. From Lemma 3.2.1, we have uniqueness. Moreover, it suffices to prove this proposition when R is local. Indeed, by a spreading out argument (as at the start of the proof of Theorem 2.2.1), for every $s \in \mathrm{Spec}(R)$, we would then have a Tate normal form of $E \times_R U_s$ over some open neighborhood U_s of s, and these agree on overlaps by uniqueness (again Lemma 3.2.1), so they globalize over S. So we may and do assume that R is local. The work in Section 2.2 shows that E has a Weierstrass model as in (2.2.1), and we want to transform it into Tate normal form.

By assumption, P is not 2 or 3-torsion on any fiber, so it is not the point at infinity in any fiber. In particular, if we write P in homogeneous coordinates $[a', b', c']$ in $\mathbf{P}^2(R)$ (as we may since R is local), c' must be a unit as $[a', b', c']$ lands in $D_+(Z)$ in every fiber. Hence we can scale by $(c')^{-1}$ to write P in the form $[a, b, 1]$. Changing variables via $(x, y) \mapsto (x - a, y - b)$ in our Weierstrass equation (which preserves $[0, 1, 0] \in \mathbf{P}^2(R)$), we move P to $(0, 0)$ and so the new Weierstrass equation has the form

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

In particular we have $a_6 = 0$ in R.

We now claim a_3 is a unit. If not, it is 0 in some geometric fiber. Working in the case over an algebraically closed field, we have $y^2+a_1xy = x^3+a_2x^2+a_4x$, and using the tangent-chord addition, we see that the line $x = 0$ intersects E at $O := [0, 1, 0]$ and at P with multiplicity 2 (note that $k[x, y]/(x, y^2+a_1xy-(x^3+a_2x^2+a_4x)) \cong k[y]/(y^2)$). In other words, $P = -P$ in that fiber, contradicting the assumption on P. Hence we may make the change of variables $y \mapsto y + (a_4/a_3)x$ over R preserving $P = (0, 0)$, so now

$$\left(y + \frac{a_4}{a_3}x\right)^2 + a_1x\left(y + \frac{a_4}{a_3}x\right) + a_3\left(y + \frac{a_4}{a_3}x\right) = x^3 + a_2x^2 + a_4x.$$

The a_4x's cancel, so (abusing notation by reusing the a_i notation) we are left with a new equation of the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2.$$

This new a_3 is equal to the old a_3, hence is a unit (or repeat the same argument for the new a_3).

We next claim a_2 is a unit. If not, it is 0 in some geometric fiber, so with a Weierstrass equation $y^2 + a_1xy + a_3y = x^3$ over an algebraically closed field, the tangent line $y = 0$ at P meets E with order 3 (note that $k[x, y]/(y, y^2 + a_1xy + a_3y - x^3) \cong k[x]/(x^3)$). Hence $P = -2P$ in that fiber, but this again contradicts the assumption on P, so a_2 is a unit.

We may make the change of variables $y \mapsto (a_2/a_3)^3y$ and $x \mapsto (a_2/a_3)^2x$, so

$$\left(\frac{a_2}{a_3}\right)^6 y^2 + a_1\left(\frac{a_2}{a_3}\right)^5 xy + a_3\left(\frac{a_2}{a_3}\right)^3 y = \left(\frac{a_2}{a_3}\right)^6 x^3 + a_2\left(\frac{a_2}{a_3}\right)^2 x$$

and hence our new Weierstrass equation looks like

$$y^2 + axy + by = x^3 + bx^2,$$

where $b = a_3(a_2/a_3)^{-3} = a_2(a_2/a_3)^{-4}$ is a unit. This is a Tate normal form. □

The importance of the Tate normal form is that it enables us to construct a representing object for F_N, along with its universal structure (which will be built as an elliptic curve in Tate normal form). In other words, the result is:

Theorem 3.2.3. Let $N \geq 4$ be an integer. Then the functor F_N is represented by an affine $\mathbf{Z}[1/N]$-scheme of finite type $Y_1(N)$, with universal object that is an elliptic curve in Tate normal form.

Proof. Consider the elliptic curve E given by the Tate normal form $y^2 + axy + by = x^3 + bx^2$ over the ring $R \coloneqq \mathbf{Z}[1/N, a, b][1/\Delta]$, where Δ is as in (3.1.2). Notice that R is a UFD, as it is a localization of one.

Now consider $NP \in \mathbf{P}^2_R(R)$, where $P \coloneqq (0,0)$. We have $\mathrm{Pic}(R) = 1$ as R is a UFD, so by the universal property of $\mathbf{P}^2_R$, everything in $\mathbf{P}^2_R(R)$ is represented by a triple (u, v, w) up to $R^\times$-scaling, with $(u, v, w) = (1)$. Thus, we have $NP = (f(a,b), g(a,b), h(a,b))$ for $f, g, h \in R$ generating 1. Then the N-torsion requirement $NP = (0, 1, 0)$ (as sections) over an R-algebra R' says exactly that f and h vanish in R', since the natural map

$$\{(a_0, \ldots, a_n) \in (R')^{n+1} | a_j\text{'s generate unit ideal in } R'\}/(R')^\times \to \mathbf{P}^2_R(R')$$

is *injective* (being the subfunctor of points with the trivial line bundle, in regards to the universal property of $\mathbf{P}^2_R$).

Hence, over $R/(f,h)$, we get a *universal* elliptic curve in Tate normal form (namely, $y^2 + axy + by = x^3 + bx^2$) where $P = (0,0)$ is N-torsion. As we vary through proper positive divisors d of N, over R we can likewise write $d(0,0,1) = (f_d, g_d, h_d)$ for some $f_d, g_d, h_d \in R$ that generate 1. To make P "exact order N", we want to avoid P being d-torsion in any fiber, so h_d has to be a unit at all points of the base. Thus, over the localization $R_N \coloneqq (R/(f,h))[1/h_d : d|N, 1 \leq d \neq N]$, we get an elliptic curve in Tate normal form in which P has exact order N, and by Proposition 3.2.2, this is the universal such curve. Hence $Y_1(N) \coloneqq \mathrm{Spec}(R_N)$ represents the functor F_N, over which the elliptic curve $y^2 + axy + by = x^3 + bx^2$ with $P = (0,0)$ is the universal structure. □

3.3 Properties of $Y_1(N)$

Having built the $\mathbf{Z}[1/N]$-scheme $Y_1(N)$, we would like to discuss some of its properties. In particular, we want to show that:

1. $Y_1(N)$ is smooth over $\mathbf{Z}[1/N]$;

2. the fibers of $Y_1(N) \to \mathrm{Spec}(\mathbf{Z}[1/N])$ are of pure dimension 1;

3. the generic fiber $Y_1(N)_{\mathbf{Q}}$ is geometrically connected.

Later, we will "compactify" $Y_1(N)$ to a relative curve over $\mathbf{Z}[1/N]$: a smooth proper scheme $X_1(N)$ of relative dimension 1 with geometrically connected fibers.

Proposition 3.3.1. The scheme $Y_1(N)$ is smooth over $\mathbf{Z}[1/N]$.

Proof. Clearly $Y_1(N)$ is of finite type over $\mathbf{Z}[1/N]$. We shall use the "functorial criterion for smoothness" as in [3, 2.2.6]. In particular, it suffices to prove that for any Artin local ring A over $\mathbf{Z}[1/N]$ with an ideal I such that $I^2 = 0$ and $A_0 := A/I$, the canonical map $Y_1(N)(A) \to Y_1(N)(A_0)$ is surjective. Because of the functor that $Y_1(N)$ represents, we pick an elliptic curve (E_0, P_0) over A_0 with P_0 of exact order N, and we want to lift this to such a pair (E, P) over A. Moreover, because A is *local*, E_0 must have a global Weierstrass form (even a Tate normal form, by Proposition 3.2.2), so we can lift its coefficients to define a curve E over A. Notice that the discriminant of E is a unit, because A is local and it is a unit in the quotient A_0. Hence E really is an elliptic curve over A.

It remains to lift P_0 to a point P of exact order N on E. Since we are over $\mathbf{Z}[1/N]$, $E[N]$ is étale by 2.3.1, so $E[N](A) \to E[N](A_0)$ is bijective by [3, 2.2.6]. Moreover, $E[N](A_0) = E_0[N](A_0)$. Hence $P_0 \in E_0[N](A_0)$ uniquely lifts to some $P \in E[N](A)$, which is N-torsion and is exact order N on fibers by design (A and A_0 are both artin local with the same residue field). □

Proposition 3.3.2. The fibers of $Y_1(N) \to \mathrm{Spec}(\mathbf{Z}[1/N])$ are nonempty of pure dimension 1.

From the classical theory, for any algebraically closed field k with $N \in k^\times$, any elliptic curve over k has a point of exact order N. Thus, $Y_1(N)(k) \neq \emptyset$. This proves that the fibers are nonempty.

For the second part of the statement, it is equivalent to check that for $y \in Y_1(N)(k)$, where k is any algebraically closed field of characteristic not dividing N, the tangent space to $Y_1(N)_k$ at y is 1-dimensional over k. For this computation, let's write $Y := Y_1(N)_k$, and $k[\epsilon] := k[x]/(x^2)$ for the dual numbers over k. Recall that the tangent space at $y \in Y(k)$ is the fiber of $Y(k[\epsilon]) \to Y(k)$ above y as a set. We now need to describe a vector space structure on it corresponding to the usual structure on $T_y(Y) = (\mathfrak{m}_y/\mathfrak{m}_y^2)^*$. Any k-map $f : \mathrm{Spec}(k[\epsilon]) \to Y$ with image the k-point y induces a k-linear map $F : \mathfrak{m}_y/\mathfrak{m}_y^2 \to (\epsilon) \cong k$. Conversely, consider the commutative diagram

$$\begin{array}{ccc} k & \xrightarrow{h} & \mathcal{O}_{Y,y} \\ \downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle \pi} \\ k & \xleftarrow[\varphi]{\sim} & k(y) = \mathcal{O}_{Y,y}/\mathfrak{m}_y \end{array} \tag{3.3.1}$$

where h is the structure map on local rings induced by $Y \to \mathrm{Spec}(k)$, φ is the unique k-algebra map $k(y) \xrightarrow{\sim} k$, and $\pi \circ h$ is inverse to φ. Then we have a composite k-algebra map

$$\mathcal{O}_{Y,y} \to \mathcal{O}_{Y,y}/\mathfrak{m}_y^2 \cong k \oplus \mathfrak{m}_y/\mathfrak{m}_y^2$$

given by

$$r \mapsto (\varphi(\overline{r}), r - h \circ \varphi(\overline{r})) =: (r_a, r_b). \tag{3.3.2}$$

So given $F \in (\mathfrak{m}_y/\mathfrak{m}_y^2)^*$, we define $f : \mathrm{Spec}(k[\epsilon]) \to Y$ in the fiber above $y \in Y(k)$ via $\mathcal{O}_{Y,y} \to k[\epsilon]$, $r \mapsto r \bmod \mathfrak{m}_y^2 \mapsto r_a + F(r_b)\epsilon$. This is a k-algebra map because (3.3.2) is a k-algebra map and $\mathfrak{m}_y/\mathfrak{m}_y^2$ is a square-zero ideal. Adding two maps $F, G \in (\mathfrak{m}_y/\mathfrak{m}_y^2)^*$ corresponds to $r \mapsto r_a + (F+G)(r_b)\epsilon$ on the level of $k[\epsilon]$-points, and similarly for k-scalar multiplication.

It is easy to check that $r \mapsto F(r_b)$ is a k-derivation. Conversely, given a k-derivation $d : \mathcal{O}_{Y,y} \to k$ over $y^* := \varphi \circ \pi : \mathcal{O}_{Y,y} \to k$, we can check that $r \mapsto \varphi(\overline{r}) + d(r)\epsilon$ is a k-algebra map $\mathcal{O}_{Y,y} \to k[\epsilon]$ lifting y^*. This defines inverse k-linear bijections between $\mathrm{Der}_k(\mathcal{O}_{Y,y}, k)$ and $T_y(Y)$, so the following identifications give us the desired vector space structure on the set-theoretic fiber of $Y(k[\epsilon]) \to Y(k)$ above y:

$$\mathrm{Der}_k(\mathcal{O}_{Y,y}, k) \Leftrightarrow T_y(Y) \Leftrightarrow \{k\text{-algebra maps } \mathcal{O}_{Y,y} \to k[\epsilon]\} \Leftrightarrow \text{fiber of } Y(k[\epsilon]) \to Y(k) \text{ above } y.$$

Let's try to describe this fiber more concretely. A point $y \in Y(k)$ has a corresponding pair (E_0, P_0) over k (so P_0 is exact order N on the elliptic curve E_0). Hence the fiber is the set of isomorphism classes of (E, P) over $k[\epsilon]$ lifting (E_0, P_0).

Recall that once we lift E_0 to some E, there is a unique choice of P lifting P_0 by étaleness of $E[N]$ (see the proof of Proposition 3.3.1). Moreover, if $e, \widetilde{e} \in E(k[\epsilon])$ lift $e_0 \in E(k)$, then in the group law of (E, e), the translation by $\widetilde{e}$ on E is an isomorphism $(E, e) \cong (E, \widetilde{e})$ of pointed curves lifting the identity on E_0. Note that this translation respects the group laws on (E, e) and $(E, \widetilde{e})$ because of Theorem 2.1.2. Thus, we're just trying to describe isomorphism classes of liftings of bare curves E_0 to E. For this, we will need to use some basic tools from deformation theory:

Definition 3.3.3. If X is a scheme over a field k and $k[\epsilon]$ is the ring of dual numbers $k[x]/(x^2)$, we say that a *deformation* of X (over $k[\epsilon]$) is a flat scheme X' over $k[\epsilon]$, together with a closed immersion $i : X \hookrightarrow X'$ such that $i \otimes_{k[\epsilon]} k : X \to X' \otimes_{k[\epsilon]} k$ is an isomorphism. The *trivial deformation* of X is $X \otimes_k k[\epsilon]$, and the notion of *isomorphism between deformations* of X is the evident one.

Lemma 3.3.4 ([14, 5.3])**.** Let X be a smooth variety over a field k. Then the set of isomorphism classes of deformations of X over $k[\epsilon]$ is in bijective correspondence with $H^1(X, \mathcal{T}_{X/k})$. Here, $\mathcal{T}_{X/k} := \mathscr{H}om_X(\Omega^1_{X/k}, \mathcal{O}_X) = (\Omega^1_{X/k})^\vee$ is the tangent sheaf of X over k.

Proof. Let X' be a deformation of X, and let $\mathfrak{U} \coloneqq \{U_i\}$ be an affine open covering of X. Over each U_i, deformations to $k[\epsilon]$ are isomorphic to the trivial deformation by Lemma A.2, so choose isomorphisms $\varphi_i : U_i \otimes_k k[\epsilon] \xrightarrow{\sim} U_i'$ as deformations, where U_i' is the induced deformation on U_i coming from X'. Note that if we restrict φ_i to the closed subscheme $U_i = (U_i \otimes_k k[\epsilon]) \otimes_{k[\epsilon]} k$, we get the identity map $U_i \to U_i$ by the very meaning of "isomorphic as deformations." Now, on each (affine) intersection $U_{ij} \coloneqq U_i \cap U_j$, we get a $k[\epsilon]$-scheme automorphism $\psi_{ij} \coloneqq \varphi_j^{-1} \circ \varphi_i$ of $U_{ij} \otimes_k k[\epsilon]$, which lifts the identity on U_{ij}.

For a k-algebra R, let's consider the elements $\theta \in \mathrm{Aut}_{k[\epsilon]}(R \otimes_k k[\epsilon]) = \mathrm{Aut}_{k[\epsilon]}(R[\epsilon]/\epsilon^2)$ reducing to the identity mod ϵ. By the latter condition, for $a \in R$, we can write $\theta(a) = a + \epsilon d(a)$ for some function $d : R \to R$, so $\theta(a + \epsilon b) = \theta(a) + \epsilon\theta(b) = a + \epsilon d(a) + \epsilon b$. Using that θ is a $k[\epsilon]$-algebra map, it's not hard to check that d is actually a k-linear derivation, and conversely such a d defines a $k[\epsilon]$-algebra automorphism of $R \otimes_k k[\epsilon]$ lifting id_R. For two such automorphisms θ_1 and θ_2 with corresponding k-linear derivations d_1 and d_2, we have $(\theta_1 \circ \theta_2)(a + \epsilon b) = a + \epsilon(d_1(a) + d_2(a)) + \epsilon b$. In other words, elements in $\mathrm{Aut}_{k[\epsilon]}(R[\epsilon]/\epsilon^2)$ correspond to k-derivations $R \to R$ (with the identity corresponding to the zero derivation), and composing automorphisms corresponds to adding derivations.

Having gone through this brief detour, we return to the situation at hand. We may think of the automorphisms ψ_{ij} as elements $\theta_{ij} \in H^0(U_{ij}, \mathcal{T}_{X/k}) = \mathrm{Der}_k(k[U_{ij}], k[U_{ij}])$. On $U_{ijk} \coloneqq U_i \cap U_j \cap U_k$, we have $\psi_{ki} \circ \psi_{jk} \circ \psi_{ij} = \mathrm{id}$, so $\theta_{ki} + \theta_{jk} + \theta_{ij} = 0$. It follows that (θ_{ij}) is a Čech 1-cocycle for the covering $\mathfrak{U}$ valued in the sheaf $\mathcal{T}_{X/k}$. Moreover, if we change each φ_i to another isomorphism $\varphi_i' : U_i \otimes_k k[\epsilon] \xrightarrow{\sim} U_i'$ as deformations, then $(\varphi_i')^{-1} \circ \varphi_i$ is an automorphism of $U_i \otimes_k k[\epsilon]$ coming from some derivation $\alpha_i \in H^0(U_i, \mathcal{T}_{X/k})$, so θ_{ij}' (corresponding to $\psi_{ij}' = (\varphi_j')^{-1} \circ \varphi_i'$) satisfies $\theta_{ij}' = \alpha_j + \theta_{ij} - \alpha_i$. In other words, (θ_{ij}) differs from (θ_{ij}') by a coboundary, which means (θ_{ij}) is a well-defined class in $\check{H}^1(\mathfrak{U}, \mathcal{T}_{X/k})$, which we can check is compatible with refinements of open covers, and hence not dependent on the affine covering $\mathfrak{U}$.

Thus, (θ_{ij}) determines an element of $H^1(X, \mathcal{T}_{X/k})$ as Čech theory for an affine open cover of X computes quasicoherent sheaf cohomology on X. We can easily reverse the preceding argument: a class (θ_{ij}) of Čech 1-cocycles in $\check{H}^1(X, \mathcal{T}_{X/k})$ glues trivial deformations of an affine open cover to define a global deformation $X \to X'$. This gives the desired bijective correspondence. □

Now, recall that we have put a k-vector space structure on the set $\mathrm{Def}_{E_0/k}(k[\epsilon])$ of deformations of the k-scheme E_0 over the first-order infinitesimal thickening $k[\epsilon]$ of k, since this is exactly the fiber of $Y(k[\epsilon]) \to Y(k)$ above y. It is concretely described as follows: given deformations E, E' of E_0 corresponding to k-algebra maps $\psi_E, \psi_{E'} : \mathcal{O}_{Y,y} \to k[\epsilon]$ over $y^* = \varphi \circ \pi$, we write

$$\psi_E(r) = \varphi(\overline{r}) + d_E(r)\epsilon, \quad \psi_{E'}(r) = \varphi(\overline{r}) + d_{E'}(r)\epsilon$$

in the notation of (3.3.1), where d_E and $d_{E'}$ are some functions $\mathcal{O}_{Y,y} \to k$. Then d_E and $d_{E'}$

are in fact k-derivations over y^*, and we define the sum $E + E'$ to be the deformation of E_0 corresponding to the k-algebra map $\psi_{E+E'} : \mathcal{O}_{Y,y} \to k[\epsilon]$ (lifting y^*) associated to $d_E + d_{E'}$:

$$\psi_{E+E'}(r) = \varphi(\overline{r}) + (d_E + d_{E'})(r)\epsilon.$$

Similarly, for a scalar $c \in k$, we define the product cE to be the deformation of E_0 corresponding to the k-algebra map $\psi_{cE} : \mathcal{O}_{Y,y} \to k[\epsilon]$ (lifting y^*) associated to cd_E:

$$\psi_{cE}(r) = \varphi(\overline{r}) + c \cdot d_E(r)\epsilon.$$

One can check that the set-theoretic bijection $H^1(E_0, \mathcal{T}_{E_0}) \cong \mathrm{Def}_{E_0/k}(k[\epsilon])$ also identifies the natural k-vector space structure on $H^1(E_0, \mathcal{T}_{E_0/k})$ (which comes from the addition or scalar multiplication of derivations in $\mathrm{Der}_k(k[U_{ij}], k[U_{ij}])$, in the notation of the proof of Lemma 3.3.4) with this k-vector space structure on $\mathrm{Def}_{E_0/k}(k[\epsilon])$ based on adding and k-multiplying k-linear derivations. Since the latter vector space structure arose from a set-theoretic identification of $\mathrm{Def}_{E_0/k}(k[\epsilon])$ with the tangent space $T_y(Y)$, we can finally give:

Proof of Proposition 3.3.2. The preceding shows that $T_y(Y) \cong H^1(E_0, \mathcal{T}_{E_0/k})$ as k-vector spaces. Thus, we just need to show that $\dim_k H^1(E_0, \mathcal{T}_{E_0/k}) = 1$. By Serre duality, this is equal to $\dim_k H^0(E_0, \Omega^1_{E_0/k} \otimes \Omega^1_{E_0/k})$. Since E_0 has genus 1, a Riemann-Roch calculation shows that $\Omega^1_{E_0/k} \cong \mathcal{O}_{E_0}$. Thus, $h^0(E_0, \Omega^1_{E_0/k} \otimes \Omega^1_{E_0/k}) = h^0(E_0, \mathcal{O}_{E_0}) = 1$. □

We postpone the discussion of the fibers of $Y_1(N) \to \mathrm{Spec}(\mathbf{Z}[1/N])$ being geometrically connected until later; this turns out to be a much harder fact (even over $\mathbf{Q}$).

4 Analytic Theory of Modular Curves

In this section, we work out parts of the theory of modular curves via analytic approaches. As in Section 3, $N \geq 4$ is an integer.

4.1 The Analytic Theory of $Y_1(N)$

In this subsection, we turn to the "classical" theory of $Y_1(N)$ as a quotient of the complex upper half-plane $\mathbf{H} = \{z \in \mathbf{C} : \mathrm{Im}(z) > 0\}$. It turns out this is the only way to get a grasp on some of the properties of $Y_1(N)_{\overline{\mathbf{Q}}}$ we want to know about (such as connectedness), a concrete description of its "regular compactification" $X_1(N)_{\overline{\mathbf{Q}}}$, and its genus (after regular compactification).

We will assume the basic facts of the theory of algebraic curves as laid out in [13, Chapter IV]. Unless otherwise specified, in the rest of this subsection 4.1, we work over the base field $\mathbf{C}$, so by $Y_1(N)$, we really mean the base change $Y_1(N)_{\mathbf{C}}$.

Lemma 4.1.1. The natural map $\mathrm{SL}_2(\mathbf{Z}) \to \mathrm{SL}_2(\mathbf{Z}/N\mathbf{Z})$ is surjective.

Proof. Let $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ be a representative of some class of $\mathrm{SL}_2(\mathbf{Z}/N\mathbf{Z})$, where $a \neq 0$ (replace it by N, if necessary). We need to find a matrix in $\mathrm{SL}_2(\mathbf{Z})$ that is equivalent to it mod N. First, we claim that there is $b' \equiv b \bmod N$ such that $(a, b') = 1$. If $a = \pm 1$, then take $b' = b$. If not, take the prime factorization $a = \pm p_1^{e_1} \dots p_r^{e_r}$. For each $1 \leq i \leq r$, write $t_i = 1$ if $p_i | b$, and 0 otherwise. By the Chinese remainder theorem, we can pick $t \in \mathbf{Z}$ such that $t \equiv t_i \bmod p_i$ for each i. We claim that $(b + tN, a) = 1$, so that $b + tN$ is our required b'. If not, pick a prime p_i dividing both. If $p_i \nmid b$, then $t \equiv 0 \bmod p_i$, a contradiction, but if $p_i | b$, then $t \equiv 1 \bmod p_i$, so p_i must divide N. Then it would not be possible for $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ to reduce to an element of $\mathrm{SL}_2(\mathbf{Z}/N\mathbf{Z})$ (as p_i divides each of a, b, N).

So with this b' coprime to a, we can find integers x, y with $ax - b'y = 1$. Define $c' \coloneqq c + y(1 - (ad - b'c))$ and $d' \coloneqq d + x(1 - (ad - b'c))$. Then $\begin{bmatrix} a & b' \\ c' & d' \end{bmatrix}$ is in $\mathrm{SL}_2(\mathbf{Z})$ and equivalent to our original matrix mod N. □

Recall that elliptic curves over $\mathbf{C}$ are analytically isomorphic to quotients $\mathbf{C}/\Lambda$ for some $\mathbf{Z}$-lattice Λ. Of course, lattices that are related by scaling by an element of $\mathbf{C}^\times$ give isomorphic elliptic curves, so we may we assume that 1 is part of a $\mathbf{Z}$-basis of Λ: it has the form $\mathbf{Z} \oplus \mathbf{Z}\tau$ for some $\tau \in \mathbf{H}$. We denote such a lattice by Λ_τ, and the corresponding elliptic curve $\mathbf{C}/\Lambda_\tau$ by E_τ. It is a classical fact (via functoriality of the complex-analytic exponential map) that two such quotients $E_\tau, E_{\tau'}$ are isomorphic if and only if $\Lambda_\tau = z\Lambda_{\tau'}$ for some $z \in \mathbf{C}^\times$.

We now define an action of $\mathrm{SL}_2(\mathbf{Z})$ on $\mathbf{H}$ that preserves such isomorphism classes of E_τ's. Suppose $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbf{Z})$. We set $\gamma(\tau) = (a\tau + b)/(c\tau + d)$, which is also in $\mathbf{H}$ by virtue of γ having positive determinant, and moreover this indeed gives a group action. On the other hand, notice that Λ_τ is $\Lambda_{\gamma(\tau)}$ scaled by $c\tau + d$, since

$$\Lambda_{\gamma(\tau)} = \mathbf{Z} \oplus \mathbf{Z}\left(\frac{a\tau + b}{c\tau + d}\right) \xrightarrow[\sim]{\cdot(c\tau+d)} \mathbf{Z}(c\tau + d) \oplus \mathbf{Z}(a\tau + b),$$

and $-b(c\tau + d) + d(a\tau + b) = \tau$, $a(c\tau + d) - c(a\tau + b) = 1$. Hence $E_\tau \cong E_{\gamma(\tau)}$.

We will now see what happens when we introduce points of exact order N:

Lemma 4.1.2. Any elliptic curve $E/\mathbf{C}$ with a point P of order N is isomorphic to some E_τ with $P = 1/N \bmod \Lambda_\tau$.

Proof. Pick $\tau \in \mathbf{H}$ so that $E = E_\tau$. We have $P = (c/N)\tau + (d/N)$, where $c, d \in \mathbf{Z}$ satisfy $(c, d) = (1)$ in $\mathbf{Z}/N\mathbf{Z}$ (equivalently, $\gcd(c, d, N) = 1$). Consider an element $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$

in $\mathrm{SL}_2(\mathbf{Z}/N\mathbf{Z})$, which by Lemma 4.1.1, lifts to some $\gamma = \begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix} \in \mathrm{SL}_2(\mathbf{Z})$. But P is also $(c'/N)\tau + (d'/N) \bmod \Lambda_\tau$, since $c' - c, d' - d \in N\mathbf{Z}$. Then the isomorphism $E_\tau \xrightarrow{\sim} E_{\gamma(\tau)}$ via scaling by $1/(c'\tau + d')$ sends the pair (E_τ, P) to $(E_{\gamma(\tau)}, 1/N \bmod \Lambda_{\gamma(\tau)})$. □

We have built a *surjective* map of sets from $\mathbf{H}$ to $Y_1(N)(\mathbf{C})$ given by $\tau \mapsto (E_\tau, 1/N)$. On the other hand, it is obviously not injective, since τ and $\tau + 1$ have the same image, for instance. It remains to find a good description of the fibers of this map. This is given by using the following "congruence subgroups":

Definition 4.1.3. We write $\Gamma(1)$ to mean $\mathrm{SL}_2(\mathbf{Z})$. We also set

$$\Gamma_1(N) \coloneqq \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma(1) : a \equiv d \equiv 1 \bmod N, c \equiv 0 \bmod N \right\}.$$

One can check that $\Gamma(1)$, and hence all the $\Gamma_1(N)$'s, act "properly discontinuously" on $\mathbf{H}$, and so the quotient of $\mathbf{H}$ by any of these groups has a natural structure of a non-compact connected Riemann surface. We will come back to this point later. For now, we just want to show that $\Gamma_1(N)$-orbits are the fibers of $\mathbf{H} \to Y_1(N)(\mathbf{C})$.

Proposition 4.1.4. The fibers of $\mathbf{H} \to Y_1(N)(\mathbf{C})$ are the $\Gamma_1(N)$-orbits.

Proof. Using the fact that $(c\tau + d)\Lambda_{\gamma(t)} = \Lambda_\tau$, where (c, d) is the bottom row of a matrix $\gamma \in \Gamma(1)$, it is easy to see that the surjection $\mathbf{H} \to Y_1(N)(\mathbf{C})$ is $\Gamma_1(N)$-invariant and so descends to a surjection $\mathbf{H}/\Gamma_1(N) \to Y_1(N)(\mathbf{C})$. Now, all we have to do is show that it is injective, so suppose that for $\tau, \tau' \in \mathbf{H}$, there is an isomorphism of pairs $(E_\tau, 1/N) \xrightarrow{\sim} (E_{\tau'}, 1/N)$. Then $\Lambda_\tau = z\Lambda_{\tau'}$ for some $z \in \mathbf{C}^\times$, so $1 = z(c\tau' + d)$ for some $c, d \in \mathbf{Z}$ and

$$\frac{1}{N} + j + k\tau = \frac{z}{N} \tag{4.1.1}$$

for some $j, k \in \mathbf{Z}$.

Note that c and d must be coprime, since 1 is part of a basis of $\Lambda_\tau = z\Lambda_{\tau'}$. Thus, we can pick $a, b \in \mathbf{Z}$ with $ad - bc = 1$. Let $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, so $z\Lambda_{\tau'} = \Lambda_{\gamma(\tau')}$, as the latter is spanned by $1 = z(c\tau' + d)$ and $(a\tau' + b)/(c\tau' + d) = z(a\tau' + b)$, whereas the former is spanned by z and $z\tau'$. Hence $\Lambda_\tau = \Lambda_{\gamma(\tau')}$, so there are integers j_1, j_2, k_1, k_2 such that $\tau = j_1\gamma(\tau') + k_1$, $\gamma(\tau') = j_2\tau + k_2$. Upon writing $\tau = j_1 j_2 \tau + j_1 k_2 + k_1$ and comparing imaginary parts, we must have $j_1 j_2 = 1$, so $j_1 = j_2 = 1$ as both τ and $\gamma(\tau')$ have positive imaginary part. Hence

$$\tau = \gamma(\tau') + k_1, \tag{4.1.2}$$

and so $\tau = \gamma'(\gamma(\tau'))$ with $\gamma' = \begin{bmatrix} 1 & k_1 \\ 0 & 1 \end{bmatrix} \in \Gamma_1(N)$.

It remains to show that $\gamma \in \Gamma_1(N)$, so τ and τ' are in the same orbit of $\Gamma_1(N)$. By (4.1.1) and (4.1.2), we have $z = 1 + jN + kN\tau = (1 + jN) + kN(\gamma(\tau') + k_1)$. Hence

$$\begin{aligned} 1 &= z(c\tau' + d) \\ &= \left((1 + jN + kNk_1) + kN\left(\frac{a\tau' + b}{c\tau' + d}\right)\right)(c\tau' + d) \\ &= (1 + jN + kNk_1)(c\tau' + d) + kN(a\tau' + b). \end{aligned} \tag{4.1.3}$$

As $\mathrm{Im}(\tau') \neq 0$, we must have $(1 + jN + kNk_1)c + kNa = 0$, so $c \equiv 0 \bmod N$. Also by (4.1.3), $(1 + jN + kNk_1)d + kNb = 1$, so $d \equiv 1 \bmod N$. Hence $a \equiv 1 \bmod N$ by looking at $\det(\gamma) \bmod N$, so $\gamma \in \Gamma_1(N)$ by definition. □

We have built a set-theoretic bijection $\mathbf{H}/\Gamma_1(N) \to Y_1(N)(\mathbf{C})$, but it is not a tautology that the complex manifold structures on $\mathbf{H}/\Gamma_1(N)$ and $Y_1(N)(\mathbf{C})$ agree. Since a full proof of this fact is quite involved, we will merely sketch the ideas:

Proposition 4.1.5. The bijection $\mathbf{H}/\Gamma_1(N) \to Y_1(N)(\mathbf{C})$ is a holomorphic isomorphism of Riemann surfaces.

Note that because $\mathbf{H}$ is connected, so is $\mathbf{H}/\Gamma_1(N)$. This in turn implies that $Y_1(N)_{\mathbf{C}}$ is connected (since the complex topology is finer than the Zariski topology), so the generic fiber $Y_1(N)_{\mathbf{Q}}$ is geometrically connected!

Sketch. Consider the free action of $\mathbf{Z} \oplus \mathbf{Z}$ on $\mathbf{C} \times \mathbf{H}$ by $(n, m) : (z, \tau) \mapsto (z + n + m\tau, \tau)$. Let $\mathcal{E}$ be the quotient space arising from this action, which has a natural map to $\mathbf{H}$ by taking the second coordinate. Let $\wp_\tau$ be the Weierstrass $\wp$-function corresponding to the lattice Λ_τ, so $\wp_\tau$ is meromorphic on $\mathbf{C}$ with double poles at the points of Λ_τ [13, IV.4.12B]. The function $\mathbf{C} \times \mathbf{H} \to \mathbf{CP}^1$ defined by $(z, \tau) \mapsto \wp_\tau(z)$ is holomorphic, and via the map

$$(z, \tau) \mapsto \begin{cases} ([\wp_\tau(z), \wp'_\tau(z), 1], \tau) & z \notin \Lambda_\tau \\ ([\wp_\tau(z)/\wp'_\tau(z), 1, 1/\wp'_\tau(z)], \tau) & z \in \Lambda_\tau \end{cases},$$

we get a holomorphic $\mathbf{H}$-isomorphism

$$\mathcal{E} \cong \{([x, y, z], \tau) : y^2 z = 4x^3 - g_2(\tau)xz^2 - g_3(\tau)z^3\} \hookrightarrow \mathbf{CP}^2 \times \mathbf{H}$$

with the classical g_2, g_3 as in [13, IV.4.12B].

We have an action of $\Gamma(1)$ on $\mathbf{H}$, and we want to lift that to an action on $\mathcal{E}$. For $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma(1)$, we can consider an action on $\mathbf{C} \times \mathbf{H}$ given by $\gamma : (z, \tau) \mapsto (z/(c\tau + d), \gamma(\tau))$,

which lies over the action on $\mathbf{H}$. Note that this map indeed defines an action, since if $\gamma' = \begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix} \in \Gamma(1)$, then the product $\gamma'\gamma$ has bottom row $\begin{bmatrix} c'a + d'c & c'b + d'd \end{bmatrix}$ and

$$\begin{aligned} \gamma'(\gamma(z,\tau)) &= \gamma'\left(\frac{z}{c\tau + d}, \gamma(\tau)\right) \\ &= \left(\frac{z}{(c\tau + d)\,(c'(a\tau + b)/(c\tau + d) + d')}, (\gamma'\gamma)(\tau)\right) \\ &= \left(\frac{z}{(c'a + d'c)\tau + (c'b + d'd)}, (\gamma'\gamma)(\tau)\right). \end{aligned}$$

We want to relate the $\Gamma(1)$ and $\mathbf{Z} \oplus \mathbf{Z}$-actions on $\mathbf{C} \times \mathbf{H}$. Define a "twisted" version of the usual $\Gamma(1)$-action on $\mathbf{Z} \oplus \mathbf{Z}$ by

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} (n, m) = (an - bm, -cn + dm).$$

A direct matrix calculation shows that this is still a group action. Then the $\Gamma(1)$-action on $\mathbf{C} \times \mathbf{H}$ is compatible with the $\mathbf{Z} \oplus \mathbf{Z}$-action on $\mathbf{C} \times \mathbf{H}$ in the sense that for any $\gamma \in \Gamma(1)$, $(n, m) \in \mathbf{Z} \oplus \mathbf{Z}$, and $(z, \tau) \in \mathbf{C} \times \mathbf{H}$,

$$\gamma((n, m) \cdot (z, \tau)) = (\gamma(n, m)) \cdot (\gamma(z, \tau)).$$

This can again be verified by direct calculation. Hence $\Gamma(1)$-action on $\mathbf{C} \times \mathbf{H}$ descends to an action on $\mathcal{E}$ over the usual $\Gamma(1)$-action on $\mathbf{H}$.

We restrict to the action of the subgroup $\Gamma_1(N)$ on $\mathcal{E}$. This action is free as it is free on $\mathbf{H}$. It turns out that the quotient $\mathbf{H}/\Gamma_1(N)$ is the representing object for the functor $\mathcal{F}$ associating a complex manifold to the set of holomorphic elliptic curves over that manifold with a holomorphic section of exact order N on fibers, and moreover that the quotient $\mathcal{E}/\Gamma_1(N)$ with the section $1/N$ over $\mathbf{H}/\Gamma_1(N)$ is the associated universal object.

Write E for the universal elliptic curve over $Y_1(N)$, as constructed in Theorem 3.2.3. By the universality of $\mathcal{E}/\Gamma_1(N)$ applied to the holomorphic elliptic curve E^{an} over $Y_1(N)^{\mathrm{an}}$, we get a unique holomorphic map $Y_1(N)^{\mathrm{an}} \to \mathbf{H}/\Gamma_1(N)$ over which there exists a (necessarily unique) Cartesian diagram

$$\begin{array}{ccc} E^{\mathrm{an}} & \longrightarrow & \mathcal{E}/\Gamma_1(N) \\ \downarrow & & \downarrow \\ Y_1(N)^{\mathrm{an}} & \longrightarrow & \mathbf{H}/\Gamma_1(N) \end{array}$$

respecting the N-torsion sections. By inspection, $Y_1(N)^{\mathrm{an}} \to \mathbf{H}/\Gamma_1(N)$ is exactly the *inverse* of the set-theoretic bijection $\mathbf{H}/\Gamma_1(N) \to Y_1(N)(\mathbf{C})$ constructed in Proposition 4.1.4 (note

how this holomorphic map goes in the opposite direction to what we might expect!). Since it is bijective and holomorphic between pure 1-dimensional complex manifolds, it must be a biholomorphism. □

4.2 The Analytic Theory of $X_1(N)$

We have seen that $Y_1(N)_{\mathbf{Q}}$ is a smooth geometrically connected affine curve, but it is not proper. This can be remedied via the *regular compactification* $X_1(N)_{\mathbf{Q}}$, which is the unique scheme fitting into the diagram

$$\begin{array}{ccc} Y_1(N)_{\mathbf{Q}} & \longrightarrow & X_1(N)_{\mathbf{Q}} \\ & \searrow & \downarrow \\ & & \mathrm{Spec}(\mathbf{Q}) \end{array}$$

such that $Y_1(N)_{\mathbf{Q}} \to X_1(N)_{\mathbf{Q}}$ is an open immersion with dense image and $X_1(N)_{\mathbf{Q}} \to \mathrm{Spec}(\mathbf{Q})$ is smooth and proper.

Remark 4.2.1. In general for any field K, the regular compactification X of a regular affine curve Y over K exists and commutes with any separable base change L/K of fields, since X is uniquely characterized as being regular and proper over the base field, containing Y as a dense open subset. Let's prove this in the case we are interested in: when K is perfect (e.g. characteristic 0). Now, suppose the open immersion $i : Y \to X$ is the regular compactification of Y. Then Y and X are both K-smooth (since the properties "regular" and "smooth" are equivalent for finite type schemes over a perfect field), so Y_L and X_L are both L-smooth, hence regular.

It remains to show that $i_L : Y_L \to X_L$ makes Y_L dense inside X_L. Since Y is a dense open inside X, it is schematically dense (as X is reduced), so the natural map $\mathcal{O}_X \to i_*\mathcal{O}_Y$ is injective. Via the *flat* base change $K \to L$, $\mathcal{O}_{X_L} \to (i_L)_*\mathcal{O}_{Y_L}$ is also injective, so again Y_L is schematically dense in X_L. But schematically dense implies topologically dense.

In particular, Y is geometrically connected over K if and only if X is. The "if" direction is clear, since a regular connected scheme over a field must be irreducible, and nonempty open subsets of irreducibles are irreducible. For the other direction, note that Y_{K_s} is regular and connected, hence irreducible, so its closure X_{K_s} is also irreducible.

It is hard to say much more about $X_1(N)_{\mathbf{Q}}$ via this definition, since it does not come with a moduli space interpretation as $Y_1(N)_{\mathbf{Q}}$ does (in fact, a moduli interpretation in terms of *generalized elliptic curves* does exist as in [7], but explaining that is well outside the scope of this thesis, though it will be essential for later arithmetic applications in Section 5). We will now take a completely different approach to describing $X_1(N)_{\mathbf{C}}$, which is via its analytic model. This will allow us to compute the genus of $X_1(N)_{\mathbf{Q}}$ as a curve over $\mathbf{Q}$ as well.

Unless otherwise specified, in the rest of this subsection 4.2, we work over the base field $\mathbf{C}$. We will follow Sections 4.1 and 4.2 of [20], as well as Lecture 12 of [27].

Definition 4.2.2. Define $\mathbf{H}^*$ to be union of the upper half-plane

$$\mathbf{H} \subset \mathbf{C} - \mathbf{R} = \mathbf{P}^1(\mathbf{C}) - \mathbf{P}^1(\mathbf{R})$$

together with the points of $\mathbf{P}^1(\mathbf{Q})$, which we call the *cusps*. We give $\mathbf{H}^*$ the natural topology, described below, extending the one on $\mathbf{H}$ (as an open subset). For a *finite-index* subgroup Γ of $\Gamma(1)$, we write X_Γ for $\mathbf{H}^*/\Gamma$ (in the future, $\Gamma \subseteq \Gamma(1)$ will always have finite index, unless otherwise specified). This is a compact Riemann surface, and we call $z \in X_\Gamma$ a *cusp* if it is the image of a cusp of $\mathbf{H}^*$ under the quotient $\mathbf{H}^* \to \mathbf{H}^*/\Gamma$.

Notice that $\Gamma(1)$ acts transitively on the set of cusps: for rational a/b with a and b coprime integers (where $\pm 1/0 = \infty$), an element of the form $\begin{bmatrix} c & d \\ b & -a \end{bmatrix}$ sends it to ∞. We can also think of the topology on $\mathbf{H}^*$ as follows: we give ∞ the neighborhood basis consisting of sets $U_k \coloneqq \{\infty\} \cup \{z \in \mathbf{H} : \mathrm{Im}(z) > k\}$, and a neighborhood basis at other cusps is given by $\Gamma(1)$-translation. Moreover, because Γ has *finite index* in $\Gamma(1)$, it follows that there are only finitely many cusps of X_Γ (as we just saw that $\Gamma(1)$ acts transitively on $\mathbf{P}^1(\mathbf{Q})$).

We now introduce some notation involving stabilizers of points.

Definition 4.2.3. Write $\overline{\Gamma}$ for the image of a subgroup $\Gamma \subset \Gamma(1)$ in $\overline{\Gamma(1)} \coloneqq \Gamma(1)/\{\pm 1\}$. Write Γ_z for the stabilizer of $z \in \mathbf{H}^*$ under the action of Γ on $\mathbf{H}^*$. Define $\overline{\Gamma}_z$ similarly.

Here, it is useful to quotient out by $\{\pm 1\}$, since -1 stabilizes all points in $\mathbf{H}^*$.

Ultimately, we would like to compute the genus of X_Γ. The approach towards doing so is as follows:

1. Understand the ramification of the quotient map $X_\Gamma \to X_{\Gamma'}$, where $\Gamma \subseteq \Gamma'$ are finite-index subgroups of $\Gamma(1)$.
2. Note that all cusps of $\mathbf{H}^*$ lie in the same orbit under the $\Gamma(1)$-action; in other words, $X(1) \coloneqq X_{\Gamma(1)}$ looks like $(\mathbf{H}/\Gamma(1)) \cup \{\infty\}$. Moreover, the j-function gives a holomorphic isomorphism $X(1) \cong \mathbf{CP}^1$, so $X(1)$ has genus 0.
3. Apply the analytic Riemann-Hurwitz formula to the map $X_\Gamma \to X(1)$ to compute the genus of X_Γ.

We begin by discussing the stabilizers of points $z \in \mathbf{H}$.

Lemma 4.2.4. For $z \in \mathbf{H}$, there is a natural group isomorphism between $\Gamma(1)_z$ and $\mathrm{Aut}(E_z)$.

Proof. Say $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma(1)$ stabilizes z. Via the $\mathbf{Z}$-basis $\{1, z\}$ of Λ_z, we can construct an automorphism g of Λ_z by setting $g(z) = az+b$ and $g(1) = cz+d$, and extending $\mathbf{Z}$-linearly to all of Λ_z. Since $z = \gamma(z) = (az+b)/(cz+d)$, we have $g(z) = (cz+d)z = g(1)z$, so g extends $\mathbf{C}$-linearly to all of $\mathbf{C}$ via multiplication by $g(1) \in \mathbf{C}^\times$. But $g(\Lambda_z) = \Lambda_z$ by construction, so it induces an automorphism of $E_z = \mathbf{C}/\Lambda_z$.

Conversely, suppose that g is an automorphism of E_z. By the basic theory of complex Lie groups, we may draw a commutative diagram

$$\begin{array}{ccc} \mathbf{C} & \xrightarrow{\mathrm{Lie}(g)} & \mathbf{C} \\ \downarrow{\scriptstyle \exp} & & \downarrow{\scriptstyle \exp} \\ E_z & \xrightarrow{g} & E_z \end{array}$$

via functoriality of the complex-analytic exponential map, where we interpret $\mathbf{C}$ as the Lie algebra of E_z and exp as the quotient map $\mathbf{C} \to E_z$ (a homomorphism since E_z is abelian). Since $\mathrm{Lie}(g)$ is $\mathbf{C}$-linear, it must be multiplication by some $\alpha \in \mathbf{C}^\times$.

Now, $\alpha\Lambda_z \subseteq \Lambda_z$, so $\alpha = cz + d$ for some integers c, d. As in the proof of Proposition 4.1.4, c and d must be coprime (since we also have $\alpha^{-1}\Lambda_z \subseteq \Lambda_z$ as α^{-1} gives the inverse automorphism), so we can put them into a matrix $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma(1)$. Then $\alpha^{-1}\Lambda_z = \Lambda_{\gamma(z)}$ as the latter is spanned by $1 = \alpha^{-1}(cz+d)$ and $(az+b)/(cz+d) = \alpha^{-1}(az+b)$. So $\Lambda_z = \Lambda_{\gamma(z)}$, meaning that there are integers a, b, a', b' such that $\gamma(z) = az + b$ and $z = a'\gamma(z) + b'$. So $z = a'(az + b) + b$, and since $\mathrm{Im}(z) \neq 0$, we must have $a'a = 1$ upon comparing imaginary parts. But then $a = 1$ as both $\gamma(z)$ and z have positive imaginary parts.

Hence $\gamma(z) + n = z$ for some integer n. In other words,

$$z = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} (z) = \begin{bmatrix} a+cn & b+dn \\ c & d \end{bmatrix} (z).$$

Therefore, we have built $\gamma' = \begin{bmatrix} a+cn & b+dn \\ c & d \end{bmatrix} \in \Gamma(1)_z$ from g. These maps $\Gamma(1)_z \to \mathrm{Aut}(E_z)$ and $\mathrm{Aut}(E_z) \to \Gamma(1)_z$ are easily checked to be inverses and group homomorphisms. □

We have shown $\Gamma(1)_z = \mathrm{End}(E_z)^\times$. From [13, IV.4.19], we know that $\mathrm{End}(E_z)^\times$ is larger than $\{\pm 1\}$ if and only if $\mathrm{End}(E_z)$ equals $\mathbf{Z}[i]$ or $\mathbf{Z}[\omega]$, for $\omega = e^{2\pi i/3}$ a primitive cube root of unity with positive imaginary part.

Lemma 4.2.5. If $\mathrm{End}(E) = \mathbf{Z}[i]$ (resp. $\mathrm{End}(E) = \mathbf{Z}[\omega]$), then $E \cong E_i$ (resp. $E \cong E_\omega$).

Proof. We first treat the case $\mathrm{End}(E) = \mathbf{Z}[i]$. Write $E = \mathbf{C}/\Lambda$, so Λ is a lattice stable under $\mathbf{Z}[i]$. Then Λ is a torsion-free $\mathbf{Z}[i]$-module of $\mathbf{Z}$-rank 2, which means it must be a free $\mathbf{Z}[i]$-module of rank 1. Hence $\Lambda = z\mathbf{Z}[i]$ for some $z \in \mathbf{C}^\times$, and so $E \cong E_i$. The case of $\mathrm{End}(E) = \mathbf{Z}[\omega]$ goes exactly the same way. □

Hence if $z \in \mathbf{H}$, one of three cases occurs:

1. if $z \in \Gamma(1)i$, then $\Gamma(1)_z = \{\pm 1, \pm i\} \cong \mathbf{Z}/4\mathbf{Z}$ and $\overline{\Gamma(1)}_z \cong \mathbf{Z}/2\mathbf{Z}$;
2. if $z \in \Gamma(1)\omega$, then $\Gamma(1)_z = \{\pm 1, \pm\omega, \pm\omega^2\} \cong \mathbf{Z}/6\mathbf{Z}$ and $\overline{\Gamma(1)}_z \cong \mathbf{Z}/3\mathbf{Z}$;
3. for all other z, $\Gamma(1)_z = \{\pm 1\} \cong \mathbf{Z}/2\mathbf{Z}$ and $\overline{\Gamma(1)}_z = 1$.

In general, for $\Gamma \subset \Gamma(1)$, we call $z \in \mathbf{H}$ an *elliptic point* of order 2 or 3 (for Γ) if $\overline{\Gamma}_z$ has order 2 or 3. We will call $a \in X_\Gamma$ an *elliptic point* of order 2 or 3 if one (any) of its preimages in $\mathbf{H}^*$ is an elliptic point of that order.

Having analyzed stabilizers at points of $\mathbf{H}$, it remains to deal with the cusps.

Lemma 4.2.6. If $z \in \mathbf{H}^*$ is a cusp, then $\overline{\Gamma(1)}_z \cong \mathbf{Z}$.

Proof. By transitivity of the $\Gamma(1)$-action on $\mathbf{P}^1(\mathbf{Q})$, we may assume $z = \infty$. Then for $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, we see that γ fixes z exactly when $c = 0$, which forces $a = d = 1$ or $a = d = -1$. Hence, the elements of $\overline{\Gamma(1)}_z$ are represented uniquely by the set of matrices of the form $\begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}$. □

We conclude that for any finite-index subgroup $\Gamma \subseteq \Gamma(1)$, $\overline{\Gamma}_z$ is nontrivial only if z is a cusp or an elliptic point, and these only have finitely many orbits under Γ.

With all of these preliminaries out of the way, we can finally understand the ramification of a quotient map $X_\Gamma \to X_{\Gamma'}$. The key result is:

Proposition 4.2.7 ([20, 1.8.1])**.** Let $\Gamma \subseteq \Gamma'$ be finite index subgroups of $\Gamma(1)$. Let $z \in \mathbf{H}^*$, and let a be its image in X_Γ. Then the ramification index at a of $f : X_\Gamma \to X_{\Gamma'}$ is $[\overline{\Gamma'_z} : \overline{\Gamma}_z]$.

Proof. First suppose that z is a point in $\mathbf{H}$. We may find a Mobius transformation $\rho \in \mathrm{SL}_2(\mathbf{C})$ such that $\rho(z) = 0$ and $\rho(\mathbf{H}) = \mathbf{D}$, where $\mathbf{D}$ is the unit open disk. Let W_r be an open ball of radius $r < 1$ about 0, and set $U \coloneqq \rho^{-1}(W_r)$. Now, we know from above that Γ_z is a finite cyclic group, being a subgroup of $\mathbf{Z}/c\mathbf{Z}$ for $c = 2$, 4, or 6, so $\rho\Gamma_z\rho^{-1}$ is as well. Hence, if $\psi \in \Gamma_z$, then $\theta \coloneqq \rho\psi\rho^{-1}$ is an automorphism of $\mathbf{D}$ fixing 0.

By the Schwarz Lemma, for all $w \in \mathbf{D}$, $|w| = |\theta(\theta^{-1}(w))| \leq |\theta^{-1}(w)| \leq |w|$, so all inequalities are equalities, and by applying Schwarz again, θ acts as multiplication by some complex number on the unit circle. But θ is also an element of a cyclic group with $\theta^{|\overline{\Gamma}_z|} = \mathrm{id}$ (even though θ and $-\theta$ are different elements of $\rho\Gamma_z\rho^{-1}$, they give the same automorphism), so θ acts as multiplication by some $e^{2\pi i n/d}$, $d = |\overline{\Gamma}_z|$. As another consequence, $\rho\Gamma_z\rho^{-1}(W_r) = W_r$, so $\Gamma_z(U) = U$.

Now, recall that $\Gamma(1) \supseteq \Gamma$ acts properly discontinuously on $\mathbf{H}$, so as U is an open neighborhood of z, we can take r so small such that $\gamma(U) \cap U \neq \emptyset$ implies $\gamma \in \Gamma_z$. Then the image $\pi(U)$ in the quotient X_Γ is biholomorphic to $U/\Gamma_z \cong W_r/\rho\Gamma_z\rho^{-1}$.

Define φ on W_r by $\varphi(w) = w^d$ for d as above. Since φ is invariant under rotation by $2\pi/d$ radians, and the group $\rho\Gamma_z\rho^{-1}$ consists of all possible rotations by integer multiples of $2\pi/d$, it induces a biholomorphism $W_r/\rho\Gamma_z\rho^{-1} \cong W_{r^d}$. We may therefore draw a commutative diagram

$$\begin{array}{ccccccc} & & U & \xrightarrow{\rho} & W_r & & \\ & \swarrow^{\pi} & \downarrow & & \downarrow & \searrow^{\varphi} & \\ \pi(U) & \longrightarrow & U/\Gamma_z & \longrightarrow & W_r/\rho\Gamma_z\rho^{-1} & \longrightarrow & W_{r^d} \end{array}$$

where all horizontal arrows are biholomorphisms.

Consider the commutative square formed by U, W_r, $\pi(U)$, and W_{r^d}. Ramification at z can be computed locally, so we are able to restrict attention to its open neighborhood U. But the ramification of φ at 0 is clearly of degree d, so the same is true about the ramification of π at $\varphi^{-1}(0) = z$. Hence, if $\Gamma \subseteq \Gamma'$ are finite index subgroups of $\Gamma(1)$, the quotient $X \to X_\Gamma \to X_{\Gamma'}$ satisfying $z \mapsto a \mapsto a'$ ramifies at z with degree $|\overline{\Gamma}_z|$ in the first step and degree $|\overline{\Gamma'_z}|$ in the composition. Hence, the ramification index of $X_\Gamma \to X_{\Gamma'}$ at a is the desired $[\overline{\Gamma'_z} : \overline{\Gamma}_z]$.

The other possibility is that a is a cusp, so we then can pick $\sigma \in \overline{\Gamma(1)}$ such that $\sigma(z) = \infty$. For $U_l \coloneqq \{w \in \mathbf{H} : \mathrm{Im}(w) > l\}$ and $U_l^* \coloneqq U_l \cup \{\infty\}$, set $U \coloneqq \sigma^{-1}(U_l)$ and $U^* \coloneqq \sigma^{-1}(U_l^*)$, so U^* is an open neighborhood of z. Similar to before, we pick l to be large enough such that $\gamma(U^*) \cap U^* \neq \emptyset$ implies $\gamma \in \Gamma_z$, which means that $\pi(U^*) \cong U^*/\Gamma_z \cong U_l^*/\sigma\Gamma_z\sigma^{-1}$. From Lemma 4.2.6 and the fact that $\Gamma_z = \Gamma(1)_z \cap \Gamma$ (in particular, Γ_z is finite index in $\Gamma(1)_z$), it follows that $\sigma\overline{\Gamma}_z\sigma^{-1}$ must be of the form $\left\{ \begin{bmatrix} 1 & h \\ 0 & 1 \end{bmatrix}^m : m \in \mathbf{Z} \right\}$ for some unique $h > 0$. Then define $\psi : U_l^* \to W_r$, where $r = e^{-2\pi l/h}$, by

$$\psi(w) = \begin{cases} e^{2\pi i w/h} & w \in U_l \\ 0 & w = \infty \end{cases}$$

Of course, ψ is invariant under the action of $\sigma\overline{\Gamma}_z\sigma^{-1}$, as the action fixes ∞ and only translates other points by integer multiples of h, so we get a map $U_l^*/\sigma\Gamma_z\sigma^{-1} \to W_r$ from the quotient, which is once again an biholomorphism. We may therefore draw a commutative diagram

$$\begin{array}{ccccccc} & & U^* & \xrightarrow{\sigma} & U_l^* & & \\ & \swarrow^{\pi} & \downarrow & & \downarrow & \searrow^{\psi} & \\ \pi(U^*) & \longrightarrow & U^*/\overline{\Gamma}_z & \longrightarrow & U_l^*/\sigma\overline{\Gamma}_z\sigma^{-1} & \longrightarrow & W_r \end{array}$$

with biholomorphisms for the horizontal arrows. Hence, via these identifications, we are able to think of $e^{2\pi iz/h}$ as a uniformizer (local coordinate) at $a = \pi(z)$.

So if we have finite-index subgroups $\Gamma \subseteq \Gamma'$ of $\Gamma(1)$, we know that $\overline{\Gamma}_z = h\mathbf{Z} \subseteq \mathbf{Z} = \overline{\Gamma(1)}_\infty$ for some positive integer h, and likewise $\overline{\Gamma'}_z = h'\mathbf{Z} \subseteq \mathbf{Z}$ for some h' necessarily dividing h. We saw that $e^{2\pi iz/h}$ is a uniformizer of the local ring $\mathcal{O}_a$, and similarly $e^{2\pi iz/h'}$ is a uniformizer of the local ring $\mathcal{O}_{a'}$ with a' the image of z in $X_{\Gamma'}$. But the valuation of $e^{2\pi iz/h'}$ in $\mathcal{O}_a$ is visibly $h/h' = [\overline{\Gamma'}_z : \overline{\Gamma}_z]$, and this is exactly the ramification of the quotient $X_\Gamma \to X_{\Gamma'}$ at a. □

We can now prove the genus formula for X_Γ. Recall the Riemann-Hurwitz formula for an analytic degree-n map $f : S' \to S$ between compact connected Riemann surfaces:

$$2g(S') - 2 = n(2g(S) - 2) + \sum_{p \in S'} (e_p - 1),$$

where e_p is the ramification index at p. We will apply this to the quotient map $X_\Gamma \to X(1)$ for a finite-index subgroup $\Gamma \subseteq \Gamma(1)$.

Theorem 4.2.8 (Genus Formula)**.** Let $\Gamma \subseteq \Gamma(1)$, and let d be the index $[\overline{\Gamma(1)} : \overline{\Gamma}]$ (notice that this is generally not $[\Gamma(1) : \Gamma]$!). Let v_2 and v_3 be the number of elliptic points of orders 2 and 3 in X_Γ, respectively. Let v_∞ be the number of cusps in X_Γ, and let g be the genus of X_Γ as a Riemann surface. Then

$$g = 1 + \frac{d}{12} - \frac{v_2}{4} - \frac{v_3}{3} - \frac{v_\infty}{2}. \tag{4.2.1}$$

Proof. The quotient $f : X_\Gamma \to X(1)$ has degree d, since any non-elliptic, non-cusp point of $\mathbf{H}^*$ has trivial $\overline{\Gamma(1)}$-stabilizer and exactly d preimages, none of which are ramified. Then by applying Riemann-Hurwitz to f, we have

$$2 - 2g = 2d - \sum_{p \in X_\Gamma} (e_p - 1).$$

Let q_2, q_3, and q_∞ be the images of i, ω, and ∞ in $X(1)$. By Proposition 4.2.7, we deduce that $e_p = 1$ unless p lies above q_2, q_3, or q_∞, since otherwise $\overline{\Gamma(1)}_z$ is already trivial for $z \in \mathbf{H}^*$ above p.

First, the points of $f^{-1}(q_2)$ that are elliptic (with respect to Γ) are unramified, since they must be elliptic of order 2, and the corresponding index $[\overline{\Gamma(1)}_z : \overline{\Gamma}_z]$ is 1. Those that are not must have $\overline{\Gamma}_z = 1$ and $e_p = 2$, but the total number of points in $f^{-1}(q_2)$, counted with multiplicity, is d. Hence the number of ramified points is $(d - v_2)/2$, so that $\sum_{f(p)=q_2}(e_p - 1) = (d - v_2)/2$. By similar logic, $\sum_{f(p)=q_3}(e_p - 1) = 2(d - v_3)/3$.

Finally, $f^{-1}(q_\infty)$ consists of *exactly* the cusps of X_Γ, since the cusps of $\mathbf{H}^*$ form a single orbit under $\Gamma(1)$. Hence $\sum_{f(p)=q_\infty}(e_p - 1) = \sum_{f(p)=q_\infty} e_p - \sum_{f(p)=q_\infty} 1 = d - v_\infty$. Plugging

these equations into the Riemann-Hurwitz formula, we get

$$2 - 2g = 2d - \frac{d - v_2}{2} - \frac{2(d - v_3)}{3} - (d - v_\infty),$$

which gives (4.2.1) when rearranged. □

We now define $X_1(N) \coloneqq X_{\Gamma_1(N)}$. It is a fact that compact Riemann surfaces are both "uniquely algebraic" and are uniquely determined by the complement of finitely many points, so this model of $X_1(N)$ over $\mathbf{C}$ agrees with the analytification of the algebro-geometric "regular compactification" introduced at the beginning of this section. Let's apply the genus formula to $X_1(N)$; the result will be of key importance to us later.

Recall from Theorem 4.2.8 that the degree of $X_1(N) \to X(1)$ is

$$d = d_N = [\overline{\Gamma(1)} : \overline{\Gamma_1(N)}] = \frac{1}{2}[\Gamma(1) : \Gamma_1(N)],$$

since $-1 \notin \Gamma_1(N)$ (as $N \geq 4$ by assumption). By a Chinese remainder theorem-style computation, we can compute $|\mathrm{SL}_2(\mathbf{Z}/N\mathbf{Z})| = N^3 \prod_{p|N} (1 - (1/p^2))$, and as there are N equivalence classes of matrices of the form $\begin{bmatrix} 1 & * \\ 0 & 1 \end{bmatrix} \bmod N$, we use the surjectivity of the reduction map $\Gamma(1) \to \mathrm{SL}_2(\mathbf{Z}/N\mathbf{Z})$ to conclude that $d = (N^2/2) \prod_{p|N} (1 - (1/p^2))$.

We next show that $\mathbf{H}^*$ has no elliptic points for $\Gamma_1(N)$. If $z \in \mathbf{H}$ and $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is in $\Gamma_1(N)_z$, then $cz^2 + (d - a)z - b = 0$. The discriminant of this quadratic is

$$(\mathrm{tr}(\gamma))^2 - 4 \det(\gamma) = (\mathrm{tr}(\gamma))^2 - 4,$$

and since z has nonzero imaginary part, this must be negative. So, $|a + d| < 2$ but $a + d \equiv 2 \bmod N$, which is impossible as we assume $N \geq 4$. Therefore $v_2, v_3 = 0$ for $\Gamma_1(N)$.

It remains to compute v_∞ for $\Gamma_1(N)$.

Lemma 4.2.9. For $\Gamma \subseteq \Gamma(1)$, $\gamma \mapsto \gamma(\infty)$ induces a bijection of $\Gamma \backslash \Gamma(1) / \Gamma(1)_\infty$ onto the cusps of X_Γ, so $|\Gamma \backslash \Gamma(1) / \Gamma(1)_\infty| = v_\infty(\Gamma)$.

Note that since $-1 \in \Gamma(1)_\infty$, we have $\Gamma \backslash \Gamma(1) / \Gamma(1)_\infty \cong \overline{\Gamma} \backslash \overline{\Gamma(1)} / \overline{\Gamma(1)}_\infty$.

Proof. If $hxk = y$ with $h \in \Gamma$, $x, y \in \Gamma(1)$, and $k \in \Gamma(1)_\infty$, then $x(\infty) = xk(\infty)$ and $y(\infty)$ are the same mod Γ. Hence the map is well-defined, and if $x(\infty), y(\infty)$ are the same in X_Γ, then $y^{-1}hx \in \Gamma(1)_\infty$ for some $h \in \Gamma$, so the map is injective. The map is also clearly surjective. □

Define $\Gamma(1)^+_\infty := \left\{ \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} : n \in \mathbf{Z} \right\}$, which is an index-2 subgroup of $\Gamma(1)_\infty$. Also, let M_N be the set of order-N elements of the additive group $(\mathbf{Z}/N\mathbf{Z})^{\oplus 2}$, so M_N consists of the ordered pairs (a, c) such that a and c generate the entire group $\mathbf{Z}/N\mathbf{Z}$. Then we put the following two equivalence relations on M_N:

$$(a, c) \sim (a', c') \text{ if } (a', c') = \pm(a + nc, c) \text{ for some } n \in \mathbf{Z}/N\mathbf{Z}.$$
$$(a, c) \sim' (a', c') \text{ if } (a', c') = (a + nc, c) \text{ for some } n \in \mathbf{Z}/N\mathbf{Z}.$$

First, we show that there is a Chinese remainder theorem-style decomposition of $M_N/\sim'$:

Lemma 4.2.10. There is a natural bijection $(M_N/\sim') \cong \prod_{p^e|N}(M_{p^e}/\sim'_{p^e})$, where the product is taken over the maximal prime powers dividing N, and $\sim'_{p^e}$ is the analogous equivalence relation on M_{p^e}.

Proof. There is an obvious surjective map $(M_N/\sim') \to \prod_{p^e|N}(M_{p^e}/\sim'_{p^e})$, and it remains to show that it is injective. If $(a, c) \sim'_{p^e} (a', c')$ for all $p^e|N$, then there is n_p such that $(a + n_p c, c) \equiv (a', c') \bmod p^e$. Then $c \equiv c' \bmod N$, and we can lift all the n_p's to a compatible $n \in \mathbf{Z}/N\mathbf{Z}$. So $(a + nc, c)$ and (a', c') are equal mod all p^e, hence equal mod N, meaning that $(a, c) \sim' (a', c')$. □

The importance of the equivalence relations $\sim$ and $\sim'$, in regards to counting cusps of $X_1(N)$, is as follows:

Lemma 4.2.11. There are bijections

$$\Gamma_1(N)\backslash\Gamma(1)/\Gamma(1)^+_\infty \to M_N/\sim', \qquad \Gamma_1(N)\backslash\Gamma(1)/\Gamma(1)_\infty \to M_N/\sim \tag{4.2.2}$$

both given by $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \mapsto (a, c) \bmod N$.

Proof. A direct computation with representatives of classes in $\Gamma_1(N)\backslash\Gamma(1)/\Gamma(1)^+_\infty$ and in $\Gamma_1(N)\backslash\Gamma(1)/\Gamma(1)_\infty$ shows that both maps are well-defined. Note that Lemma 4.1.1 shows that for any integers a, c with $(a, c, N) = 1$, there are integers a', c' with $a' \equiv a \bmod N$, $c' \equiv c \bmod N$, and $(a', c') = 1$. Hence the maps of (4.2.2) are surjective, so we only need to show their injectivity. We omit the remainder of the proof, as it is just a long computation in matrix and modular arithmetic. See [8, 3.8.3] for the details. □

So we may draw a commutative diagram

$$\begin{array}{ccc} \Gamma_1(N)\backslash\Gamma(1)/\Gamma(1)^+_\infty & \longrightarrow & M_N/\sim' \\ \downarrow & & \downarrow \psi \\ \Gamma_1(N)\backslash\Gamma(1)/\Gamma(1)_\infty & \longrightarrow & M_N/\sim \end{array}$$

where the horizontal arrows are the bijections of (4.2.2) and the vertical arrows are the natural quotient maps. We claim that the fibers of ψ each have size 2 when $N \geq 5$.

For $(a, c) \in M_N/\sim$, we just need to check that $(a, c) \not\sim' (-a, -c)$. If there is such an equivalence, then $c \equiv -c$ and $a + nc \equiv -a \bmod N$ for some n. If $c \equiv 0$, then $a \equiv -a$, which is impossible unless $N = 2$ due to the condition that (a, c) is order N in $(\mathbf{Z}/N\mathbf{Z})^{\oplus 2}$. If $c \not\equiv 0$, then $nc \equiv -2a$, but nc is either c or 0 (as $c \equiv -c$), so a has order 2 or 4 in $\mathbf{Z}/N\mathbf{Z}$. Hence (a, c) has order 2 or 4 in $(\mathbf{Z}/N\mathbf{Z})^{\oplus 2}$, but again this cannot happen for $N \geq 5$. Hence $|M_N/\sim'| = 2|M_N/\sim|$ when $N \geq 5$ (note that when $N = 4$, $|M_N/\sim'| = 5$ and $|M_N/\sim| = 3$, so by Lemma 4.2.9, $v_\infty(\Gamma_1(4)) = 3$; this is related to the phenomenon of "irregular cusps").

It remains to compute $|M_N/\sim'|$ for $N \geq 5$. By Lemma 4.2.10, we can reduce to the case where $N = p^e$ is a prime power. Considering a fixed $(a, c) \in M_{p^e}$, let f be the largest integer with $0 \leq f \leq e$ such that $p^f | c$. Then it is easy to see that $(a, c) \sim'_{p^e} (a', c)$ exactly when $a \equiv a' \bmod p^f$. So, for a fixed c, the number of inequivalent (a, c) under $\sim'$ is $\varphi(p^f)$, since a and c must generate 1 in $\mathbf{Z}/p^f\mathbf{Z}$. On the other hand, for any $0 \leq f \leq e$, the number of corresponding c is $\varphi(p^{e-f})$, since such c are described as up^f for $u \in (\mathbf{Z}/p^e\mathbf{Z})^\times$, where u, u' determine the same c exactly when $u - u'$ is in the additive subgroup $p^{e-f}\mathbf{Z}/p^e\mathbf{Z}$. Hence

$$|M_{p^e}/\sim'_{p^e}| = \sum_{f=0}^{e} \varphi(p^{e-f})\varphi(p^f),$$

and taking the product over all $p^e | N$, we get

$$|M_N/\sim'| = \sum_{d|N} \varphi(d)\varphi(N/d).$$

Thus, by Lemma 4.2.9 and the above discussion, for $N \geq 5$, we have

$$v_\infty(\Gamma_1(N)) = |\Gamma_1(N)\backslash\Gamma(1)/\Gamma(1)_\infty| = \frac{1}{2}\sum_{d|N} \varphi(d)\varphi(N/d).$$

More importantly,

Proposition 4.2.12. For $N \geq 5$, the genus of $X_1(N)$ is

$$g(X_1(N)) = 1 + \frac{N^2 \prod_{p|N} (1 - (1/p^2))}{24} - \frac{\sum_{d|N} \varphi(d)\varphi(N/d)}{4}. \tag{4.2.3}$$

For $N = 4$, the genus is calculated by replacing the last term above with $3/2$, so $g(X_1(4)) = 0$. One can further compute that $g(X_1(N)) = 0$ for $4 \leq N \leq 10$ and $N = 12$, and it equals 1 for $N = 11$ and 2 for $N = 13$. As mentioned in the introduction, these computations have arithmetic significance: the cases where $g(X_1(N)) = 0$ are exactly those

values of $N \geq 4$ for which there are "one-parameter algebraic families" (in Tate normal form) consisting of an elliptic curve over $\mathbf{Q}$ with a point of exact order N. Much deeper, as Ogg conjectured [22], for other $N \geq 4$ there are *no* elliptic curves E over $\mathbf{Q}$ with a point $P \in E(\mathbf{Q})$ of exact order N. We will not prove this, but rather focus on the case when $N = 13$ in the following section.

5 Points of Order 13

In this section, we will consider $Y_1(N)$ and $X_1(N)$ as schemes over $\mathbf{Q}$, unless otherwise mentioned. We now come to the main result of this thesis:

Theorem 5.0.1 (Mazur-Tate)**.** There is no elliptic curve over $\mathbf{Q}$ with a rational point of order 13.

Equivalently, we need to show that $Y_1(13)(\mathbf{Q})$ is empty, or that $X_1(13)(\mathbf{Q})$ contains no non-cusp points. We will closely follow the paper [19] of Mazur and Tate with help from Lecture 22 of [27], filling in extra details when necessary, but also taking some "standard" facts as black boxes.

5.1 Preliminaries

We fix some notation. For an algebraic closure $\overline{\mathbf{Q}}$ of $\mathbf{Q}$, set $G := \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. Also, for an integer $N \geq 4$, set $K := \mathbf{Q}(\zeta_N)$, so there is a canonical isomorphism $\mathrm{Gal}(K/\mathbf{Q}) \cong (\mathbf{Z}/N\mathbf{Z})^\times$. Write Γ for the group $(\mathbf{Z}/N\mathbf{Z})^\times/\{\pm 1\}$, so Γ is the Galois group of the maximal real subfield $K^+ := \mathbf{Q}(\zeta_N + \zeta_N^{-1})$ of K (note that $[K : K^+] = 2$, and K^+ is the fixed field of $\{\pm 1\}$). For $m \in (\mathbf{Z}/N\mathbf{Z})^\times$ (resp. an automorphism α in G or $\mathrm{Gal}(K/\mathbf{Q})$, considering $\mathrm{Gal}(K/\mathbf{Q})$ as a quotient of G), write γ_m (resp. γ_α) for its image in Γ.

We now define an action of Γ on $X := X_1(N)_{\mathbf{Q}}$. For $\alpha \in (\mathbf{Z}/N\mathbf{Z})^\times$, we define a functor on isomorphism classes of pairs (E, P) (where E is an elliptic curve over a $\mathbf{Q}$-scheme S and $P \in E(S)$ has exact order N) by sending (E, P) to $(E, \alpha P)$. This defines compatible actions of $(\mathbf{Z}/N\mathbf{Z})^\times$ on the set of points $Y_1(N)(S)$ for any $\mathbf{Q}$-scheme S, so it defines an action on $Y := Y_1(N)_{\mathbf{Q}}$ and then extends to an action on X. But $(E, P) \cong (E, -P)$ by the inversion map, and the moduli problem represented by Y does not distinguish isomorphic pairs (E, P), so in fact the action factors through to an action of Γ on X over $\mathbf{Q}$.

On the other hand, we may describe a family of automorphisms of X_K over K, namely the *Atkin-Lehner* involutions, as follows. Fix a primitive Nth root of unity $\zeta \in K$. Then for a K-scheme S and an elliptic curve $E \to S$ equipped with $P \in E[N](S)$ of exact order N (so $\langle P \rangle \cong \mathbf{Z}/N\mathbf{Z}$ as S-groups), there is a short exact sequence of S-group schemes

$$0 \to \mathbf{Z}/N\mathbf{Z} \to E[N] \to \mu_{N,S} \to 0, \tag{5.1.1}$$

which is the quotient identification via the N-torsion Weil pairing [15, 2.8.5]. Our choice of $\zeta \in \mu_{N,S}(S')$ with fiberwise order N can be lifted to $Q \in E[N](S')$ satisfying $\langle P, Q\rangle_{E,N} = \zeta$ for an étale cover $S' \to S$, and this lift is well-defined and unique up to $\langle P\rangle$. We define τ_ζ as the map $X_K \to X_K$ given on S-points of Y_K by

$$(E, P) \to (E/\langle P\rangle, \zeta = Q \bmod \langle P\rangle),$$

and extended via isomorphism functoriality of the smooth compactification X_K over K. We see that $\tau_\zeta = \tau_{\zeta^{-1}}$, since inversion defines an isomorphism $(E/\langle P\rangle, \zeta) \cong (E/\langle P\rangle, \zeta^{-1})$.

We claim that the τ_ζ interact with the γ_m on X_K, where $m \in (\mathbf{Z}/N\mathbf{Z})^\times$, via the following rules:

$$(\tau_\zeta)^2 = 1, \quad \gamma_m\tau_\zeta = \tau_{\zeta^m}, \quad \tau_\zeta\gamma_m(\tau_\zeta)^{-1} = (\gamma_m)^{-1}. \tag{5.1.2}$$

By continuity and reducedness, it suffices to check these identities on points $x \in Y(\overline{\mathbf{Q}})$, where x corresponds to a pair (E, P) consisting of an elliptic curve E over $\overline{\mathbf{Q}}$ and a point P of exact order N. Using the notation of the previous paragraph for the action of τ_ζ, $\tau_\zeta(x)$ corresponds to a pair $(E/\langle P\rangle, Q)$ with $\langle P, Q\rangle_{E,N} = \zeta$. To check that $(\tau_\zeta)^2 = 1$, pick $P' \in E(\overline{\mathbf{Q}})$ such that $NP' = P$, which is unique up to $E[N] = \langle P, Q\rangle$ (the subgroup scheme generated by P and Q). Then we claim $(\tau_\zeta)^2$ acts as

$$(E, P) \mapsto (E/\langle P\rangle, Q) \mapsto (E/\langle P, Q\rangle, -P') = (E/E[N], -P') \xrightarrow[\sim]{\cdot N} (E, -P) \cong (E, P).$$

Indeed, since $E \to E/\langle P\rangle$ is an isogeny with $NP' \in \ker(f)$, adjointness of the Weil pairing for elliptic curves over an algebraically closed field [26, III.8.2] gives

$$\langle Q, NP'\rangle_{E,N} = \langle f(Q), f(P')\rangle_{E/\langle P\rangle,N},$$

so $\langle Q, -P'\rangle_{E/\langle P\rangle,N} = \langle Q, -P\rangle_{E,N} = \langle P, Q\rangle_{E,N} = \zeta$.

For the second equality $\gamma_m\tau_\zeta = \tau_{\zeta^m}$ in (5.1.2), we note that $\langle P, mQ\rangle_{E,N} = \zeta^m$, so both sides of the desired equality send (E, P) to $(E/\langle P\rangle, mQ)$. Finally, the third equality rearranges as $\tau_\zeta\gamma_m = \gamma_{m^{-1}}\tau_\zeta$, since $(\gamma_m)^{-1} = \gamma_{m^{-1}}$. But $\langle mP, m^{-1}Q\rangle_{E,N} = \zeta$, so $\tau_\zeta\gamma_m$ acts on (E, P) as

$$(E, P) \mapsto (E, mP) \mapsto (E/\langle P\rangle, m^{-1}Q).$$

On the other hand, $\gamma_{m^{-1}}\tau_\zeta$ acts on (E, P) as

$$(E, P) \mapsto (E/\langle P\rangle, Q) \mapsto (E/\langle P\rangle, m^{-1}Q),$$

so indeed $\tau_\zeta\gamma_m = \gamma_{m^{-1}}\tau_\zeta$.

We now combine our two families of automorphisms, given by the γ_m's and the τ_ζ's, into a group acting on X_K. Indeed, define a formal symbol τ_ζ for each primitive Nth root of

unity ζ, and set $\tau_\zeta = \tau_{\zeta^{-1}}$. Let Δ be the group defined by the generating set $\Gamma \cup \{\tau_\zeta\}_{\zeta \in \mu_N^\times(K)}$ with the relations of (5.1.2), where $\mu_N^\times(K)$ denotes the set of primitive Nth roots of unity. One can check that Δ acts on X_K and that the map of groups $\Gamma \to \Delta$ is injective with image of index 2, where the τ_ζ's are the elements of the non-trivial coset.

We now describe an action of G, descending through $\mathrm{Gal}(K^+/\mathbf{Q})$, on Δ: for $\alpha \in G$,

$$\alpha(\gamma_m) = \gamma_m, \quad \alpha(\tau_\zeta) = \tau_{\zeta^\alpha} = \gamma_\alpha \tau_\zeta,$$

where we define $\zeta^\alpha := \alpha(\zeta)$ (a power of ζ). This respects the relations in (5.1.2), so it extends to an action on the group Δ.

Proposition 5.1.1. For $\delta \in \Delta$, $\alpha \in G$, and $x \in X(\overline{\mathbf{Q}})$,

$$\alpha(\delta \cdot x) = \alpha(\delta) \cdot (\alpha(x)).$$

Proof. By continuity, we may take $x \in Y(\overline{\mathbf{Q}})$, which corresponds to a pair (E, P) consisting of an elliptic curve E over $\overline{\mathbf{Q}}$ and a point P of exact order N. If $\delta = \gamma_m \in \Gamma$, then $\alpha(\delta \cdot x)$ corresponds to $(\alpha(E), \alpha(mP))$ and $\alpha(\delta) \cdot (\alpha(x)) = \delta \cdot (\alpha(x))$ corresponds to $(\alpha(E), m\alpha(P))$, where $\alpha(E)$ denotes the base change by α. These are of course the same pair, since the group law commutes with base change.

If $\delta = \tau_\zeta \notin \Gamma$, then $\alpha(\delta \cdot x)$ corresponds to $(\alpha(E/\langle P \rangle), \alpha(Q))$, where $\langle P, Q \rangle_{E,N} = \zeta$, and $\alpha(\delta) \cdot (\alpha(x)) = \tau_{\zeta^\alpha} \cdot (\alpha(x))$ corresponds to $(\alpha(E)/\langle \alpha(P) \rangle, Q')$, where $\langle \alpha(P), Q' \rangle_{E,N} = \zeta^\alpha$. Galois-compatibility and perfectness of the Weil pairing [26, III.8.1(d)] forces $Q' = \alpha(Q)$ up to $\langle P \rangle$, so the natural isomorphism $\alpha(E/\langle P \rangle) \cong \alpha(E)/\langle \alpha(P) \rangle$ does the job. □

In the remaining discussion, we will only ever need the actions of elements in $\Delta - \Gamma$ on $X_{\overline{\mathbf{Q}}}$, but we *will* need the action of Γ on X (over $\mathbf{Q}$).

In the remainder of this subsection, we briefly recall some facts about Jacobians, stating the key results in [21, Sections 0.5, 6.1]. Let X be a flat, proper scheme over a locally Noetherian base S with geometrically integral fibers, and suppose there is a fixed section $e \in X(S)$. We define the relative Picard functor on S-schemes as follows:

$$\mathbf{Pic}_{X/S}(T) := \{\text{isomorphism classes of pairs } (\mathcal{L}, \alpha), \text{ where } \mathcal{L} \text{ is an invertible sheaf on } X_T \\ \text{and } \alpha \text{ is an isomorphism } e_T^*(\mathcal{L}) \cong \mathcal{O}_T, \text{ equipped with the evident group structure}\}.$$

This functor is in fact representable by an S-group scheme $\mathrm{Pic}_{X/S}$ locally of finite type, called the *relative Picard scheme*. We will now specialize to the case when $S = \mathrm{Spec}(k)$ for a field k. The key result is:

Theorem 5.1.2. If X is smooth of dimension 1 then the identity component $\mathrm{Pic}^0_{X/k}$ is projective and smooth, with dimension equal to $\dim_k H^1(X, \mathcal{O}_X)$. Moreover, it is naturally self-dual as an abelian variety. There is also canonical k-morphism $X \to \mathrm{Pic}^0_{X/k}$, described on field-valued points $p \in X(k')$ by $p \mapsto [p] - [e_{k'}]$.

For X a curve of genus g over k, we set $J(X) \coloneqq \mathrm{Pic}^0_{X/k}$, and call it the *Jacobian variety* of X. The image $X(\overline{k}) \to J(X)(\overline{k})$ can be shown to generate $J(X)(\overline{k})$, and $J(X)(\overline{k})$ is identified with $\mathrm{Div}^0(X_{\overline{k}})/\overline{k}(X)^\times$, the group of degree-zero divisors of $X_{\overline{k}}$ up to linear equivalence.

5.2 The Curve $X_1(13)$ and its Jacobian

From now on, we take $N = 13$, so $K = \mathbf{Q}(\zeta_{13})$, $K^+ = \mathbf{Q}(\zeta_{13}+\zeta_{13}^{-1})$, and $\Gamma = (\mathbf{Z}/13\mathbf{Z})^\times/\{\pm 1\}$ is cyclic of order 6 and is generated by γ_2. Moreover, $\Delta \cong D_6$. Write $X \coloneqq X_1(13)$ and $Y \coloneqq Y_1(13)$ (remember that these are schemes over $\mathbf{Q}$ unless otherwise specified), so X is a genus 2 curve by the discussion in Section 4.2. It also has 12 cusps in its complex-analytic model $X_{\mathbf{C}}$, and we will require the following fact:

Fact 5.2.1. The 12 (geometric) cusps of X consist of 6 cusps rational over $\mathbf{Q}$ and 6 cusps rational over K^+. The group Γ acts cyclically on each of these subsets of 6 cusps, and Δ acts freely on the set of all cusps.

To prove the first statement, one uses the interpretation of X as the moduli space of generalized elliptic curves with a point of exact order 13, as described in [7]. We now give some details as to what this means. By "generalized elliptic curve," we mean $f : E \to S$, where S is a Noetherian $\mathbf{Q}$-scheme, such that:

1. The map f is proper, flat, and has connected and reduced geometric fibers with dimension 1 and arithmetic genus 1.

2. There is a section $e \in E^{\mathrm{sm}}(S)$ into the smooth locus of f, and a group law on (E^{sm}, e) with an action $E^{\mathrm{sm}} \times E \to E$ extending the group law.

A *point of exact order* N on a generalized elliptic curve over S is an S-homomorphism $\mathbf{Z}/N\mathbf{Z} \hookrightarrow E^{\mathrm{sm}}$ from the constant S-group scheme $(\mathbf{Z}/N\mathbf{Z})$ into the smooth locus, fiberwise of exact order N, such that the image meets all irreducible components of any geometric fiber $E_{\overline{s}}$ (an "ampleness" condition). Of course, if $E \to S$ is already smooth, then the above recovers the original Definitions 2.0.1 and 3.1.1 (the latter since $E_{\overline{s}}$ is irreducible when it is smooth).

The key fact is that such generalized elliptic curves over $\mathbf{C}$ with a point of exact order N have the structure of a "d-gon", where $d|N$. Here, we think of a d-gon as d copies of $\mathbf{P}^1_S$, where ∞ on the ith copy of $\mathbf{P}^1$ is glued to 0 on the $(i+1)$st copy (with the dth copy glued to the 1st). Suppose $N = p \geq 5$ is prime, so there are only two choices for d. Moreover, on the p-gon, there are (up to its geometric automorphism group) $(p-1)/2$ non-isomorphic choices of an exact order-p point, and these can be realized over $\mathbf{Q}$, giving rise to $(p-1)/2$ $\mathbf{Q}$-rational cusps on $X_1(p)$. On the 1-gon, there are $(p-1)/2$ non-isomorphic choices of an exact order-p point, and these correspond to 1 physical point on $X_1(p)$ with residue field

$\mathbf{Q}(\zeta_p)^+$, which splits into $(p-1)/2$ geometric cusps. One can also show that ∞ corresponds to a 1-gon, so it does not arise from a $\mathbf{Q}$-rational cusp, and to find the $(p-1)/2$ non-rational cusps, we can simply act on ∞ by elements of $\Gamma \subset \Delta$ (seen to be pairwise distinct via the moduli interpretation of $X_1(p)$ or via analytic calculation). On the other hand, 0 is *not* in that orbit (as can be seen analytically), so it arises from a $\mathbf{Q}$-rational cusp, and one can find the $(p-1)/2$ rational cusps from its Γ-orbit.

Example 5.2.2. Here is an example illustrating the analytic description of the action of Δ on $Y_{\mathbf{C}}$. Since Δ is generated by γ_2 and τ_ζ where $\zeta := e^{2\pi i/13}$, it suffices to understand the action of these elements on $Y_{\mathbf{C}}$. We see that

$$\gamma_2 \cdot (E_\tau, 1/13) = (E_\tau, 2/13) \cong \left(E_{(7\tau+1)/(13\tau+2)}, 1/13\right),$$

since $2/13$ is the same as $(13/13)\tau + 2/13$ in E_τ, so γ_2 is induced by $\begin{bmatrix} 7 & 1 \\ 13 & 2 \end{bmatrix}$ on $\mathbf{H}$. For τ_ζ, we need the fact that $\langle 1/13, \tau/13\rangle_{E_\tau,13} = \zeta$, so

$$\tau_\zeta \cdot (E_\tau, 1/13) = (\mathbf{C}/(\Lambda_\tau + 1/13\mathbf{Z}), \tau/13) \cong (E_{13\tau}, \tau) \cong \left(E_{-1/(13\tau)}, 1/13\right),$$

where the first isomorphism is given by multiplication by 13, and the second isomorphism is given by multiplication by $-1/(13\tau)$ (since $-1/(13\tau) \in \mathbf{H}$) and inversion. Hence, τ_ζ is induced by $\begin{bmatrix} 0 & 1 \\ -13 & 0 \end{bmatrix}$ on $\mathbf{H}$.

Now, X is a genus 2 curve, so by Theorem 5.1.2, its Jacobian J is an abelian variety of dimension 2. We will need the following fact:

Fact 5.2.3. The Jacobian J has good reduction at all primes $p \neq 13$.

This rests on using the integral theory of generalized elliptic curves in [7] to build $X_1(N)$ as a $\mathbf{Z}[1/N]$-scheme that is smooth and proper, for $N \geq 5$.

Let $P_1, \ldots, P_6$ be the six rational cusps in $X(\mathbf{Q})$. Then we have the following theorem, due to Ogg [23]:

Theorem 5.2.4. For each $i \neq j$, the nonzero divisor class $[P_i] - [P_j] \in J(\mathbf{Q})$ is of order 19, and these each generate the same subgroup T of $J(\mathbf{Q})_{\text{tors}} \subseteq J(\mathbf{Q})$. Moreover, the image of $X(\mathbf{Q})$ in $J(\mathbf{Q})$ via the embedding $P \mapsto [P] - [P_6]$ intersects T at only those 6 points $[P_i] - [P_6]$.

Since this is proved using analytic methods, we will postpone the proof to Section 5.4. On the other hand, given this result, we can prove:

Proposition 5.2.5. The group $J(\mathbf{Q})_{\text{tors}}$ is cyclic of order 19, so is equal to T.

Proof. For this proof, we use the fact that there exists a proper smooth scheme X over $\mathbf{Z}[1/13]$ with generic fiber $X_{\mathbf{Q}}$ and having $Y \coloneqq Y_1(13)$ over $\mathbf{Z}[1/13]$ as an open subscheme. Thus, $A \coloneqq \mathrm{Pic}^0_{X/\mathbf{Z}[1/13]}$ is an abelian scheme over $\mathbf{Z}[1/13]$ with generic fiber J (in particular, it is the Néron model of J over $\mathbf{Z}[1/13]$). Now, by the Hasse bound [26, V.1.1] that

$$||E(\mathbf{F}_q)| - q - 1| \leq 2\sqrt{q}$$

for an elliptic curve $E/\mathbf{F}_q$, we see that there are no elliptic curves over $\mathbf{F}_2$, $\mathbf{F}_3$, $\mathbf{F}_4$ with a point of exact order 13. Hence $Y(\mathbf{F}_q)$ is empty for $q = 2, 3, 4$. On the other hand, by Proposition A.3, there is a unique elliptic curve E over $\mathbf{F}_9$ with a point of exact order 13, and $\mathrm{Aut}_{\mathbf{F}_9}(E) \cong \mathbf{Z}/6\mathbf{Z}$. Since $E(\mathbf{F}_9)$ must contain exactly 12 points of exact order 13 (otherwise violating the Hasse bound, since $|E(\mathbf{F}_9)| \in 13\mathbf{Z}$), this gives $12/6 = 2$ points on $Y(\mathbf{F}_9)$.

Now, using the moduli-theoretic interpretation of X, for *any* field k with $\mathrm{char}(k) \neq 13$, the discussion over $\mathbf{Q}$ after Fact 5.2.1 adapts over k to build exactly 6 non-isomorphic pairs of 13-gons over k with a point of exact order 13. Moreover, there are no 1-gon k-rational cusps when $\mu_{13}(k) = 1$. Thus, there are exactly 6 cusps of $X(\mathbf{F}_q)$ for $q = 2, 3, 4, 9$, so $|X(\mathbf{F}_q)| = 6$ for $q = 2, 3, 4$, and $|X(\mathbf{F}_9)| = 6 + 2 = 8$.

Pick a prime power q not divisible by 13. We now claim the following identity:

$$|A(\mathbf{F}_q)| = -q + \frac{1}{2}|X(\mathbf{F}_{q^2})| + \frac{1}{2}|X(\mathbf{F}_q)|^2. \tag{5.2.1}$$

To prove this, write $V \coloneqq H^1_{\text{ét}}(X_{\overline{\mathbf{F}}_q}, \mathbf{Q}_l)$ for a prime $l \nmid q$, so V is a 4-dimensional vector space over $\mathbf{Q}_l$ (as X has genus 2). By the Lefschetz fixed-point theorem and the fact that $X_{\mathbf{F}_q}$ (resp. $A_{\mathbf{F}_q}$) has dimension 1 (resp. 2), we have

$$|X(\mathbf{F}_q)| = \sum_{i=0}^{2} (-1)^i \mathrm{tr}(F, H^i_{\text{ét}}(X_{\overline{\mathbf{F}}_q}, \mathbf{Q}_l)),$$

$$|X(\mathbf{F}_{q^2})| = \sum_{i=0}^{2} (-1)^i \mathrm{tr}(F^2, H^i_{\text{ét}}(X_{\overline{\mathbf{F}}_q}, \mathbf{Q}_l)),$$

and

$$|A(\mathbf{F}_q)| = \sum_{i=0}^{4} (-1)^i \mathrm{tr}(F, H^i_{\text{ét}}(A_{\overline{\mathbf{F}}_q}, \mathbf{Q}_l)),$$

where $F = \mathrm{Frob}_q$ is the q-Frobenius morphism $x \mapsto x^q$. We will need the following additional facts:

Fact 5.2.6. The vector space $H^2_{\text{ét}}(X_{\overline{\mathbf{F}}_q}, \mathbf{Q}_l)$ is 1-dimensional, on which F acts as multiplication by q.

Fact 5.2.7. Via the cup product, $H^i_{\text{ét}}(A_{\overline{\mathbf{F}}_q}, \mathbf{Q}_l) \cong \bigwedge^i (H^1_{\text{ét}}(X_{\overline{\mathbf{F}}_q}, \mathbf{Q}_l)) = \bigwedge^i (V)$.

Fact 5.2.8. The map $\alpha \mapsto q/\alpha$ is a bijection from the multiset of eigenvalues of F on V to itself (this is due to "qF^{-1} being dual to F").

From Facts 5.2.6 and 5.2.7, we conclude that

$$|X(\mathbf{F}_q)| = 1 - \operatorname{tr}(F|V) + q,$$
$$|X(\mathbf{F}_{q^2})| = 1 - \operatorname{tr}(F^2|V) + q^2,$$

and

$$|A(\mathbf{F}_q)| = \sum_{i=0}^{4} (-1)^i \operatorname{tr}(F, \bigwedge^i V).$$

Now, F has 4 eigenvalues $a, b, q/a, q/b$ on V by Fact 5.2.8, so the eigenvalues of F^2 on V are $a^2, b^2, (q/a)^2, (q/b)^2$, and the eigenvalues of F on $\bigwedge^i V$ are the i-fold products without repetition from the 4-tuple $(a, b, q/a, q/b)$. It follows that

$$\begin{aligned}
|A(\mathbf{F}_q)| &= (1-a)(1-b)(1-(q/a))(1-(q/b)) \\
&= \frac{1}{2}\left(-2q + \left(1 + q - \left(a^2 + b^2 + \left(\frac{q}{a}\right)^2 + \left(\frac{q}{b}\right)^2\right)\right) + \left(1 + q - \left(a + b + \frac{q}{a} + \frac{q}{b}\right)\right)^2\right) \\
&= -q + \frac{1}{2}|X(\mathbf{F}_{q^2})| + \frac{1}{2}|X(\mathbf{F}_q)|^2.
\end{aligned}$$

We conclude that $|A(\mathbf{F}_2)| = 19$ and $|A(\mathbf{F}_3)| = 19$. Now, note that for $p = 2, 3$, we have a natural group homomorphism $A(\mathbf{Q})_{\text{tors}} \hookrightarrow A(\mathbf{Q}) = A(\mathbf{Z}_{(p)}) \to A(\mathbf{F}_p)$ given by reduction, where the equality is given by the valuative criterion of properness. By Lemma A.5 and the fact that $A(\mathbf{Q})[ab] \cong A(\mathbf{Q})[a] \times A(\mathbf{Q})[b]$ inside $A(\mathbf{Q})_{\text{tors}}$ for coprime integers a, b, the reduction map

$$A(\mathbf{Q})_{\text{tors}} \to A(\mathbf{F}_p) \cong \mathbf{Z}/19\mathbf{Z} \tag{5.2.2}$$

is injective on prime-to-p-torsion. Since $A(\mathbf{Q})_{\text{tors}}$ contains a subgroup of order 19, and $A(\mathbf{Q})[19^\infty] \to A(\mathbf{F}_p)$ is injective for $p \neq 13, 19$, the map (5.2.2) with $p = 2$ shows that there is no nonzero l-torsion of $A(\mathbf{Q})$ for prime $l \neq 2, 19$, whence $|A(\mathbf{Q})[19^\infty]| \leq 19$. Similarly, the map with $p = 3$ shows that there is no nonzero 2-torsion, so $J(\mathbf{Q})_{\text{tors}} = A(\mathbf{Q})_{\text{tors}} \cong \mathbf{Z}/19\mathbf{Z}$. □

Hence, to prove Theorem 5.0.1, it suffices to prove:

Theorem 5.2.9. The group $J(\mathbf{Q})$ (a finitely generated abelian group by the Mordell-Weil Theorem) has rank 0.

Indeed, then $J(\mathbf{Q}) = J(\mathbf{Q})_{\text{tors}} = T$ by Proposition 5.2.5, so

$$X(\mathbf{Q}) = X(\mathbf{Q}) \cap J(\mathbf{Q}) = X(\mathbf{Q}) \cap T,$$

and $X(\mathbf{Q}) \cap T$ consists of only the 6 rational cusps by Theorem 5.2.4. Hence, $Y(\mathbf{Q})$ is empty.

We now must investigate the structure of J in more detail.

Proposition 5.2.10. The abelian variety J is $\mathbf{Q}$-simple (i.e. it doesn't contain a proper nonzero abelian subvariety over $\mathbf{Q}$).

Proof. If not, then we could write an exact sequence

$$0 \to J_1 \to J \to J_2 \to 0$$

of abelian varieties over $\mathbf{Q}$, where J_1 and J_2 are elliptic curves. Since $J(\mathbf{Q})$ has a nonzero 19-torsion point, one of J_1 or J_2, say J_i, must have a rational point P of order 19. By the Néron-Ogg-Shafarevich criterion for good reduction, J_i has good reduction away from 13, as J does [25, Corollary 3]. Hence the natural reduction map $J_i(\mathbf{Q})[19] \to \overline{J_i}(\mathbf{F}_2)$ is an injection [26, VII.3.1]. But the Hasse bound tells us that an elliptic curve over $\mathbf{F}_2$ has at most 5 $\mathbf{F}_2$-rational points, so $\overline{J_i}(\mathbf{F}_2)$ cannot have a point of order 19. □

Now, note that J is contravariantly functorial in X via pullback of line bundles. On the other hand, J is also *covariantly* functorial in X via *norm* of line bundles [9, 6.5], which is the relative version of pushforward of divisors on curves over algebraically closed fields. In particular, for a finite map of $\overline{\mathbf{Q}}$-curves $\varphi : X' \to Y'$, the norm associated to φ acts on points $P \in X'(\overline{\mathbf{Q}})$ as $N(\mathscr{I}_P) = \mathscr{I}_{\varphi(P)}$, which becomes the familiar map $\sum n_i P_i \mapsto \sum n_i \varphi(P_i)$ on Weil divisors. In this way, the (left) action of Γ on X described in Section 5.1 induces an action on J, given on $\overline{\mathbf{Q}}$-points by the aforementioned map of divisors.

Consider the generator γ_2 of $\Gamma = (\mathbf{Z}/13\mathbf{Z})^\times/\{\pm 1\} \cong \mathbf{Z}/6\mathbf{Z}$, which acts on X with order 6 (as one sees from the action on geometric points) and so also acts with order 6 on J, since the Jacobian functoriality is faithful for positive genus. We want to consider the "minimal polynomial" of the action of γ_2 on J. We know that γ_2 satisfies $x^6 - 1$, which factors into irreducibles over $\mathbf{Q}$ as

$$x^6 - 1 = (x-1)(x+1)(x^2+x+1)(x^2-x+1).$$

By Lemma A.6, we see that γ_2 satisfies the polynomial $x^2 - x + 1$, since it does not satisfy any of the other irreducible polynomials (which are factors of $x^n - 1$ for $n = 1, 2, 3$).

Via the action of Δ on $X_{\overline{\mathbf{Q}}}$, by covariant functoriality of J in X, Δ induces an action of the quotient ring $D \coloneqq \mathbf{Z}[\Delta]/(\gamma_2^2 - \gamma_2 + 1)$ on $J_{\overline{\mathbf{Q}}}$. One can check that D is a free $\mathbf{Z}$-module with $D \otimes_{\mathbf{Z}} \mathbf{Q} \cong M_2(\mathbf{Q})$ (the algebra of 2-by-2 matrices over $\mathbf{Q}$), and that the subring $\mathbf{Z}[\gamma_2]$ of D is isomorphic to $\mathbf{Z}[\omega]$ via $\gamma_2 \mapsto -\omega$, where ω is a primitive cube root of unity. Moreover:

Proposition 5.2.11. The action of D on $J_{\overline{\mathbf{Q}}}$ is faithful.

Proof. For a fixed prime l, write T_l for the l-adic Tate module of $J_{\overline{\mathbf{Q}}}$, and write V_l for $T_l[1/l]$, which is a $\mathbf{Q}_l$-module. Then there is a $\mathbf{Z}$-algebra map $\mathrm{End}_{\overline{\mathbf{Q}}}(J_{\overline{\mathbf{Q}}}) \to \mathrm{End}_{\mathbf{Q}_l}(V_l)$ (which is injective; see [5, 7.6.7]), and by the action of D on J, we also have a $\mathbf{Z}$-algebra map $D \to \mathrm{End}_{\overline{\mathbf{Q}}}(J_{\overline{\mathbf{Q}}})$. Upon tensoring the composite map against $\mathbf{Q}$, we get a $\mathbf{Q}$-algebra map $D_{\mathbf{Q}} \to \mathrm{End}_{\mathbf{Q}_l}(V_l)$. Since $D_{\mathbf{Q}} \cong M_2(\mathbf{Q})$ is a *simple* $\mathbf{Q}$-algebra, this latter map is injective. Then we get a commutative diagram

$$\begin{array}{ccc} D & \longrightarrow & D_{\mathbf{Q}} \\ \downarrow & & \downarrow \\ \mathrm{End}_{\overline{\mathbf{Q}}}(J_{\overline{\mathbf{Q}}}) & \longrightarrow & \mathrm{End}_{\mathbf{Q}_l}(V_l) \end{array}$$

where the top and right arrows are injective (the former since D is $\mathbf{Z}$-free). Hence the map $D \to \mathrm{End}_{\overline{\mathbf{Q}}}(J_{\overline{\mathbf{Q}}})$ is injective as well.

□

Define $V \coloneqq J[19](\overline{\mathbf{Q}})$ to be the G-module of 19-torsion points in J, so $V \cong (\mathbf{Z}/19\mathbf{Z})^{\oplus 4}$. We also have an action of Δ on $J_{\overline{\mathbf{Q}}}$ via covariant functoriality that is G-compatible on $\overline{\mathbf{Q}}$-points in the sense of Proposition 5.1.1, since the $\mathbf{Q}$-map $X \to J$ via a $\mathbf{Q}$-cusp yields a Δ-compatible map $X_{\overline{\mathbf{Q}}} \to J_{\overline{\mathbf{Q}}}$ and a G-compatible map $X(\overline{\mathbf{Q}}) \to J(\overline{\mathbf{Q}})$ whose image generates $J(\overline{\mathbf{Q}})$. In particular, V is a module over $\mathbf{Z}[\gamma_2] \cong \mathbf{Z}[\omega] \subseteq D$.

Note that 19 splits in $\mathbf{Z}[\gamma_2]$ since $x^2 - x + 1 \equiv (x-8)(x-12) \bmod 19$, and since $\mathbf{Z}[\gamma_2]$ is a PID, we can write $19 = \pi\overline{\pi}$ for a prime $\pi \in \mathbf{Z}[\gamma_2]$. Let V_π (resp. $V_{\overline{\pi}}$) be the kernel of the action of π (resp. $\overline{\pi}$) on V. Then $V = V_\pi \oplus V_{\overline{\pi}}$: since π and $\overline{\pi}$ generate 1, the Chinese remainder theorem gives an isomorphism

$$\mathbf{Z}[\gamma_2]/(19) \cong \mathbf{Z}[\gamma_2]/(\pi) \times \mathbf{Z}[\gamma_2]/(\overline{\pi}),$$

so the $\mathbf{Z}[\gamma_2]/(19)$-module V splits into a direct sum as claimed.

Note that π and $\overline{\pi}$ are integer combinations of γ_2 and 1. Clearly γ_2 commutes with all elements of Γ (being cyclic) and G (as Γ acts on J over $\mathbf{Q}$), so the subspaces V_π and $V_{\overline{\pi}}$ are stable under the Γ and G-actions. On the other hand, for any τ_ζ, we have $\tau_\zeta \gamma_2 (\tau_\zeta)^{-1} = (\gamma_2)^{-1}$ and $\omega^{-1} = \overline{\omega}$, so conjugation by τ_ζ swaps π and $\overline{\pi}$. Hence it also swaps V_π and $V_{\overline{\pi}}$, which means they must both be dimension 2 inside the 4-dimensional space V.

Proposition 5.2.12. Under the self-duality of V via the Weil pairing and autoduality of J, V_π and $V_{\overline{\pi}}$ are isotropic (i.e. self-annihilating) and hence are dual to each other as G-modules.

Proof. Recall that we factored $19 = \pi\overline{\pi}$ in $\mathbf{Z}[\gamma_2]$, where γ_2 plays the role of a primitive 6th root of unity. In terms of prime ideals, this is the factorization $(19) = (19, \gamma_2 - 8)(19, \gamma_2 - 12)$,

as $x^2 - x + 1 \equiv (x-8)(x-12) \bmod 19$ (note that 8 and 12 are primitive 6th roots of unity in $\mathbf{F}_{19}$). Hence, upon swapping π and $\overline{\pi}$ if necessary, $(\gamma_2 - 8) \cdot V_\pi = 0$ and $(\gamma_2 - 12) \cdot V_{\overline{\pi}} = 0$. This says that V_π and $V_{\overline{\pi}}$ are eigenspaces of γ_2 over $\mathbf{F}_{19}$ with eigenvalues $z^{\pm 1}$ for $z = 8$ or $12 \equiv 8^{-1} \bmod 19$. For $u, v \in V_\pi$, we claim

$$\langle u, v \rangle_{J,19} = \langle \gamma_2 \cdot u, \gamma_2 \cdot v \rangle_{J,19} = \langle zu, zv \rangle_{J,19} = (\langle u, v \rangle_{J,19})^{z^2}.$$

The first equality holds by the naturality of the Weil pairing with respect to isomorphisms. Of course, $z^2 \neq 1$ as z has multiplicative order 6, so the only way the above equality is possible is if the 19th root of unity $\langle u, v \rangle_{J,19}$ is trivial. This shows the self-orthogonality of V_π, and the statement for $V_{\overline{\pi}}$ is deduced in the same way. □

Now, let $V(1)$ be the subspace of V given by the cyclic group $T \subseteq J(\mathbf{Q})$ of 19 rational points coming from the cusps of X. By Proposition 5.2.5, $V(1)$ is the entire subset of rational points inside V. Obviously, G acts trivially on $V(1)$, and $V(1)$ is also stable under γ_2 by construction. Hence the *1-dimensional* subspace $V(1)$ must be contained in either V_π or $V_{\overline{\pi}}$, since for nonzero $v \in V(1)$, at least one of $\overline{\pi} \cdot v \in V_\pi$ or $\pi \cdot v \in V_{\overline{\pi}}$ is nonzero and in $V(1)$ (again, both π and $\overline{\pi}$ are integer combinations of γ_2 and 1). Without loss of generality (swapping π and $\overline{\pi}$ if necessary), suppose $V(1)$ is contained in $V_{\overline{\pi}}$.

We lastly define the subspace $V(\gamma)$ to be $\{v \in V : \alpha(v) = \gamma_\alpha \cdot v \text{ for all } \alpha \in G\}$. Recall we defined an action by Δ on $J_{\overline{\mathbf{Q}}}$ by covariant functoriality in $X_{\overline{\mathbf{Q}}}$.

Lemma 5.2.13. The action on V of any $\tau_\zeta \in \Delta$ interchanges $V(1)$ and $V(\gamma)$.

Proof. If $v \in V(1)$ and $\alpha \in G$, we have by Proposition 5.1.1 (adapted to J)

$$\alpha(\tau_\zeta \cdot v) = \alpha(\tau_\zeta) \cdot (\alpha(v)) = \alpha(\tau_\zeta) \cdot v = \gamma_\alpha \cdot (\tau_\zeta \cdot v),$$

where the second equality comes from the fact that v is a $\mathbf{Q}$-rational point. Conversely, if $v \in V(\gamma)$, then

$$\alpha(\tau_\zeta \cdot v) = \alpha(\tau_\zeta) \cdot (\alpha(v)) = (\gamma_\alpha \tau_\zeta) \cdot (\gamma_\alpha \cdot v) = \tau_\zeta \cdot v,$$

since $\gamma_\alpha \tau_\zeta \gamma_\alpha = \tau_\zeta$ (see (5.1.2)). Hence $\tau_\zeta \cdot v \in V(1)$ since it is fixed by all $\alpha \in G$. □

This shows that $V(\gamma)$ has dimension 1, and since $V(1) \subseteq V_{\overline{\pi}}$ yet any τ_ζ swaps V_π and $V_{\overline{\pi}}$, we conclude that $V(\gamma)$ is contained in V_π. This yields:

Remark 5.2.14. The subspaces $V(1)$ and $V(\gamma)$ have vanishing intersection. Thus, the action of G on $V(\gamma)$ is not trivial. This fact will be useful to us later.

It is also now possible to describe the quotient $V_\pi / V(\gamma)$:

Proposition 5.2.15. Write $V(\chi)$ for the G-module of 19th roots of unity, so $V(\chi)$ is an $\mathbf{F}_{19}$-vector space in the canonical way. Then there is a short exact sequence

$$0 \to V(\gamma) \to V_\pi \xrightarrow{b} V(\chi) \to 0 \tag{5.2.3}$$

of G-modules.

Proof. Let us first define the G-module map b. By Proposition 5.2.12, the Weil pairing on V gives a perfect G-equivariant pairing $V_\pi \times V_{\overline{\pi}} \to \mu_{19}$. Via the inclusion $V(1) \hookrightarrow V_{\overline{\pi}}$, we get a surjective map

$$V_\pi \cong \mathrm{Hom}_{\mathbf{F}_{19}}(V_{\overline{\pi}}, \mu_{19}) \twoheadrightarrow \mathrm{Hom}_{\mathbf{F}_{19}}(V(1), \mu_{19}) \cong V(\chi),$$

where the last isomorphism follows from the definitions of $V(1)$ and $V(\chi)$. The composition of the above maps defines the map b.

Going back to the original problem, we are done if $V(\gamma) \subseteq \ker(b)$ by just counting the dimensions. We claim that the G-representations $V(\gamma)$ and $V(\chi)$ are not isomorphic (as representations over $\mathbf{F}_{19}$). On the latter, the G-action factors through $\mathrm{Gal}(\mathbf{Q}(\zeta_{19})/\mathbf{Q})$, which acts faithfully. But on $V(\gamma)$, the action of G factors through $\Gamma = \mathrm{Gal}(K^+/\mathbf{Q})$ by definition, and $\mathbf{Q}(\zeta_{19})$ and $\mathbf{Q}(\zeta_{13})$ have intersection $\mathbf{Q}$. So $V(\gamma)$ and $V(\chi)$ are 1-dimensional non-isomorphic G-representations, so *any* G-equivariant map $V(\gamma) \to V(\chi)$ must be the zero map. In particular $V(\gamma) \subseteq \ker(b)$, as desired. □

5.3 Proof of Theorem 5.2.9

With the previous setup, we are finally in a position to prove Theorem 5.2.9 (and hence establish Theorem 5.0.1). As in the proof of Proposition 5.2.5, we extend J to an abelian scheme A over $\mathbf{Z}[1/13]$, and $A(\mathbf{Z}[1/13]) = J(\mathbf{Q})$ by the valuative criterion for properness over Dedekind domains applied to the diagram

$$\begin{array}{ccc} \mathrm{Spec}(\mathbf{Q}) & \longrightarrow & A \\ \downarrow & \overset{!}{\nearrow} & \downarrow \\ \mathrm{Spec}(\mathbf{Z}[1/13]) & \xrightarrow{=} & \mathrm{Spec}(\mathbf{Z}[1/13]) \end{array}$$

Note that the action of D on J extends to A by the Néron mapping property of abelian schemes over Dedekind domains, and there is a short exact sequence of $\mathbf{Z}[1/13]$-group schemes

$$0 \to F \to A \xrightarrow{\pi} A \to 0, \tag{5.3.1}$$

where π is finite flat (as we may check on fibers over $\mathbf{Z}[1/13]$, using that $\pi|19$), and F is defined as the finite flat kernel A_π. In particular, the generic fiber of F corresponds to $V_\pi \subseteq V$.

To prove Theorem 5.2.9, we claim it suffices to show that:

Proposition 5.3.1. The map π induces a surjection on $A(\mathbf{Z}[1/13]) = J(\mathbf{Q})$.

Indeed, if multipliction by π acts surjectively on $J(\mathbf{Q})$ then so does multiplication by 19, forcing the finitely generated abelian group $J(\mathbf{Q})$ to be finite.

We now consider a commutative diagram with exact rows arising from (5.3.1) over $\mathbf{Z}[1/13]$ and over $\mathbf{Q}$ (we will recall the necessary facts about the fppf cohomology as they are needed):

$$\begin{array}{ccccc} A(\mathbf{Z}[1/13]) & \xrightarrow{\pi} & A(\mathbf{Z}[1/13]) & \xrightarrow{\delta} & H^1_{\mathrm{fppf}}(\mathbf{Z}[1/13], F) \\ \downarrow & & \downarrow & & \downarrow \rho \\ A(\mathbf{Q}_{13}) & \xrightarrow{\pi} & A(\mathbf{Q}_{13}) & \xrightarrow{\delta} & H^1_{\mathrm{fppf}}(\mathbf{Q}_{13}, F) \end{array} \tag{5.3.2}$$

To prove Proposition 5.3.1, the diagram (5.3.2) tells us that it suffices to show the following two statements.

Proposition 5.3.2. The map π induces a surjection on $A(\mathbf{Q}_{13})$.

Proposition 5.3.3. The map $\rho : H^1_{\mathrm{fppf}}(\mathbf{Z}[1/13], F) \to H^1_{\mathrm{fppf}}(\mathbf{Q}_{13}, F)$ is injective.

Proof of Proposition 5.3.2. Extend the abelian variety $J_{\mathbf{Q}_{13}}$ to its (non-proper, but smooth and separated) Néron model A' over $\mathbf{Z}_{13}$. Let N be the kernel of the reduction map $A'(\mathbf{Z}_{13}) \to A'(\mathbf{Z}/13\mathbf{Z})$. We have a diagram of exact sequences

$$\begin{array}{ccccccccc} 0 & \longrightarrow & N & \longrightarrow & A'(\mathbf{Z}_{13}) & \longrightarrow & A'(\mathbf{Z}/13\mathbf{Z}) & \longrightarrow & 0 \\ & & \downarrow \pi & & \downarrow \pi & & \downarrow \pi & & \\ 0 & \longrightarrow & N & \longrightarrow & A'(\mathbf{Z}_{13}) & \longrightarrow & A'(\mathbf{Z}/13\mathbf{Z}) & \longrightarrow & 0 \end{array} \tag{5.3.3}$$

We claim that N is a pro-13 group. Since $A'(\mathbf{Z}_{13}) = \varprojlim_{n\geq 1} A'(\mathbf{Z}_{13}/13^n)$, and inverse limits preserve kernels (being left exact), we see that $N = \varprojlim_{n\geq 1} \ker(A'(\mathbf{Z}_{13}/13^n) \to A'(\mathbf{Z}/13\mathbf{Z}))$. Hence we only need to show that each $\ker(A'(\mathbf{Z}_{13}/13^n) \to A'(\mathbf{Z}/13\mathbf{Z}))$ is a finite (abelian) 13-group. The finiteness is clear, since $\mathbf{Z}_{13}/13^n$ is finite and A' is finite type over $\mathbf{Z}_{13}$. Then Lemma A.5 says that for all primes $l \neq 13$, the map $A'[l](\mathbf{Z}_{13}/13^n) \to A'[l](\mathbf{Z}/13\mathbf{Z})$ is injective, so $\ker(A'(\mathbf{Z}_{13}/13^n) \to A'(\mathbf{Z}/13\mathbf{Z}))$ is a 13-group.

Since N is a pro-13 group, and 19 is prime to 13, clearly $19 = \pi\overline{\pi}$ acts bijectively on N. Hence π also acts bijectively on N. Now, the universal property of Néron models [3, 1.2.1] says that the canonical map

$$A'(\mathbf{Z}_{13}) \to A'_{\mathbf{Q}_{13}}(\mathbf{Q}_{13}) = J_{\mathbf{Q}_{13}}(\mathbf{Q}_{13}) = J(\mathbf{Q}_{13}) = A(\mathbf{Q}_{13})$$

is an isomorphism, so the middle vertical map in (5.3.3) is simply $A(\mathbf{Q}_{13}) \xrightarrow{\pi} A(\mathbf{Q}_{13})$ under this identification. We see via the snake lemma that this is surjective if the right vertical

map $A'(\mathbf{Z}/13\mathbf{Z}) \xrightarrow{\pi} A'(\mathbf{Z}/13\mathbf{Z})$ in (5.3.3) is surjective. But $A'(\mathbf{Z}/13\mathbf{Z})$ is a finite group, so it suffices to prove that π is injective on $A'(\mathbf{Z}/13\mathbf{Z})$. Again by the snake lemma, it in turn suffices to show that $A(\mathbf{Q}_{13}) \xrightarrow{\pi} A(\mathbf{Q}_{13})$, or equivalently $J(\mathbf{Q}_{13}) \xrightarrow{\pi} J(\mathbf{Q}_{13})$, is *injective*. So the goal is to prove that $J[\pi](\mathbf{Q}_{13}) = 0$.

By Lemma A.7 (with $p = 13$) and the $\mathbf{Q}$-finiteness of $J[\pi]$, we see that $J[\pi](\mathbf{Q}_{13})$ is exactly $(V_\pi)^H \coloneqq \{x \in J[\pi](\overline{\mathbf{Q}}) : Hx = x\}$, where $H \subseteq G$ is a decomposition subgroup of G corresponding to 13. Now, recall from Proposition 5.2.15 the short exact sequence (5.2.3)

$$0 \to V(\gamma) \to V_\pi \to V(\chi) \to 0$$

of G-representations over $\mathbf{F}_{19}$. To show that $J[\pi](\mathbf{Q}_{13}) = (V_\pi)^H$ is 0, it suffices to show that $V(\gamma)^H = 0$ and $V(\chi)^H = 0$.

Recall that the action of G on the line $V(\chi)$ descends to a *faithful* action of $\mathrm{Gal}(\mathbf{Q}(\zeta_{19})/\mathbf{Q})$, But $13 \not\equiv 1 \bmod 19$, so 13 doesn't split completely in $\mathbf{Q}(\zeta_{19})$. On the other hand, because H is a decomposition group over 13, the fixed field $L \subseteq \mathbf{Q}(\zeta_{19})$ of H is the largest subextension such that 13 splits completely in L. So $L \neq \mathbf{Q}(\zeta_{19})$, meaning that the image of H in $\mathrm{Gal}(\mathbf{Q}(\zeta_{19})/\mathbf{Q})$ is nontrivial. Hence $V(\chi)^H = 0$.

It remains to show that $V(\gamma)^H = 0$. As $\dim_{\mathbf{F}_{19}} V(\gamma) = 1$ by Lemma 5.2.13, it suffices to show that $V(\gamma)^H \neq V(\gamma)$; i.e. that H doesn't fix all of $V(\gamma)$. By definition of $V(\gamma)$, G acts on $V(\gamma)$ through $\Gamma = \mathrm{Gal}(K^+/\mathbf{Q})$, where $K^+ = \mathbf{Q}(\zeta_{13} + \zeta_{13}^{-1})$. But 13 is ramified in *any non-trivial subextension* of $\mathbf{Q}(\zeta_{13})$, since 13 is the only prime ramified in $\mathbf{Q}(\zeta_{13})$ and it is totally ramified. Hence the fixed field $L \subseteq K^+$ of the image of H in Γ must be $\mathbf{Q}$, which means this image is all of Γ. So if $V(\gamma)^H = V(\gamma)$, the action of G on $V(\gamma)$ would be trivial. But as per Remark 5.2.14, this is not the case. □

It remains to prove that ρ is injective. We know that $\mathbf{Z}[\zeta_{13}]$ is the integral closure of $\mathbf{Z}$ inside $K = \mathbf{Q}(\zeta_{13})$, so $\mathbf{Z}[\zeta_{13}, 1/13]$ is the integral closure of $\mathbf{Z}[1/13]$. The ring map $\mathbf{Z}[1/13] \to \mathbf{Z}[\zeta_{13}, 1/13]$ is étale, since $\mathbf{Q} \to \mathbf{Q}(\zeta_{13})$ is unramified away from 13.

Recall from (5.3.1) that we write F for the finite flat kernel A_π of $\pi : A \to A$ over $\mathbf{Z}[1/13]$.

Lemma 5.3.4. There is a short exact sequence of finite flat $\mathbf{Z}[1/13]$-group schemes

$$0 \to E \to F \to \mu_{19} \to 0, \tag{5.3.4}$$

where the base change of E to the finite étale cover $\mathbf{Z}[\zeta_{13}, 1/13]$ is isomorphic to the constant group scheme $\mathbf{Z}/19\mathbf{Z}$.

This lemma is essentially a "globalization" of Proposition 5.2.15.

Proof. Let E be the Zariski closure of $V(\gamma) \subseteq V_\pi \subseteq J[19]$ in A. Then we claim E is a finite flat closed subgroup scheme of the finite flat F. The subscheme E is clearly finite, since $F = A[\pi]$ is finite. It is also flat, since for any Dedekind domain R with fraction field

K and any flat R-scheme X, the schematic closure in X of any closed subscheme of X_K is R-flat. Moreover, $E \subseteq F$ is a subgroup scheme since $E \times E \to F \times F \xrightarrow{m} F$ factors through the closed immersion $E \hookrightarrow F$ because R-flatness of $E \times E$ allows us to check the claim on $\mathbf{Q}$-fibers, where it is clear.

From Proposition 5.2.15, we see that the quotient F/E over $\mathbf{Z}[1/13]$ has generic fiber $V(\chi) = \mu_{19}$. Also, $E_{\mathbf{Z}[\zeta_{13},1/13]}$ has generic fiber $\mathbf{Z}/19\mathbf{Z}$ as $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}(\zeta_{13}))$-modules, since $V(\gamma) \cong V(1) \cong \mathbf{Z}/19\mathbf{Z}$ by Lemma 5.2.13. It remains to extend the generic fiber isomorphisms $(F/E)_{\mathbf{Q}} \cong \mu_{19}$ and $E_{\mathbf{Q}(\zeta_{13})} \cong \mathbf{Z}/19\mathbf{Z}$ over $\mathbf{Z}[1/13]$ and $\mathbf{Z}[\zeta_{13}, 1/13]$ respectively.

We now consider a local version. Suppose R is a discrete valuation ring with characteristic 0 and fraction field K, but its residue field k has characteristic $p > 0$. Set $e \coloneqq \mathrm{ord}_R(p)$, the absolute ramification index. Consider the functor

$$\begin{aligned} &\{\text{finite flat commutative group schemes } G/R \text{ with } p\text{-power order}\} \\ \to\ &\{\text{finite flat commutative group schemes } H/K \text{ with } p\text{-power order}\} \end{aligned}$$

that sends G to its generic fiber. It is visibly faithful, and a theorem of Raynaud [24, 3.3.6] says that if $e < p - 1$ then the above functor is even fully faithful. Also, from Lemma A.8, we know that the functor

$$\begin{aligned} &\{\text{finite étale commutative group schemes } G/R\} \\ \to\ &\{\text{finite étale commutative group schemes } H/K\} \end{aligned}$$

is fully faithful, where R can be any Dedekind domain.

To apply these facts, let $T \coloneqq \mathbf{Z}[\zeta_{13}, 1/13]$. The T-groups E_T and $(\mathbf{Z}/19\mathbf{Z})_T$ agree on their generic fibers, and we want to extend such an isomorphism over T. We first look at these groups over $T[1/19]$. Let's show that $E_{T[1/19]}$ is étale. Let s be a non-generic point of $\mathrm{Spec}(T[1/19])$, so $\mathrm{char}(k(s)) = p \neq 19$. Then the fiber E_s is a finite flat group scheme over $k(s)$ of order 19, so its tangent space at the identity is killed by both p and 19, the latter being true since the generic fiber of E_T is killed by 19. Hence the tangent space is 0, so E_s is étale over $k(s)$ at the identity and hence everywhere (via translation over $\overline{k(s)}$). So by the fibral étaleness criterion, the finite flat scheme $E_{T[1/19]}$ is étale over $T[1/19]$. The isomorphism of E_T and $\mathbf{Z}/19\mathbf{Z}$ on generic fibers extends to an isomorphism $E_{T[1/19]} \cong (\mathbf{Z}/19\mathbf{Z})_{T[1/19]}$, since $T[1/19]$ is Dedekind.

It remains to understand what happens at primes over 19. At any non-generic point s of $\mathrm{Spec}(T_{(19)})$, $k(s)$ is a field of characteristic 19. Moreover, 19 does not ramify at all in $\mathcal{O}_s$, since the only rational prime ramifying in $\mathbf{Z}[\zeta_{13}]$ is 13. So the absolute ramification index e of $\mathcal{O}_s$ is $1 < 19 - 1$, so the isomorphism of E_T and $\mathbf{Z}/19\mathbf{Z}$ on generic fibers extends to an isomorphism over $\mathcal{O}_{T,s}$. These isomorphisms for such s spread out and agree on overlaps (as we can check at the generic point), so they glue together to an isomorphism $E_T \cong \mathbf{Z}/19\mathbf{Z}$ of T-groups. Note that E is then étale over $\mathbf{Z}[1/13]$ by faithfully flat descent.

The same type of argument applied over $\mathbf{Z}[1/13]$ shows that F/E and μ_{19} are isomorphic as $\mathbf{Z}[1/13]$-groups. □

Now, using that (5.3.4) is short exact for the fppf topology over $\mathbf{Z}[1/13]$, we can draw a commutative diagram with exact rows:

$$\begin{array}{ccccc} H^1_{\mathrm{fppf}}(\mathbf{Z}[1/13], E) & \longrightarrow & H^1_{\mathrm{fppf}}(\mathbf{Z}[1/13], F) & \longrightarrow & H^1_{\mathrm{fppf}}(\mathbf{Z}[1/13], \mu_{19}) \\ & & \downarrow{\scriptstyle \rho} & & \downarrow{\scriptstyle \rho'} \\ & & H^1_{\mathrm{fppf}}(\mathbf{Q}_{13}, F) & \longrightarrow & H^1_{\mathrm{fppf}}(\mathbf{Q}_{13}, \mu_{19}) \end{array} \tag{5.3.5}$$

Hence, to prove ρ is injective as in Proposition 5.3.3, it suffices to show that ρ' is injective and $H^1_{\mathrm{fppf}}(\mathbf{Z}[1/13], E) = 0$.

Lemma 5.3.5. The map $\rho' : H^1_{\mathrm{fppf}}(\mathbf{Z}[1/13], \mu_{19}) \to H^1_{\mathrm{fppf}}(\mathbf{Q}_{13}, \mu_{19})$ is injective.

Proof. Consider the exact sequence

$$0 \to \mu_{19} \to \mathbf{G}_m \xrightarrow{x \mapsto x^{19}} \mathbf{G}_m \to 0$$

of $\mathbf{Z}[1/13]$-group schemes. This induces a commutative diagram with exact rows:

$$\begin{array}{ccccccc} \mathbf{G}_m(\mathbf{Z}[1/13]) & \xrightarrow{x \mapsto x^{19}} & \mathbf{G}_m(\mathbf{Z}[1/13]) & \longrightarrow & H^1_{\mathrm{fppf}}(\mathbf{Z}[1/13], \mu_{19}) & \longrightarrow & H^1_{\mathrm{fppf}}(\mathbf{Z}[1/13], \mathbf{G}_m) \\ \downarrow & & \downarrow & & \downarrow{\scriptstyle \rho'} & & \downarrow \\ \mathbf{G}_m(\mathbf{Q}_{13}) & \xrightarrow{x \mapsto x^{19}} & \mathbf{G}_m(\mathbf{Q}_{13}) & \longrightarrow & H^1_{\mathrm{fppf}}(\mathbf{Q}_{13}, \mu_{19}) & \longrightarrow & H^1_{\mathrm{fppf}}(\mathbf{Q}_{13}, \mathbf{G}_m) \end{array} \tag{5.3.6}$$

By Lemma A.9, $H^1_{\mathrm{fppf}}(\mathbf{Z}[1/13], \mathbf{G}_m)$ and $H^1_{\mathrm{fppf}}(\mathbf{Q}_{13}, \mathbf{G}_m)$ are both 0, since they are isomorphic to the Picard groups of a UFD and a field, respectively. Hence from (5.3.6) we get a commutative diagram

$$\begin{array}{ccc} \mathbf{G}_m(\mathbf{Z}[1/13])/(\mathbf{G}_m(\mathbf{Z}[1/13]))^{19} & \xrightarrow{\sim} & H^1_{\mathrm{fppf}}(\mathbf{Z}[1/13], \mu_{19}) \\ \downarrow & & \downarrow{\scriptstyle \rho'} \\ \mathbf{G}_m(\mathbf{Q}_{13})/(\mathbf{G}_m(\mathbf{Q}_{13}))^{19} & \xrightarrow{\sim} & H^1_{\mathrm{fppf}}(\mathbf{Q}_{13}, \mu_{19}) \end{array} \tag{5.3.7}$$

Thus, ρ' is injective if the left vertical arrow is injective. But by the very meaning of $\mathbf{G}_m$, this is the natural map

$$\mathbf{Z}[1/13]^\times/(\mathbf{Z}[1/13]^\times)^{19} \to \mathbf{Q}_{13}^\times/(\mathbf{Q}_{13}^\times)^{19} = (\mu_{12}/\mu_{12}^{19}) \times 13^{\mathbf{Z}} \times \left((1 + 13\mathbf{Z}_{13})/(1 + 13\mathbf{Z}_{13})^{19}\right).$$

Since $\mathbf{Z}[1/13]^\times = \{\pm 13^n\}$ and $-1 = (-1)^{19}$, injectivity is clear. □

The last step is to prove:

Lemma 5.3.6. The group $H^1_{\mathrm{fppf}}(\mathbf{Z}[1/13], E)$ vanishes.

Proof. For this proof, we may and do work with étale cohomology (cf. Lemma A.10). We consider E as an étale sheaf over $\mathbf{Z}[1/13]$ via the functor of points of E.

Let $T := \mathrm{Spec}(\mathbf{Z}[\zeta_{13}, 1/13])$ and let $f : T \to \mathrm{Spec}(\mathbf{Z}[1/13])$ be the structure map. We have the Leray spectral sequence [1, 59.54.2]

$$E_2^{i,j} = H^i_{\text{ét}}(\mathbf{Z}[1/13], R^j f_*(E_T)) \Rightarrow H^{i+j}_{\text{ét}}(T, E_T).$$

The map f is also finite, so $R^j f_*(E_T)$ vanishes for all $j > 0$ [1, 59.25.2]. Hence, the edge map $E_2^{i,0} = H^i_{\text{ét}}(\mathbf{Z}[1/13], f_*(E_T)) \to H^i_{\text{ét}}(T, E_T)$ is an isomorphism for all i.

Now, there is a *trace map* $f_*(E_T) \to E$ with the following property [1, 59.66]: if $E \to f_*(E_T)$ is the natural map which sends $\sigma \in E(U)$ to the base change $\sigma_T \in E_T(U_T)$ for an étale map $U \to \mathbf{Z}[1/13]$, then the composition

$$E \to f_*(E_T) \xrightarrow{\text{trace}} E \tag{5.3.8}$$

is multiplication by $\deg(f) = 12$.

Notice that multiplication by 12 is an isomorphism on E, since this can be checked over the finite étale base change E_T, which is the constant group $\mathbf{Z}/19\mathbf{Z}$. Hence the maps in (5.3.8) induce maps

$$H^1_{\text{ét}}(\mathbf{Z}[1/13], E) \to H^1_{\text{ét}}(\mathbf{Z}[1/13], f_*(E_T)) \to H^1_{\text{ét}}(\mathbf{Z}[1/13], E),$$

where the composite map is an isomorphism. It follows that $H^1_{\text{ét}}(\mathbf{Z}[1/13], E)$ injects into $H^1_{\text{ét}}(\mathbf{Z}[1/13], f_*(E_T)) \cong H^1_{\text{ét}}(T, E_T)$, so our problem reduces to proving that $H^1_{\text{ét}}(T, E_T) = 0$.

By Lemma 5.3.4, E_T is the constant T-group scheme $\mathbf{Z}/19\mathbf{Z}$. Our goal is thus to show $H^1_{\text{ét}}(T, \mathbf{Z}/19\mathbf{Z}) = 0$. We now use the fact [1, 21.4.3] that there is a set-theoretic bijection between $H^1_{\text{ét}}(T, \mathbf{Z}/19\mathbf{Z})$ and isomorphism classes of $\mathbf{Z}/19\mathbf{Z}$-torsors over T for the étale topology; i.e. finite étale covers $U \to T$ with a $\mathbf{Z}/19\mathbf{Z}$-action such that the U-morphism $\mathbf{Z}/19\mathbf{Z} \times U \to U \times_T U$ given by $(g, u) \mapsto (g \cdot u, u)$ is an isomorphism. Here, the bijection sends the zero element to the trivial torsor $\mathbf{Z}/19\mathbf{Z} \times U$.

Now, $\mathbf{Z}/19\mathbf{Z}$ acts simply transitively on geometric fibers of $U \to T$, and connected components of U are irreducible (as U inherits the Dedekind property from T) with each component having nonempty generic fiber over T. Therefore U can only have either 1 connected component or 19 such. In the latter case, we get the trivial torsor. Suppose we are in the former case, so U is a connected finite étale cover of the Dedekind affine T. Thus, U must be irreducible and equal to the normalization of T in the function field $k(U)$.

Looking at the function fields $k(U)$ and $k(T)$, we note that $[k(U) : k(T)] = 19$ and $\mathbf{Z}/19\mathbf{Z}$ acts naturally on $k(U)$ over $k(T)$. We conclude that any nontrivial element of $H^1_{\text{ét}}(T, \mathbf{Z}/19\mathbf{Z})$

corresponds to a degree-19 Galois extension L of $k(T) = K = \mathbf{Q}(\zeta_{13})$ which is unramified away from 13 (since $T = \mathrm{Spec}(\mathcal{O}_K[1/13])$ and étale morphisms are unramified). Hence it suffices to show that there are no such extensions L.

Suppose such an extension L/K exists. The prime 13 is totally ramified in K; write λ for the unique prime of K over it. By class field theory, for any non-archimedean place v of K, we have a commutative diagram

$$\begin{array}{ccc} \mathbf{A}_K^\times/K^\times & \twoheadrightarrow & \mathrm{Gal}(L/K) \cong \mathbf{Z}/19\mathbf{Z} \\ \uparrow & & \uparrow \\ K_v^\times & \longrightarrow & D_v \\ \uparrow & & \uparrow \\ \mathcal{O}_v^\times & \twoheadrightarrow & I_v \end{array}$$

where the top horizontal map is the global Artin map. But since L is unramified away from λ, all the inertia groups I_v in $\mathrm{Gal}(L/K)$ are trivial at non-archimedean places $v \neq \lambda$ of K. Also, all archimedean places of $K = \mathbf{Q}(\zeta_{13})$ are clearly complex, so $K_\infty^\times$ is a product of copies of $\mathbf{C}^\times$ and hence has no nontrivial finite quotient, so it is killed by the Artin map. Thus, the Artin map induces a surjection $K^\times \backslash \mathbf{A}_K^\times/(K_\infty^\times \times \prod_{v\neq\lambda} \mathcal{O}_v^\times) \twoheadrightarrow \mathrm{Gal}(L/K)$.

On the other hand, we know that

$$K^\times \backslash \mathbf{A}_K^\times/(K_\infty^\times \times \prod_v \mathcal{O}_v^\times) \cong \mathrm{Cl}(K),$$

and $\mathrm{Cl}(K) = 1$ by [29, 11.1]. Thus, we have a composition of surjections

$$\mathcal{O}_\lambda^\times \twoheadrightarrow K^\times \backslash \mathbf{A}_K^\times/(K_\infty^\times \times \prod_{v\neq\lambda} \mathcal{O}_v^\times) \twoheadrightarrow \mathrm{Gal}(L/K)$$

We have $\mathcal{O}_\lambda^\times \cong k(\lambda)^\times \times (1+\mathfrak{m}_\lambda)$ as abelian groups, where $\mathfrak{m}_\lambda$ is the maximal ideal of $\mathcal{O}_\lambda$ and $k(\lambda)$ denotes the residue field $\mathcal{O}_K/\lambda \cong \mathcal{O}_\lambda/\mathfrak{m}_\lambda$. Since λ is the unique prime of K above 13, the group $k(\lambda)^\times \cong \mathbf{F}_{13}^\times$ is of order 12. Also, the multiplicative group $1+\mathfrak{m}_\lambda$ is pro-13, since $(1+\mathfrak{m}_\lambda^j)/(1+\mathfrak{m}_\lambda^{j+1}) \cong \mathfrak{m}_\lambda^j/\mathfrak{m}_\lambda^{j+1}$ is 13-torsion for all $j \geq 1$ and $1+\mathfrak{m}_\lambda^N \cong \mathfrak{m}_\lambda^N$ via the 13-adic logarithm for sufficiently large N. Hence $t \mapsto t^{19}$ is invertible on $\mathcal{O}_\lambda^\times$, so it is impossible for a group homomorphism $\mathcal{O}_\lambda^\times \to \mathrm{Gal}(L/K) \cong \mathbf{Z}/19\mathbf{Z}$ to be a surjection.

This contradicts the existence of L, so $H^1_{\text{ét}}(T, E_T) = 0$. □

5.4 Proof of Theorem 5.2.4

In this subsection, we prove Theorem 5.2.4. To recall the statement, let $P_1, \ldots, P_6$ be the six rational cusps in $X(\mathbf{Q})$. The claims are:

(i) for each $i \neq j$, the nonzero class $[P_i]-[P_j] \in J(\mathbf{Q})$ (which is nonzero since $g(X) = 2 > 0$) is of order 19;

(ii) all of these classes $[P_i] - [P_j]$ generate the same subgroup T of $J(\mathbf{Q})_{\mathrm{tors}} \subseteq J(\mathbf{Q})$;

(iii) the image of $X(\mathbf{Q})$ in $J(\mathbf{Q})$ via the embedding $P \mapsto [P] - [P_6]$ intersects T at only those 6 points $[P_i] - [P_6]$.

To check equivalences of various divisor classes $\sum_{i=1}^6 a_i[P_i]$, we can use Lemma A.11 to pass to checking equalities of divisor classes $\sum_{i=1}^6 a_i[(P_i)_{\mathbf{C}}]$, so we will now work with the analytic model of X (while invoking some knowledge about $\mathbf{Q}$-cusps among $\mathbf{C}$-cusps). Note that all meromorphic functions on $X_{\mathbf{C}}^{\mathrm{an}}$ are rational functions on $X_{\mathbf{C}}$.

Now, we need to define another family of finite-index subgroups of $\Gamma(1)$. Write

$$\Gamma(N) \coloneqq \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma(1) : a \equiv d \equiv 1 \bmod N, b \equiv c \equiv 0 \bmod N \right\},$$

which is a subgroup of $\Gamma_1(N)$ of index N. We write $X(N)$ for $X_{\Gamma(N)} \coloneqq \mathbf{H}^*/\Gamma(N)$ and $Y(N) \coloneqq \mathbf{H}/\Gamma(N)$ for the open submanifold obtained by removing the cusps. As with $Y_1(N)$, we can actually build $Y(N)$ over $\mathbf{Q}$ as a moduli scheme, now for elliptic curves with a "full level-N structure": pairs (E, φ), where E is an elliptic curve over a $\mathbf{Q}$-scheme S and φ is an isomorphism $(\mathbf{Z}/N\mathbf{Z})_S \times \mu_{N,S} \xrightarrow{\sim} E[N]$. Similarly, $X(N)$ can be built as the regular compatification of $Y(N)$, and can be given a moduli-theoretic interpretation: $X(N)(S)$ is the set of isomorphism classes of generalized elliptic curves E/S equipped with a full level-N structure (in this case, the isomorphism φ by definition has image in the smooth locus E^{sm}, and satisfies an ampleness condition).

Adapting the discussion following Fact 5.2.1, the geometric cusps of $X(N)$ correspond to full level-N structures on N-gons. For each cusp C of $X(N)_{\overline{\mathbf{Q}}}$ over an N-gon cusp of $X_1(N)_{\overline{\mathbf{Q}}}$, we can verify the functorial criterion of étaleness for the natural quotient map $X(N) \to X_1(N)$ at C. In particular, $X(13) \to X$ is étale, hence unramified by [3, 2.2.6], over the $\mathbf{Q}$-rational cusps of X.

We now describe certain modular forms on X. These will be used to find relations between the divisor classes $[P_i] - [P_j]$. Define the Eisenstein series

$$E_2(\tau; \alpha, \beta) \coloneqq \sum_{(m,n) \equiv (\alpha,\beta) \bmod 13} (m\tau + n)^{-2}.$$

for $\alpha, \beta \in \mathbf{Z}$. By [8, 4.6.1], differences of the form $E_2(\alpha, \beta) - E_2(\alpha', \beta')$ are modular forms of weight 2 for $\Gamma(13)$. We will also need the following fact about the order of zeroes of $E_2(\alpha, \beta)$ at cusps, which is proved by taking the Fourier expansion of $E_2(\alpha, \beta)$ at cusps:

Fact 5.4.1. For an integer x, write $\{x\}$ for the unique integer $0 \leq n \leq 6$ such that $n \equiv \pm x \bmod 13$. Then $E_2(\alpha, \beta)$ has a zero of order at least $\{\alpha a + \beta c\}$ at the cusp (a, c) of $X(13)$.

With this setup, we can finally start proving Ogg's result in earnest. For $1 \leq i \leq 6$, let P_i be the cusp of X represented by $(0, i)$, and let $\varphi_i(\tau) = E_2(\tau; 0, i)$. We know that the $\varphi_{ij} \coloneqq \varphi_i - \varphi_j$ are modular forms of weight 2 for $\Gamma(13)$. Note that $\Gamma_1(13)/\Gamma(13) \cong \mathbf{Z}$ is generated by $\gamma \coloneqq \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$, which acts on $\tau \in \mathbf{H}$ by adding 1, and

$$\varphi_{ij}(\gamma(\tau)) = \sum_{(m,n) \equiv (0,i) \bmod 13} (m\tau + (m+n))^{-2} - \sum_{(m,n) \equiv (0,j) \bmod 13} (m\tau + (m+n))^{-2} = \varphi_{ij}(\tau).$$

Hence φ_{ij} satisfies the invariance condition for both $\Gamma(13)$ and $\mathbf{Z}$, which means it satisfies the same functional equation for $\Gamma_1(13)$. Therefore we may consider φ_{ij} as a modular form on $\Gamma_1(13)$.

If we consider the form φ_{ij} on $\Gamma_1(13)$ as a global section of the line bundle $\omega^{\otimes 2}$ for $\omega \coloneqq e^*(\Omega^1_{E^{\mathrm{sm}}/X}) \cong f_*(\omega_{E/X})$, where $f : E \to X$ is the universal generalized elliptic curve, it pulls back to the form φ_{ij} on $\Gamma(13)$ (considered as a section of the analogous $\omega^{\otimes 2}$ on $X(13)$). Since $X(13) \to X$ is *unramified* over the $\mathbf{Q}$-rational cusps of X, the order of the zero of the section φ_{ij} of $\omega^{\otimes 2}$ at $(0, c)$ is the *same* whether we consider this form and cusp as objects on $X(13)$ or on X.

By the above discussion and Fact 5.4.1, we can calculate lower bounds on the orders of the φ_i at $P_1, \ldots, P_6$. Below, by a 6-tuple $(a_1, \ldots, a_6)$, we mean that a_i is the order of the zero at P_i.

- φ_1 has zeroes of orders at least $(1, 2, 3, 4, 5, 6)$.
- φ_2 has zeroes of orders at least $(2, 4, 6, 5, 3, 1)$.
- φ_3 has zeroes of orders at least $(3, 6, 4, 1, 2, 5)$.
- φ_4 has zeroes of orders at least $(4, 5, 1, 3, 6, 2)$.
- φ_5 has zeroes of orders at least $(5, 3, 2, 6, 1, 4)$.
- φ_6 has zeroes of orders at least $(6, 1, 5, 2, 4, 3)$.

Now, φ_{ij} is actually a modular form of weight 2 for $\Gamma_1(13)$, and we saw in Section 4.2 that $\Gamma_1(13)$ has index $(13^2/2) \prod_{p|13} (1 - (1/p^2)) = 84$ in $\Gamma(1)$. But in general, a modular form of weight k for an index-d subgroup $\Gamma \subseteq \Gamma(1)$ has $kd/12$ zeros, counted with multiplicity, in any fundamental domain for Γ. So, if we find $2 \cdot 84/12 = 14$ zeros of φ_{ij} at the P_i, we know that we have found *all* the zeros of φ_{ij}. Since the order $\mathrm{ord}_{\varphi_{ij}}(P_i)$ of a zero of φ_{ij} at P_i is at least $\min\big(\mathrm{ord}_{\varphi_i}(P_i), \mathrm{ord}_{\varphi_j}(P_i)\big)$, we see that

- φ_{12} has zeroes of orders at least $(1, 2, 3, 4, 3, 1)$.

- φ_{13} has zeroes of orders at least $(1, 2, 3, 1, 2, 5)$.
- φ_{14} has zeroes of orders at least $(1, 2, 1, 3, 5, 2)$.
- φ_{15} has zeroes of orders at least $(1, 2, 2, 4, 1, 4)$.
- φ_{16} has zeroes of orders at least $(1, 1, 3, 2, 4, 3)$.
- φ_{23} has zeroes of orders at least $(2, 4, 4, 1, 2, 1)$.

All of these 6-tuples sum to 14, so the above discussion shows that the above modular forms φ_{ij} have zeros of *exactly* the indicated orders at each P_i, as well as *no other zeros*.

We now take certain ratios of the above modular forms φ_{ij}, considered as meromorphic functions on X with no zeros or poles away from the cusps (thanks to the absence of zeros on $\mathbf{H}$ shown above). We can explicitly compute the corresponding principal divisors on X:

$$\begin{aligned} (\varphi_{12}/\varphi_{13}) &= (0, 0, 0, 3, 1, -4) & (\varphi_{12}/\varphi_{14}) &= (0, 0, 2, 1, -2, -1) \\ (\varphi_{12}/\varphi_{15}) &= (0, 0, 1, 0, 2, -3) & (\varphi_{12}/\varphi_{16}) &= (0, 1, 0, 2, -1, -2). \\ (\varphi_{12}/\varphi_{23}) &= (-1, -2, -1, 3, 1, 0) \end{aligned} \tag{5.4.1}$$

Here we consider a 6-tuple $(a_1, \ldots, a_6)$ as the divisor $\sum_{i=1}^{6} a_i P_i$.

For $1 \leq i \leq 5$, let t_i be the linear equivalence class of $[P_i] - [P_6]$, which is the image of P_i under the embedding $X(\mathbf{C}) \to J(\mathbf{C})$. We claim that all of these have order 19 and generate the same subgroup T of $J(\mathbf{C})$ (recall that this is really a statement about $X(\mathbf{Q})$ and $J(\mathbf{Q})$, but equalities of divisor classes can be checked over $\mathbf{C}$). This would prove that any $[P_i] - [P_j]$ for $i \neq j$ is of order 19 and generates T, since it is nontrivial can be written as a difference of two of the divisors $[P_i] - [P_6]$. One can check using the principal divisors listed in (5.4.1) that

$$\begin{aligned} t_5 &= -3t_4 & 2t_3 &= -7t_4 & t_3 &= 6t_4 \\ t_2 &= -5t_4 & t_1 &= 4t_4 \end{aligned}. \tag{5.4.2}$$

For instance, $2t_3 = (0, 0, 2, 0, 0, -2)$ and $-7t_4 = (0, 0, 0, -7, 0, 7)$ represent the same linear equivalence class, since they differ by $-2(\varphi_{12}/\varphi_{13}) - (\varphi_{12}/\varphi_{14}) = (0, 0, -2, -7, 0, 9)$. Similarly, $t_3 = (0, 0, 1, 0, 0, -1)$ and $6t_4 = (0, 0, 0, 6, 0, -6)$ represent the same linear equivalence class, since they differ by $2(\varphi_{12}/\varphi_{13}) - (\varphi_{12}/\varphi_{15}) = (0, 0, -1, 6, 0, -5)$.

From the second and third equation in (5.4.2), we have $19t_4 = 0$, and so the rest of the equations show that each of the t_i generate $\langle t_4 \rangle = T$. This proves claims (i) and (ii) of Theorem 5.2.4.

It remains to show that the image of $X(\mathbf{Q})$ in $J(\mathbf{Q})$ via the embedding $P \mapsto [P] - [P_6]$ intersects T at only those 6 points $[P_i] - [P_6]$. This can be checked after passing from $\mathbf{Q}$ to

$\mathbf{C}$, since we will even show $X(\mathbf{C}) \cap T$ consists of the points $[P_i] - [P_6]$. From (5.4.2), we see that $t_1 + t_5 = t_4 = t_2 + t_3$, which is to say that there are linear equivalences

$$P_1 + P_5 \sim P_4 + P_6 \sim P_2 + P_3. \tag{5.4.3}$$

Write D for the divisor $P_1 + P_5$, so $\dim_{\mathbf{C}}|D| \geq 1$. If K is a canonical divisor on X, then a Riemann-Roch calculation (using $g(X) = 2$) shows that $\deg(K) = 2$. Moreover, any degree 2, effective divisor D' on X with $\dim_{\mathbf{C}}|D'| \geq 1$ is linearly equivalent to K, since Riemann-Roch again gives

$$\dim_{\mathbf{C}}|D'| - \dim_{\mathbf{C}}|K - D'| = \deg(D') + 1 - g(X) = 1,$$

so $\dim_{\mathbf{C}}|K - D'| \geq 0$. But $K - D'$ has degree 0, and the only linear equivalence class of degree-0 divisors corresponding to a nonempty complete linear system is the trivial equivalence class, so $K \sim D'$. In particular, all the linearly equivalent divisors of (5.4.3) are linearly equivalent to K, so $|D| = |K| = 1$.

Now, suppose for contradiction that there is a point $P \in X(\mathbf{C}) \notin \{P_1, \ldots, P_6\}$ such that $t \coloneqq [P] - [P_6]$ is equal to vt_4 for some $v \in \mathbf{Z}/19\mathbf{Z}$. Since $X(\mathbf{C}) \to J(\mathbf{C})$ is injective, we know that $v \notin \{0, 1, 4, -5, 6, -3\}$ by the relations of (5.4.2). Indeed, if v were any of these values, the relations of (5.4.2) would force P to be one of P_6, P_4, P_1, P_2, P_3, or P_5, contrary to assumption.

Suppose $t = -t_i$ for some i, and hence $P + P_i \sim 2P_6$. Then there is a nonzero rational function f on X determining a degree 2 cover $X \to \mathbf{P}^1$, where f has simple zeros at P and P_i and a double pole at P_6. By what we showed above, f must also arise from the complete linear system $|K|$, so $f^*(\infty) = 2P_6$ is a canonical divisor. But then $P_4 + P_6 \sim D \sim 2P_6$ and so $P_4 \sim P_6$, which would imply $X \cong \mathbf{P}^1$, a contradiction. Hence $v \notin \{-1, -4, 5, -6, 3\}$, since the relations of (5.4.2) show that $-t_1 = -4t_4$, $-t_2 = 5t_4$, $-t_3 = 6t_4$, and $-t_5 = 3t_4$.

Next, if $t = 2t_i$ for some i, then $P + P_6 \sim 2P_i$. But the same argument as in the previous paragraph shows that $2P_i$ is a canonical divisor, but so are $D = P_1 + P_5$, $P_4 + P_6$, and $P_2 + P_3$ (5.4.3). So we may find some $P_i + P_j$ linearly equivalent to $2P_i$, upon which $P_i \sim P_j$ for $i \neq j$, giving a contradiction again. So $v \notin \{2, 8, 9, -7, -6\}$, since the relations of (5.4.2) show that $2t_1 = 8t_4$, $2t_2 = 9t_4$, $2t_3 = -7t_4$, and $2t_5 = -6t_4$.

The only remaining possibilities for v are $\{-2, 7, -8, -9\}$. We can look at each case individually:

- By (5.4.2), we have $-2t_4 = t_1 - t_3 = [P_1] - [P_3]$. If $t = -2t_4$, then $P - P_6 \sim P_1 - P_3$, so $P_1 + P_6$ would be canonical and hence linearly equivalent to $P_1 + P_5$, by (5.4.3). Then $P_5 \sim P_6$, a contradiction.

- By (5.4.2), we have $7t_4 = t_3 + t_4 = [P_3] + [P_4] - 2[P_6]$. If $t = 7t_4$, then $P + P_6 \sim P_3 + P_4$, so $P_3 + P_4$ would be canonical and hence linearly equivalent to $P_2 + P_3$, by (5.4.3). Then $P_2 \sim P_4$, a contradiction.

- By (5.4.2), we have $-8t_4 = t_2+t_5 = [P_2]+[P_5]-2[P_6]$. If $t = -8t_4$, then $P+P_6 \sim P_2+P_5$, so $P_2 + P_5$ would be canonical and hence linearly equivalent to $P_1 + P_5$, by (5.4.3). Then $P_1 \sim P_2$, a contradiction.
- By (5.4.2), we have $-9t_4 = t_2 - t_1 = [P_2] - [P_1]$. If $t = -9t_4$, then $P - P_6 \sim P_2 - P_1$, so $P_2 + P_6$ would be canonical and hence linearly equivalent to $P_4 + P_6$, by (5.4.3). Then $P_2 \sim P_4$, a contradiction.

So no such v with $t = vt_4$ exists, and hence claim (iii) of Theorem 5.2.4 is proved.

Appendices

A Results from Algebraic Geometry

In this Appendix, we collect useful results from algebraic geometry. We will simply state the results and proofs, and indicate where they are used in the main exposition.

The following result is used in the proof of Proposition 2.3.1.

Lemma A.1. Let G be a commutative group scheme locally of finite type over a field k, with identity e and multiplication m. Then the composite map

$$dm_{(e,e)} : T_e(G) \oplus T_e(G) \cong T_{(e,e)}(G \times_k G) \to T_e(G) \tag{A.1}$$

is addition of tangent vectors.

Proof. Let's begin by explaining the first isomorphism. More generally, for locally finite type k-schemes X, Y with $x_0 \in X(k)$ and $y_0 \in Y(k)$, we claim the natural map

$$T_{(x_0,y_0)}(X \times_k Y) \to T_{x_0}(X) \oplus T_{y_0}(Y)$$

via covariance is an isomorphism. For affine opens $\mathrm{Spec}(A) \subseteq X$ and $\mathrm{Spec}(B) \subseteq Y$ around x_0 and y_0 respectively,

$$\mathfrak{m}_{x_0} \otimes_k k + k \otimes_k \mathfrak{m}_{y_0} + \mathfrak{m}_{x_0} \otimes_k \mathfrak{m}_{y_0} = \mathfrak{m}_{x_0} \otimes_k B + A \otimes_k \mathfrak{m}_{y_0} = \mathfrak{m}_{(x_0,y_0)}.$$

Thus, $\mathfrak{m}_{x_0}/\mathfrak{m}_{x_0}^2 \oplus \mathfrak{m}_{y_0}/\mathfrak{m}_{y_0}^2 \xrightarrow{\sim} \mathfrak{m}_{(x_0,y_0)}/\mathfrak{m}_{(x_0,y_0)}^2$. Dualizing this isomorphism gives the claim.

Now, the map $dm_{(e,e)}$ is necessarily k-linear, so it suffices to show that the composite maps

$$T_e(G) \overset{i_1}{\underset{i_2}{\rightrightarrows}} T_e(G) \oplus T_e(G) \xrightarrow{dm(e,e)} T_e(G)$$

are the identity, where i_1 and i_2 are inclusions into the first and second factors, respectively. By functoriality of tangent spaces, the composition

$$T_e(G) \xrightarrow{i_1} T_e(G) \oplus T_e(G) \xrightarrow{dm(e,e)} T_e(G)$$

is induced by the composition $G \xrightarrow{g\mapsto(g,e)} G \times_k G \xrightarrow{m} G$, which is the identity. Therefore $dm(e,e) \circ i_1 = \mathrm{id}$, and similarly $dm(e,e) \circ i_2 = \mathrm{id}$, so by linearity, $dm(e,e)$ is addition.

□

The following result is used in the proof of Lemma 3.3.4. The result actually holds for any artin local ring over k, but we only need the result for the dual numbers.

Lemma A.2 ([14, 4.8])**.** Let X be a smooth affine scheme over a field k, and let $k[\epsilon]$ be the ring $k[x]/(x^2)$ of dual numbers over k. If X' is a flat scheme over $k[\epsilon]$ such that $X' \otimes_{k[\epsilon]} k \cong X$ over k, then $X' \cong X \otimes_k k[\epsilon]$.

Proof. We will apply the "functorial criterion for smoothness" of [3, 2.2.6]; suppose we have a k-morphism $f : Y_0 \to X$, where Y_0 is an *affine* scheme of finite type over k. Let $Y_0 \subseteq Y$ be a first-order infinitesimal thickening of Y, meaning that Y_0 is a closed subscheme of Y such that its ideal sheaf has square 0 (note that Y is also affine since $(Y_0)_{\mathrm{red}} = Y_{\mathrm{red}}$, see [13, Ex. III.3.1]). Then f lifts to some $g : Y \to X$ restricting to f on Y_0.

In the case that $Y_0 = X$, $f = \mathrm{id}$, and the infinitesimal thickening is the closed immersion $i : X \hookrightarrow X'$ given by the isomorphism $X' \otimes_{k[\epsilon]} k \cong X$, we may find a lift $p : X' \to X$ such that $p \circ i = \mathrm{id}$. Via p and the structure map $X' \to k[\epsilon]$, we get a $k[\epsilon]$-map $f : X' \to X \otimes_k k[\epsilon]$, which induces the original isomorphism $X' \otimes_{k[\epsilon]} k \cong X$ upon taking the fiber product $\otimes_{k[\epsilon]} k$ (since this fiber product just looks at the closed subscheme defined by killing ϵ).

Everything is affine, so let's just work with rings. In the ring setting, we have a map $f : R \otimes_k k[\epsilon] \to R'$ over $k[\epsilon]$, inducing $R \cong R' \otimes_{k[\epsilon]} k$ upon tensoring with k over $k[\epsilon]$. To see that f is an isomorphism, consider the following exact sequence of modules over $k[\epsilon]$:

$$R \otimes_k k[\epsilon] \to R' \to \mathrm{coker}(f) \to 0.$$

After tensoring this with k over $k[\epsilon]$, we get

$$R \to R' \otimes_{k[\epsilon]} k \to \mathrm{coker}(f) \otimes_{k[\epsilon]} k \to 0,$$

where the first map is an isomorphism, so $\mathrm{coker}(f) \otimes_{k[\epsilon]} k = 0$. As $k = k[\epsilon]/(\epsilon)$, it follows that $\mathrm{coker}(f) = 0$, so in fact we have a short exact sequence

$$0 \to \ker(f) \to R \otimes_k k[\epsilon] \to R' \to 0$$

over $k[\epsilon]$. Again, tensor this with k over $k[\epsilon]$, and since R' is $k[\epsilon]$-flat by assumption, the tensored sequence stays exact, and we conclude $\ker(f) = 0$ as well. □

The following result is used in the proof of Proposition 5.2.5.

Proposition A.3. There is a unique elliptic curve E over $\mathbf{F}_9$ with 13 dividing $|E(\mathbf{F}_9)|$, and for this E, $\mathrm{Aut}_{\mathbf{F}_9}(E) \cong \mathbf{Z}/6\mathbf{Z}$.

The following proof is due to Brian Conrad (for the existence) and Noam Elkies (for the uniqueness).

Proof. Note that by the Hasse bound $||E(\mathbf{F}_9)| - 9 - 1| \leq 2\sqrt{9} = 6$ [26, V.1.1], any E as in the lemma equivalently satisfies $|E(\mathbf{F}_9)| = 13$.

Existence: To build the desired E, we start with a specific elliptic curve E_0 over $\mathbf{F}_3$(!) with $j(E_0) = 0$, and then make a sextic twist over $\mathbf{F}_9$. Let E_0 be given by the Weierstrass equation $y^2 = x^3 - x$, which by the proof of [26, A.1.2], has automorphisms given by the coordinate transformations $x = u^2x' + r$ and $y = u^3y'$, where $u^4 = 1$ and $r^3 - r = 0$. In $\mathbf{F}_3$, there are 2 possibilities for u and 3 for r, so $|\mathrm{Aut}_{\mathbf{F}_3}(E_0)| = 6$.

We now prove an intermediate result:

Lemma A.4. Let k be a field with $\mathrm{char}(k) \neq 2$. Suppose E is an elliptic curve over k satisfying:

i. For some prime $l \geq 5$ with $l \neq \mathrm{char}(k)$, $E[l](k) \cong \mathbf{Z}/l\mathbf{Z}$.

ii. 6 divides $|\mathrm{Aut}_k(E)|$.

Then $\mathrm{Aut}_k(E)$ has order 6 and is cyclic.

Proof. The cyclicity is automatic once $|\mathrm{Aut}_k(E)| = 6$, since $-1 \in \mathrm{Aut}_k(E)$ is central with order 2 (all maps of elliptic curves commute with inversion) but S_3 has trivial center.

The only way that $|\mathrm{Aut}_k(E)| > 6$ can occur is for k to be characteristic 3, in which case $\mathrm{Aut}_k(E) = \mathrm{Aut}_{\overline{k}}(E_{\overline{k}})$ is a *non-abelian* group of order 12 (by [26, A.1.2], using the assumption $\mathrm{char}(k) \neq 2$). Thus, we just need to check that $\mathrm{Aut}_k(E)$ is abelian.

The action of $\mathrm{Aut}_k(E)$ on $E[l](k) \cong \mathbf{Z}/l\mathbf{Z}$ defines a map $\alpha : \mathrm{Aut}_k(E) \to (\mathbf{Z}/l\mathbf{Z})^\times$, so $\mathrm{Aut}_k(E)$ is abelian if $\ker(\alpha) = 1$. But if $\gamma \in \ker(\alpha)$, then γ is a k-automorphism of (E, P) with $P \in E(k)$ of exact order $l \geq 5$. Such pairs have no nontrivial automorphisms, so $\gamma = 1$. □

Now, let $C \coloneqq \mathrm{Aut}_{\mathbf{F}_3}(E_0)$ act on E_0. The group C of order 6 is cyclic, since $-1 \in C$ is in its center. Consider the C-action on $E_0[13](\overline{\mathbf{F}}_3) \cong \mathbf{F}_{13}^{\oplus 2}$. Since $13 \nmid |C|$, this $\mathbf{F}_{13}$-representation is completely reducible. Moreover, $\mathbf{F}_{13}^\times$ contains a primitive 6th root of unity and C is abelian, so irreducible $\mathbf{F}_{13}[C]$-modules are 1-dimensional. Hence, $E_0[13](\overline{\mathbf{F}}_3) \cong L_1 \oplus L_2$ as C-representations, with the C-action on the line L_i being via some character $\chi_i : C \to \mathbf{F}_{13}^\times$.

But the action of $C = \mathrm{Aut}_{\mathbf{F}_3}(E_0)$ leaves the 13-Weil pairing $\langle \cdot, \cdot \rangle_{E_0,13}$ unaffected, so for any $c \in C$ and non-identity points $P_1 \in L_1$ and $P_2 \in L_2$,

$$\langle P_1, P_2 \rangle_{E_0,13} = \langle c(P_1), c(P_2) \rangle_{E_0,13} = \langle \chi_1(c) \cdot P_1, \chi_2(c) \cdot P_2 \rangle_{E_0,13} = (\langle P_1, P_2 \rangle_{E_0,13})^{(\chi_1\chi_2)(c)}.$$

Since the Weil pairing is non-degenerate and symplectic, it follows that $\langle P_1, P_2 \rangle_{E_0,13} \neq 1$ and hence $\chi_1\chi_2 = 1$. Therefore C acts on $E_0[13](\overline{\mathbf{F}}_3)$ via the representation $\chi \oplus (1/\chi)$ for some character $\chi : C \to \mathbf{F}_{13}^\times$.

The C-action on $E_0[13](\overline{\mathbf{F}}_3)$ has trivial stabilizer at nonzero points P, since the pair (E, P) with P of exact order 13 has no nontrivial automorphisms. Thus, χ is injective and hence yields an isomorphism $\chi : C \xrightarrow{\sim} \mu_6(\mathbf{F}_{13})$. In particular, $\chi^2 \neq 1$, so $\chi \neq 1/\chi$. This implies that L_1 and L_2 are the *unique* C-stable lines in $E_0[13](\overline{\mathbf{F}}_3)$.

The action on $E_0[13](\overline{\mathbf{F}}_3)$ by $\Gamma_{\mathbf{F}_3} := \mathrm{Gal}(\overline{\mathbf{F}}_3/\mathbf{F}_3)$ commutes with the C-action (as the latter action is defined over $\mathbf{F}_3$), so it preserves the L_i's by the aforementioned uniqueness. Hence $\Gamma_{\mathbf{F}_3}$ acts on each L_i by scalar multiplications, so let $\theta_i : \Gamma_{\mathbf{F}_3} \to \mathbf{F}_{13}^\times$ be the visibly continuous action on L_i. Since $\Gamma_{\mathbf{F}_9} = (\Gamma_{\mathbf{F}_3})^2$ (as $\mathrm{Frob}_9 = (\mathrm{Frob}_3)^2$), we see that the image of $\Gamma_{\mathbf{F}_9}$ under either θ_i is contained in $(\mathbf{F}_{13}^\times)^2 = \mu_6(\mathbf{F}_{13})$. Hence, the action of $\Gamma_{\mathbf{F}_9}$ on $E_0[13](\overline{\mathbf{F}}_3)$ is given by $\theta_1 \oplus \theta_2$ for characters $\theta_i : \Gamma_{\mathbf{F}_9} \to \mu_6(\mathbf{F}_{13})$.

But $\chi : C \xrightarrow{\sim} \mu_6(\mathbf{F}_{13})$ is the action on L_1, so via the continuous map

$$\Gamma_{\mathbf{F}_9} \xrightarrow{\theta_1} \mu_6 \xrightarrow[\sim]{\chi^{-1}} C = \mathrm{Aut}_{\mathbf{F}_3}(E_0) \subseteq \mathrm{Aut}_{\mathbf{F}_9}(E_0),$$

we may form the sextic twist E over $\mathbf{F}_9$ of $(E_0)_{\mathbf{F}_9}$ by the *reciprocal* character $1/(\chi^{-1} \circ \theta_1)$ of $\chi^{-1} \circ \theta_1 : \Gamma_{\mathbf{F}_9} \to C$. Note that here, χ^{-1} denotes the inverse of the isomorphism $\chi : C \xrightarrow{\sim} \mu_6(\mathbf{F}_{13})$, whereas $1/\chi$ as used before denotes the reciprocal of χ as characters (i.e. the composition $C \xrightarrow{\chi} \mu_6(\mathbf{F}_{13}) \xrightarrow{a \mapsto a^{-1}} \mu_6(\mathbf{F}_{13})$). Then via the construction of twisting, $E[13](\overline{\mathbf{F}}_3) = E_0[13](\overline{\mathbf{F}}_3)$ with the $\Gamma_{\mathbf{F}_9}$-action on L_1 in $E[13](\overline{\mathbf{F}}_3)$ being the product of θ_1 and $\chi \circ (1/(\chi^{-1} \circ \theta_1)) = 1/\theta_1$, hence trivial.

Therefore $E(\mathbf{F}_9)[13] \supseteq L_1$ is nonempty, so 13 divides $|E(\mathbf{F}_9)|$ and thus $E(\mathbf{F}_9) \cong \mathbf{Z}/13\mathbf{Z}$. Moreover, by the commutativity of C and the construction of E by twisting, we have $C \subseteq \mathrm{Aut}_{\mathbf{F}_9}(E)$, so Lemma A.4 with $k = \mathbf{F}_9$ and $l = 13$ shows that $\mathrm{Aut}_{\mathbf{F}_9}(E) = C \cong \mathbf{Z}/6\mathbf{Z}$. This settles the existence of E as in Proposition A.3.

Uniqueness: Let E be an elliptic curve over $\mathbf{F}_9$ with $|E(\mathbf{F}_9)| = 13$. Since we are in characteristic 3, E is given by some Weierstrass equation

$$E_{a,b,c} : y^2 = x^3 + ax^2 + bx + c.$$

We will determine the possibilities for the coefficients $a, b, c \in \mathbf{F}_9$ such that $|E_{a,b,c}(\mathbf{F}_9)| = 13$, and we will then show all such $E_{a,b,c}$ are isomorphic. This will also give a more explicit proof of the existence of an E with the desired properties.

By the proof of [26, V.4.1], E is supersingular since the trace of Frobenius is

$$\mathrm{tr}(\mathrm{Frob}_9) = 9 + 1 - |E(\mathbf{F}_9)| = -3 \equiv 0 \bmod 3.$$

The same proof shows that the supersingularity of $E_{a,b,c}$ is equivalent to the j-invariant $(4a)^2 - 24(2b) = 16a^2$ of $E_{a,b,c}$ being 0, so $a = 0$ and we write $E_{b,c}$ instead of $E_{a,b,c}$. This also forces b to be nonzero to ensure that the discriminant $\Delta = -16(4b^3 + 27c^2)$ is nonzero in $\mathbf{F}_9$. Therefore (b, c) must be among $8 \cdot 9 = 72$ possible choices.

Moreover, by the duplication formula given in [26, III.2.3], we see that $(x_0, y_0) \in E_{b,c}(\mathbf{F}_9)$ is a nontrivial 2-torsion point exactly when $x_0^3 + bx_0 + c = 0$. Hence $N_{b,c} := |E_{b,c}(\mathbf{F}_9)|$ is odd exactly when the polynomial $x^3 + bx + c$ has no roots (i.e. is irreducible) over $\mathbf{F}_9$, since any root x_0 gives the nontrivial 2-torsion point $(x_0, 0)$, and vice-versa. There are $9 \cdot 8/6 = 12$ such polynomials $x^3 + bx + c$ that split completely, corresponding to unordered 3-tuples of distinct roots $(r, s, -r - s)$ (as $x^3 + bx + c$ has no repeated roots; note that if $r \neq s$ then $r \neq -r - s$ and $s \neq -r - s$). Similarly, there are $9 \cdot 4 = 36$ such polynomials $x^3 + bx + c$ that split as a monic linear times a monic quadratic, corresponding to unordered 3-tuples of distinct roots $(r, r + s\sqrt{\rho}, r - s\sqrt{\rho})$ where $s \in \mathbf{F}_9^\times$ and $\rho \in \mathbf{F}_9^\times$ is a quadratic nonresidue. Indeed, there are 9 choices for r, 4 choices for s (note that s and $-s$ determine the same unordered 3-tuple), and the description of the roots is constrained by the given factorization of $x^3 + bx + c$ and the fact that they must sum to 0. So because we are trying to find (b, c) such that $N_{b,c} = 13$, we have cut our search down to $72 - 12 - 36 = 24$ possible pairs.

For such pairs (b, c) (so $N_{b,c}$ is odd), the Hasse bound gives $|N_{b,c} - 10| \leq 6$, and we have also constructed $E_{b,c}$ to be supersingular, so $\mathrm{tr}(\mathrm{Frob}_9) = 10 - N_{b,c} \equiv 0 \bmod 3$. These facts constrain $N_{b,c}$ to be either 7 or 13, so Frob_9 on $E_{b,c}$ respectively satisfies $x^2 + 3x + 9$ or $x^2 - 3x + 9$ in those cases [26, V.2.3.1]. By the construction of quadratic twists, the traces of Frob_9 acting on $E_{b,c}$ and its quadratic twist $E'_{b,c}$ are negatives of each other, so quadratic twisting on $E_{b,c}$ switches the characteristic polynomial of Frob_9 from x^2+3x+9 to x^2-3x+9 and vice-versa. Thus, there are exactly $24/2 = 12$ pairs (b, c) with $N_{b,c} = 13$.

We claim that if i is a primitive 4th root of unity in $\mathbf{F}_9^\times$, then $N_{-1,i} = 13$. Indeed, if $\rho \in \mathbf{F}_9^\times$ satisfies $\rho^2 = i$, then ρ is a non-square (as ρ has multiplicative order 8), and by inspection $E_{-1,i}(\mathbf{F}_9)$ already has the 12 nonidentity points

$$\{(0, \pm\rho), (\pm 1, \pm\rho), (i, \pm\rho^3), (i \pm 1, \pm\rho^3)\}.$$

Hence, it suffices to show that the polynomial $x^3 - x + i$ has no roots in $\mathbf{F}_9$ (in which case $N_{b,c}$ is either 7 or 13, so must be 13), and this amounts to a brute-force check. Also, $E_{-1,i}$ has automorphisms $(x, y) \mapsto (x+1, y)$ and $(x, y) \mapsto (x, -y)$ with orders 3 and 2 respectively, so Lemma A.4 shows that $\mathrm{Aut}_{\mathbf{F}_9}(E_{-1,i}) \cong \mathbf{Z}/6\mathbf{Z}$. Hence we can take E to be $E_{-1,i}$.

For any $u \in \mathbf{F}_9^\times$, the curves E_{u^4b,u^6c} and $E_{b,c}$ are isomorphic via $(x, y) \mapsto (u^2x, u^3y)$. Likewise, for any $q \in \mathbf{F}_9$, E_{b,q^3+bq+c} and $E_{b,c}$ are isomorphic via $(x, y) \mapsto (x - q, y)$. Hence, these u- and q-transformations act on pairs (b, c). We claim that the orbit of $(b, c) = (-1, i)$

under this action consists at least 12 distinct pairs, which would show that any $E_{b,c}$ with $N_{b,c} = 13$ is isomorphic to $E_{-1,i}$. Indeed, since the actions of $u = -1$ and $q = \pm 1$ are the only ones fixing $(-1, i)$, let u_1, u_2, u_3, u_4 be representatives of the 4 elements of the multiplicative group $\mathbf{F}_9^\times/\{\pm 1\}$, and let q_1, q_2, q_3 be representatives of the 3 elements of the additive group $\mathbf{F}_9/\{0, 1, -1\}$. Then it is clear that all 12 possible pairs $q_j \cdot (u_i \cdot (-1, i))$ are distinct, and we are done. □

The following result is used in the proof of Proposition 5.2.5 and Proposition 5.3.2.

Lemma A.5. Let R be a local ring with residue field k. Let A be a smooth separated commutative group scheme over R. Then for any prime $l \neq \mathrm{char}(k)$, the reduction map

$$A[l](R) \to A[l](k)$$

is injective.

Proof. The same argument as in the proof of Proposition 2.3.1 shows that $A[l]$ is separated and étale over R. Now, any section $g \in A[l](R)$ is a closed immersion, but it is also étale since both $\mathrm{Spec}(R)$ and $A[l]$ are étale R-schemes, so it must be an open immersion as well [3, 2.2.4]. Hence g cuts out a clopen subscheme (also denoted g) in $A[l]$, so $A[l]$ topologically breaks up as a disjoint union of clopen subschemes $g \coprod (A[l] - g)$. Thus, if two R-points $g, g' \in A[l](R)$ induce the same k-point, they must be the same connected component C (containing that physical k-point) as their image, so they agree topologically. Since g and g' are both sections to the restriction $C \xrightarrow{\sim} \mathrm{Spec}(R)$ of the structure map $A[l] \to \mathrm{Spec}(R)$, they must be the same R-point.

□

The following result is used in the discussion of the minimal polynomial of γ_2 (after Proposition 5.2.10):

Lemma A.6. Let A be any simple abelian variety over a field k, and $f, g \in \mathrm{End}(A)$ with $g \circ f = 0$. Then either $g = 0$ or $f = 0$.

Proof. A nonzero endomorphism f of A must be surjective: the scheme-theoretic image $f(A)$ is an abelian subvariety of A, forcing $f(A) = A$ since f is nonzero and A is simple over k. Hence, if g and f are both nonzero, $g \circ f$ is surjective. But $g \circ f = 0$, so either $g = 0$ or $f = 0$. □

The following number-theoretic result is used in the proof of Proposition 5.3.2.

Lemma A.7. Let p be a prime and $D \subseteq G$ be a decomposition group corresponding to p; that is, $D = D(\overline{v}|v)$ fixes a place $\overline{v}$ on $\overline{\mathbf{Q}}$ extending $v := |\cdot|_p$ on $\mathbf{Q}$. Then naturally $D \cong \mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$ as topological groups.

Proof. Write G_p for $\mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$. We know that the place $\overline{v}$ is induced by an embedding $i : \overline{\mathbf{Q}} \hookrightarrow \overline{\mathbf{Q}}_p$ over $\mathbf{Q} \to \mathbf{Q}_p$ (giving $\mathbf{Q}_p$ and $\overline{\mathbf{Q}}_p$ the unique absolute values extending v). We then have a map $G_p \to G$ by restriction. Any $\sigma \in G_p$ preserves the unique absolute value on $\overline{\mathbf{Q}}_p$ over $|\cdot|_p$ on $\mathbf{Q}_p$, hence is an isometry and thus continuous.

We now claim that the image of $\overline{\mathbf{Q}}$ inside $\overline{\mathbf{Q}}_p$ is dense. Since any element of $\overline{\mathbf{Q}}_p$ appears in a finite subextension, it suffices to show that $L \cap \overline{\mathbf{Q}}$ is dense inside L for any finite extension $L/\mathbf{Q}_p$.

By the primitive element theorem, L has the form $\mathbf{Q}_p(a)$; let $g \in \mathbf{Q}_p[x]$ be the minimal polynomial of a. Since $\mathbf{Q}$ is dense in $\mathbf{Q}_p$, we can perturb the non-leading coefficients of g slightly to create a nearby monic polynomial $g' \in \mathbf{Q}[x]$, and by Krasner's Lemma, g' is still irreducible (over $\mathbf{Q}_p \supseteq \mathbf{Q}$) with $L \cong \mathbf{Q}_p[x]/(g) \cong \mathbf{Q}_p[x]/(g')$. Now, $\mathbf{Q}[x]/(g')$ is a finite extension F of $\mathbf{Q}$, and $F \otimes_{\mathbf{Q}} \mathbf{Q}_p \cong L$ by construction. But tensoring a number field with $\mathbf{Q}_p$ gives a product of completions of F at places over v, so it follows that there is a *unique* place w of F over v and $F_w = L$. Hence F is dense in L, so *a fortiori*, $L \cap \overline{\mathbf{Q}}$ is also dense in L.

By the preceding density, the restriction map $G_p \to G$ is injective. The image lands in D, since the embedding i induces $\overline{v}$ on $\overline{\mathbf{Q}}$ and the G_p action on $\overline{\mathbf{Q}}_p$ fixes the unique place on $\overline{\mathbf{Q}}_p$ over $|\cdot|_p$ on $\mathbf{Q}_p$.

We now show that the image of this map is all of D. We saw above that for all finite subextensions $L/\mathbf{Q}_p$ inside $\overline{\mathbf{Q}}_p$, there is a finite extension $F/\mathbf{Q}$ with $F_w \cong L$ where w is a place on F extending v. Increasing F (hence L) if necessary, we can focus on F that is Galois over $\mathbf{Q}$. An element $\sigma' \in \mathrm{Gal}(F/\mathbf{Q})$ fixing w gives a unique isometric automorphism $\tau : F_w \to F_w$ such that $\tau \circ j = j \circ \sigma'$, where j is the isometric embedding $F \hookrightarrow F_w$. This τ must fix $\mathbf{Q}_p$ pointwise as it fixes its dense subset $\mathbf{Q}$, so it is an automorphism of $F_w/\mathbf{Q}_p$. Note also that we can find an embedding $F \hookrightarrow \overline{\mathbf{Q}}$ so that $\overline{v}$ restricts to w on F.

Given $\sigma' \in D$, look at its actions on all finite Galois subextensions $\overline{\mathbf{Q}}/F/\mathbf{Q}$, where F gets the restricted place w of $\overline{v}$. By the above discussion, this induces an automorphism σ_F on $F_w/\mathbf{Q}_p$. But these F_w's account for a *cofinal system* of finite subextensions $\overline{\mathbf{Q}}_p/L/\mathbf{Q}_p$, since L is isomorphic to some such F_w and Galois extensions have a *unique* image in an algebraic closure. These automorphisms σ_F are clearly compatible, so we may patch them together to an automorphism $\sigma \in G_p$ which restricts to $\sigma'|_F$ for all finite $F/\mathbf{Q}$. Hence the image of σ under $G_p \to G$ is σ', which means $G_p \to G$ surjects onto D.

Note that this group isomorphism $G_p \to D$ is a continuous map of topological groups, since it's enough to check continuity at the identity, which is clear. As a bijection from a compact space to a Hausdorff space, it is a homeomorphism. □

The following result is used in the proof of Lemma 5.3.4.

Lemma A.8. For a Dedekind domain R with fraction field K, the generic-fiber functor

$$\{\text{finite étale } R\text{-schemes}\} \to \{\text{finite étale } K\text{-schemes}\}$$

is fully faithful.

Proof. Let B be a finite étale algebra over R. We claim that B is equal to the integral closure C of R in the generic fiber B_K, which gives the result. Since B_K is finite étale over K, it is a finite product $\prod_i K_i$ of finite separable field extensions of K.

Now, since R is Dedekind and each K_i/K is separable, C is a finitely generated R-module. It is torsion-free since it sits inside the K-vector space $\prod_i K_i$. Since B is finite over R, it is integral and hence contained in C. Therefore it suffices to check that the inclusion $B \subseteq C$ is an equality after localizing at each maximal ideal of R. Hence we may assume R is a discrete valuation ring.

In this local case, B and C are R-free, and they have the same rank since their K-fibers coincide. We can choose R-bases $\{b_i\}$ and $\{c_i\}$ for B and C respectively such that $b_i = r_i c_i$ for some nonzero $r_i \in R$, and hence

$$\operatorname{disc}(B/R) = \operatorname{disc}(C/R) \cdot \prod_{i=1}^{n} r_i$$

as ideals of R. We claim that $\operatorname{disc}(B/R)$ is the unit ideal in R, so then the r_i are units and hence $B = C$ as desired.

Letting k be the residue field of R, it suffices to check that $\operatorname{disc}(B_k/k)$ is nonzero. But B_k is k-étale, so it is a product of finite separable extensions of k, implying $\operatorname{disc}(B_k/k) \neq 0$. □

The following result is used in the proof of Lemma 5.3.5.

Lemma A.9. For any scheme X, we have naturally $H^1_{\text{fppf}}(X, \mathbf{G}_m) \cong \operatorname{Pic}(X)$.

Proof. To calculate $H^1_{\text{fppf}}(X, \mathbf{G}_m)$, we use the fact that the derived H^1_{fppf} functor is the same as the Cech $\check{H}^1_{\text{fppf}}$ functor. By definition, $\check{H}^1_{\text{fppf}}(X, \mathbf{G}_m) = \varinjlim_{\mathfrak{U} \to X} (\check{H}^1(\mathfrak{U}, \mathbf{G}_m))$, where the direct limit is taken over fppf covers $\mathfrak{U}$ of X (by which we mean a collection of flat and locally finitely presented maps $\{U_i \xrightarrow{f_i} X\}$ such that the open images $f_i(U_i)$ form a cover of X).

Now, $\check{H}^1(\mathfrak{U}, \mathbf{G}_m) = Z^1(\mathfrak{U}, \mathbf{G}_m)/B^1(\mathfrak{U}, \mathbf{G}_m)$, and we claim that

$$Z^1(\mathfrak{U}, \mathbf{G}_m)/B^1(\mathfrak{U}, \mathbf{G}_m) \cong \operatorname{Pic}_{\mathfrak{U}}(X),$$

where $\operatorname{Pic}_{\mathfrak{U}}(X)$ is defined as

$$\operatorname{Pic}_{\mathfrak{U}}(X) \coloneqq \{\mathcal{L} \in \operatorname{Pic}(X) : \mathcal{L}_{U_i} = f_i^* \mathcal{L} \cong \mathcal{O}_{U_i} \text{ for all } U_i \xrightarrow{f_i} X\}.$$

We see that $Z^1(\mathfrak{U}, \mathbf{G}_m)$ consists of collections of units on the fppf cover $\mathfrak{U}$ satisfying the "triple overlap" condition:

$$\{(u_{ij} \in \mathcal{O}(U_i \times_X U_j)^\times) : u_{ij} u_{jk} u_{ik}^{-1} = 1 \in \mathcal{O}(U_i \times_X U_j \times_X U_k)^\times\},$$

and that $B^1(\mathfrak{U}, \mathbf{G}_m)$ is the collection

$$\{(u_{ij} \in \mathcal{O}(U_i \times_X U_j)^\times) : \text{there exists } (u_i \in \mathcal{O}(U_i)^\times)_i \text{ such that } u_{ij} = p_i^*(u_i)/p_j^*(u_j)\},$$

where p_i, p_j are the projection maps out of $U_i \times_X U_j$. Hence we have a map

$$\mathrm{Pic}_{\mathfrak{U}}(X) \to Z^1(\mathfrak{U}, \mathbf{G}_m)/B^1(\mathfrak{U}, \mathbf{G}_m), \tag{A.2}$$

given as follows: if $\mathcal{L} \in \mathrm{Pic}_{\mathfrak{U}}(X)$ has generators $e_i \in (f_i^*\mathcal{L})(U_i)$ over U_i for each i, then we send $\mathcal{L}$ to the collection (u_{ij}), where $u_{ij} \in \mathcal{O}(U_i \times_X U_j)^\times$ is such that $p_i^*(e_i) = p_j^*(e_j)u_{ij}$. This map is well-defined, since if we adjust the e_i to a different compatible set of local generators e_i' and determine a new collection (u_{ij}'), then u_{ij} is adjusted by $p_i^*(e_i'/e_i)/p_j^*(e_j'/e_j)$.

To see that the map of (A.2) is an isomorphism, we use the theorem that all descent data for a quasicoherent sheaf with respect to an fppf cover $\{S_i' \to S\}$ are effective. Note that because fppf maps are (universally) *open* [1, 29.25.10], the proof of this theorem reduces to the case of a single fppf map $S' \to S$, which is a theorem of Grothendieck [3, 6.1.4].

Given $\mathcal{L}, \mathcal{L}' \in \mathrm{Pic}_{\mathfrak{U}}(X)$ with the same image (u_{ij}) in $Z^1(\mathfrak{U}, \mathbf{G}_m)/B^1(\mathfrak{U}, \mathbf{G}_m)$, we deduce that the isomorphisms $f_i^*\mathcal{L} \cong f_i^*(\mathcal{L}')$, coming from the given isomorphisms $f_i^*\mathcal{L} \cong \mathcal{O}_{U_i}$ and $f_i^*(\mathcal{L}') \cong \mathcal{O}_{U_i}$, are compatible on triple overlaps (in the language of [3, 6.1], this is an isomorphism of descent data). These isomorphisms $f_i^*\mathcal{L} \cong f_i^*(\mathcal{L}')$ descend to an isomorphism $\mathcal{L} \to \mathcal{L}'$, which gives injectivity. For surjectivity, we simply note that a choice of (u_{ij}) in $Z^1(\mathfrak{U}, \mathbf{G}_m)/B^1(\mathfrak{U}, \mathbf{G}_m)$ gives a descent datum on the structure sheaves $\mathcal{O}_{U_i}$ "glued" across the disjoint union $\coprod_i U_i$ via the u_{ij} (using compatibility of (u_{ij}) on triple overlaps). By effective descent, this invertible sheaf is isomorphic to the pullback of some $\mathcal{L} \in \mathrm{Pic}_{\mathfrak{U}}(X)$.

This argument shows that

$$H^1_{\mathrm{fppf}}(X, \mathbf{G}_m) = \varinjlim_{\mathfrak{U} \to X} (\check{H}^1(\mathfrak{U}, \mathbf{G}_m)) = \varinjlim_{\mathfrak{U} \to X} \mathrm{Pic}_{\mathfrak{U}}(X),$$

and the last term is exactly $\mathrm{Pic}(X)$, since every invertible sheaf is trivialized over *some* open cover. □

The following result is used in the proof of Lemma 5.3.6.

Lemma A.10. The cohomologies $H^1_{\mathrm{fppf}}(S, E)$ and $H^1_{\text{ét}}(S, E)$ are in natural bijection for any scheme S and any commutative finite étale S-group E.

This natural bijection is even a group isomorphism, but we do not need this stronger statement.

Proof. By [1, 21.4.3], there is a set-theoretic bijection between $H^1_{\mathrm{fppf}}(S, E)$ (resp. $H^1_{\text{ét}}(S, E)$) and the set of isomorphism classes of E-torsors over S for the fppf (resp. étale) topologies. Thus, it suffices to show that every fppf E-torsor over S is also an étale torsor, and vice-versa.

One direction is clear, as étale maps are flat and locally of finite presentation. Conversely, if U is an fppf E-torsor over S, then because $E \to S$ is étale, $\mathrm{pr}_2 : E \times_S U \to U$ is étale as well. But by assumption, the map $\varphi : E \times_S U \to U \times_S U$ given functorially on points valued in S-schemes by $(e, u) \mapsto (e \cdot u, u)$ is an isomorphism, so it follows that the composition $\mathrm{pr}_2 \circ \varphi^{-1} : U \times_S U \to U$ is étale. This is simply the second projection map for the base change of $U \to S$ by itself, so by fppf descent, $U \to S$ is étale (and surjective, since it was already a cover). □

The following result is used in the proof of Theorem 5.2.4 (cf. Section 5.4).

Lemma A.11. Let C be a proper, smooth, geometrically connected scheme over a field k. Then for any extension field K/k, the pullback map $\mathrm{Pic}(C) \to \mathrm{Pic}(C_K)$ is injective.

Proof. Let $\mathcal{L}$ be an invertible sheaf on C whose pullback $\mathcal{L}_K$ is trivial. As $\mathrm{Spec}(K) \to \mathrm{Spec}(k)$ is flat, we have an isomorphism $H^0(C, \mathcal{L}) \otimes_k K \cong H^0(C_K, \mathcal{L}_K) \cong H^0(C_K, \mathcal{O}_{C_K}) \cong K$ (since C is geometrically integral), which implies $H^0(C, \mathcal{L})$ is 1-dimensional. Since pullback commutes with dual, $H^0(C, \mathcal{L}^{-1})$ is likewise 1-dimensional. By choosing nonzero global sections of $\mathcal{L}$ and $\mathcal{L}^{-1}$, corresponding to nonzero maps $\mathcal{O}_C \to \mathcal{L}$ and $\mathcal{L} \to \mathcal{O}_C$ respectively, the composite map $\mathcal{O}_C \to \mathcal{L} \to \mathcal{O}_C$ is certainly nonzero, hence multiplication by some $c \in k^\times$ and thus an isomorphism. Therefore $\mathcal{L} \to \mathcal{O}_C$ is a surjection of invertible sheaves and hence an isomorphism. □

References

[1] The Stacks Project Authors, *Stacks project*.

[2] G. Billing and Kurt Mahler, *On exceptional points on cubic curves*, Journal of the London Mathematical Society **s1-15** (1940), no. 1, 32–43.

[3] Siegfried Bosch, Werner Lütkebohmert, and Michel Raynaud, *Néron models*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], vol. 21, Springer-Verlag, Berlin, 1990.

[4] Amanda Clemm and Sarah Trebat-Leder, *Elliptic curves with everywhere good reduction*, Journal of Number Theory **161** (2016), 135–145, Special Issue on Applications of Automorphic Forms in Number Theory and Combinatorics.

[5] Brian Conrad, *Lecture notes, introduction to abelian varieties*.

[6] ———, *Lecture notes, modular curves*.

[7] Pierre Deligne and Michael Rapoport, *Les schémas de modules de courbes elliptiques*, Modular Functions of One Variable II (Berlin, Heidelberg) (Pierre Deligne and Willem Kuijk, eds.), Springer Berlin Heidelberg, 1973, pp. 143–316.

[8] Fred Diamond and Jerry Shurman, *A first course in modular forms*, Graduate Texts in Mathematics, vol. 228, Springer-Verlag, New York, 2005.

[9] Alexander Grothendieck, *Éléments de Géométrie Algébrique : II. Étude globale élémentaire de quelques classes de morphismes*, Publications Mathématiques de l'IHÉS **8** (1961), 5–222 (fr).

[10] ———, *Éléments de Géométrie Algébrique : III. Étude cohomologique des faisceaux cohérents, Seconde partie*, vol. 17, Institut des Hautes Études Scientifiques, 1963 (fr). MR 163911

[11] ———, *Éléments de Géométrie Algébrique : IV. Étude locale des schémas et des morphismes de schémas, Troisième partie*, Publications Mathématiques de l'IHÉS **28** (1966), 5–255 (fr).

[12] ———, *Éléments de Géométrie Algébrique : IV. Étude locale des schémas et des morphismes de schémas, Quatrième partie*, vol. 32, Institut des Hautes Études Scientifiques, 1967 (fr).

[13] Robin Hartshorne, *Algebraic geometry*, Graduate Texts in Mathematics, No. 52, Springer-Verlag, New York-Heidelberg, 1977.

[14] ———, *Deformation theory*, Graduate Texts in Mathematics, vol. 257, Springer, New York, 2010.

[15] Nicholas M. Katz and Barry Mazur, *Arithmetic moduli of elliptic curves*, Annals of Mathematics Studies, vol. 108, Princeton University Press, Princeton, NJ, 1985.

[16] Daniel Sion Kubert, *Universal bounds on the torsion of elliptic curves*, Proceedings of the London Mathematical Society **s3-33** (1976), no. 2, 193–237.

[17] Qing Liu, *Algebraic geometry and arithmetic curves*, Oxford Graduate Texts in Mathematics, vol. 6, Oxford University Press, Oxford, 2002, Translated from the French by Reinie Erné, Oxford Science Publications.

[18] Barry Mazur, *Modular curves and the Eisenstein ideal*, Publications Mathématiques de l'IHÉS **47** (1977), 33–186 (eng).

[19] Barry Mazur and John Tate, *Points of order 13 on elliptic curves.*, Inventiones mathematicae **22** (1973), 41–50.

[20] Toshitsune Miyake, *Modular forms*, Springer-Verlag, Berlin, 1989, Translated from the Japanese by Yoshitaka Maeda.

[21] David Mumford, *Geometric invariant theory*, Ergebnisse der Mathematik und ihrer Grenzgebiete, (N.F.), Band 34, Springer-Verlag, Berlin-New York, 1965.

[22] Andrew Ogg, *Rational points of finite order on elliptic curves.*, Inventiones mathematicae **12** (1971), 105–111.

[23] ———, *Rational points on certain elliptic modular curves.*, Proceedings of Symposia in Pure Mathematics **XXIV** (1972), 221–231.

[24] Michel Raynaud, *Schémas en groupes de type* $(p, \ldots, p)$, Bulletin de la Société Mathématique de France **102** (1974), 241–280 (fre).

[25] Jean-Pierre Serre and John Tate, *Good reduction of abelian varieties*, Annals of Mathematics **88** (1968), no. 3, 492–517.

[26] Joseph H. Silverman, *The arithmetic of elliptic curves*, second ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009.

[27] Andrew Snowden, *Lecture notes, course on Mazur's theorem.*

[28] R. J. Stroeker, *Reduction of elliptic curves over imaginary quadratic number fields*, Pacific Journal of Mathematics **108** (1983), no. 2, 451 – 463.

[29] Lawrence C. Washington, *Introduction to cyclotomic fields*, second ed., Graduate Texts in Mathematics, vol. 83, Springer-Verlag, New York, 1997.