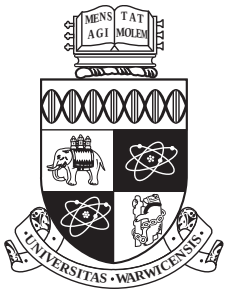
THE UNIVERSITY OF
WARWICK



Modular curves and surjectivity of Galois representations attached to elliptic curves over $\mathbb{Q}$

MSc Thesis

by

Lambros Mavrides

Supervisors:

Dr. Martin Bright

Dr. David Loeffler

MATHEMATICS INSTITUTE

SEPTEMBER 2011

Acknowledgements

I was graced to have two wonderful supervisors for this dissertation, Dr. Martin Bright and Dr. David Loeffler, to whom I express my deep gratitude. Dr. David Loeffler suggested the topic of this dissertation and drew my attention to the paper "Elliptic curves with 3-adic Galois representation surjective mod 3 but not mod 9" of Professor Noam D. Elkies. He has spent several hours explaining this densely written paper and he was always there when help was needed. Dr. Martin Bright has also offered excellent assistance and has devoted a great deal of time helping me, especially in the second half of the period spent on this dissertation. He has taught me how to think geometrically, providing numerous astonishing insights. He has also offered great assistance in programming in the computer package MAGMA.

My gratitude to my two supervisors is two-fold; Dr. Martin Bright was responsible for teaching me Galois theory through a third year module bearing the same title and hence responsible in me developing an early interest in the arithmetic aspects of mathematics. Dr. David Loeffler was the lecturer of the course Modular Forms, where I got baptised in the world of modularity and automorphy. Both of them are amazing lecturers.

I am grateful to the authors of the book "A First Course in Modular Forms", Professor Fred Diamond and Professor Jerry Shurman. Their excellent book was the cornerstone in learning the theory of modular curves and without it, my task would have been notoriously difficult.

Many thanks go to my friends and colleagues Kostas, Martha, Michael, Sam and Stephanos for many helpful discussions and assistance. I would also like to thank Thekla for all her love and support throughout the Warwick era. Last but not least, I would like to thank my parents Phedias and Chryso for their unconditional love and their full support in following my dreams.

"There are five elementary arithmetical operations: addition, subtraction, multiplication, division and modular forms." - Martin Eichler

Contents

Chapter 1

Introduction

This dissertation has stemmed out of the need to understand the paper "Elliptic curves with 3-adic Galois representation surjective mod 3 but not mod 9", by Noam D. Elkies [Elkies]. It is of expository nature and is divided into two parts; the first part includes material from the theory of modular curves and Galois representations attached to elliptic curves and is based on the book "An introduction to the theory of modular forms", by Fred Diamond and Jerry Shurman [Dia & Shur]. The second part aims to answer the question which elliptic curves defined over $\mathbb{Q}$ have 3-adic Galois representation surjective mod 3 but not mod 9, using the above paper as well as explaining an alternative approach.

In this essay we start with (chapter 2, section 1) an introduction to the theory of modular forms and present the modular curve $X(\Gamma)$ as the space of orbits of the action of a congruence subgroup Γ on the upper half plane together with the set of cusps of Γ. We then move on to give a topology on $X(\Gamma)$ that makes it a connected, compact, Hausdorff, second countable topological space. We naturally progress to define charts on $X(\Gamma)$ and give it a complex structure so that it becomes a compact, connected Riemann surface. We then come across a way of reading off the "number of holes" (also known as the genus) of $X(\Gamma)$ and have a first glimpse of the archetypical example of a modular curve, that is $X(1)$. We also define a complex elliptic curve as a Riemann surface, with this case the number of holes always being equal to 1.

In section 2 of chapter 2, we quote Serre's GAGA which guarantees for any compact, connected Riemann surface R the existence of polynomial equations over $\mathbb{C}$ such that R can be written as the zero locus of these polynomials. It turns out that the resulting projective algebraic variety is smooth and 1-dimensional, i.e. a smooth, projective algebraic curve. As a result any modular curve or complex

elliptic curve can be viewed as a smooth, projective algebraic curve. This opens up the way for the use of algebraic geometry in our study. In section 2.2 we explore some algebro-geometric tools being used in the study of algebraic curves that we will make use of throughout this essay (such as valuations, divisors, the Riemann-Roch theorem, etc.). This route we have chosen is though quite restrictive since we are bound to work with algebraic varieties defined over a subfield of $\mathbb{C}$. We can open up the way to allow for varieties over an arbitrary field (even over those fields that cannot be embedded in $\mathbb{C}$, such as finite fields) by redefining a modular curve as a smooth, projective algebraic curve that satisfies certain properties (this is normally done via its function field, however it is beyond the scope of this essay since we will only be interested in modular curves defined over subfields of $\mathbb{C}$) and an elliptic curve over a field K as a genus 1, smooth, projective algebraic curve over K together with a K-rational point (this definition of elliptic curve we are going to see in more detail since it is needed for the purpose of this essay). We conclude section 2.2 with the study of the Weil pairing which turns out to be a fundamental tool in the study of Galois representations attached to elliptic curves. The third section of chapter 2 is devoted to the study of the remarkable property of modular curves being moduli spaces to isomorphism classes of elliptic curves satisfying certain properties. This is essentially motivated by the archetypical example of $X(1)$ that parametrizes isomorphism classes of complex elliptic curves. In the main theorem we make this idea more explicit; we give a description of the parametrized set of isomorphism classes of elliptic curves over $\mathbb{C}$ for the case of the modular curves $X(N)$, $X_1(N)$, $X_0(N)$.

Chapter 3 is devoted to the study of Galois representations attached to elliptic curves over $\mathbb{Q}$. In particular, we study the action of the absolute Galois group of $\mathbb{Q}$ on the $\mathbb{Z}/l^n\mathbb{Z}$-module $E[l^n]$ of an elliptic curve $E/\mathbb{Q}$ and how this action is compatible with the multiplication-by-l map. This action gives the mod l^n l-adic representation with image in $\mathrm{GL}_2(\mathbb{Z}/l^n\mathbb{Z})$ and passing to the inverse limit we obtain the l-adic Galois representation with image in $\mathrm{GL}_2(\mathbb{Z}_l)$. The second topic we choose to study in this chapter is the Galois theory of number fields and its generalization to the pro-finite absolute Galois group of $\mathbb{Q}$. This theory is one of the basic tools that allows one to extract arithmetic information encapsulated by the l-adic Galois representation attached to an elliptic curve. In the last section of chapter 3, we see the theory explored in the previous section in action. In fact we see even more; we view how the modularity theorem gives a link between the arithmetic information extracted from the l-adic Galois representation of an elliptic curve over $\mathbb{Q}$ with the arithmetic information encoded in a certain modular form.

In chapter 4 we answer the following question (following Elkies' work in [Elkies]); which elliptic curves defined over $\mathbb{Q}$ have 3-adic Galois representation surjective mod 3 but not mod 9? This set of elliptic curves would essentially be empty if the prime 3 was replaced by any other prime $l \geq 5$. This follows from a theorem proved by Serre in his book "Abelian l-adic representations and elliptic curves" [Serre 2]. However this fails for the case of the primes 2 and 3 (the case of the prime 2 is treated in the paper [Dokchitser]). Indeed there are elliptic curves defined over $\mathbb{Q}$ with $\bar{\rho}_{3,E}$ mod 3 surjective and $\bar{\rho}_{3,E}$ mod 9 not; an example is the elliptic curve $y^2 = x^3 - 27x - 42$. Elkies (and so do we) uses the theory of modular curves as moduli spaces to classify all elliptic curves with the required property. He does this by finding a lift of $\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$ in $\mathrm{SL}_2(\mathbb{Z}/9\mathbb{Z})$ (that he calls G), that is a proper subgroup of and unique up to conjugation. In fact with the aid of the computer package GAP we find that up to conjugacy, no other proper subgroup of $\mathrm{SL}_2(\mathbb{Z}/9\mathbb{Z})$ surjects on $\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$. As a result, if an elliptic curve $E/\mathbb{Q}$ has the above property then the image of $\bar{\rho}_{3,E}$ mod 9 in $\mathrm{SL}_2(\mathbb{Z}/9\mathbb{Z})$ must be a conjugate of G. The modular curve that parametrizes such elliptic curves is the curve $X(9)/G$. However, $X(9)/G$ is not a priori defined over $\mathbb{Q}$ as an algebraic curve and so we are forced to consider the modular curve $\tilde{X}(9)/G'$. G' is a subgroup of $\mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z})$ satisfying $G = G' \cap \mathrm{SL}_2(\mathbb{Z}/9\mathbb{Z})$ and $\tilde{X}(9)/G'$ equals to $[(\mathbb{Z}/9\mathbb{Z})^* : \det(G')]$ copies of $X(9)/G$. $\tilde{X}(9)/G'$ now has a natural structure over $\mathbb{Q}$. Moreover, in our case we are lucky since there is a plethora of subgroups of the form G' that also satisfy $\det(G') \cong (\mathbb{Z}/9\mathbb{Z})^*$ and hence give $\tilde{X}(9)/G' = X(9)/G$.

We then move on to study $X(9)/G$ as a Riemann surface; we compute its cusps, elliptic points and genus. It turns out that $X(9)/G$ has genus 0 and thus it is analytically isomorphic to $\mathbb{P}^1_{\mathbb{C}}$. By finding a $\mathbb{Q}$-rational divisor of odd degree on $X(9)/G$ and quoting a theorem of Max Noether we also conclude that $X(9)/G$ is algebraically isomorphic over $\mathbb{Q}$ to $\mathbb{P}^1_{\mathbb{Q}}$. It also turns out that the field of definition of the cusps of $X(9)/G$ is not the field $\mathbb{Q}$ but $K := \mathbb{Q}(\zeta + \zeta^{-1})$, for ζ a primitive 9-th root of unity, which makes the computation of the above algebraic isomorphism a harder task. The first step in computing this isomorphism is to find a function F defined on $X(9)/G$ that gives an isomorphism with $\mathbb{P}^1_{\mathbb{C}}$. We do this by choosing a modular unit, i.e. a function that its divisor is supported at the cusps of $X(9)/G$. But since the cusps of $X(9)/G$ are defined over the field K then so are the coefficients of F. So we then find an automorphism A of $\mathbb{P}^1_{\mathbb{C}}$ with coefficients in K that changes the $\mathbb{Q}$ structure of $\mathbb{P}^1_{\mathbb{C}}$ by sending the image of the cusps of $X(9)/G$ under F to a $\mathrm{Gal}(K/\mathbb{Q})$-orbit in K. As a result, the j-function as a function of F is not defined over $\mathbb{Q}$, but $f := j \circ A^{-1}$ as a function of $x := A \circ F$ is. In fact, we compute that

$f(x)$ is a rational function of degree 27 and this is the algebraic isomorphism we are after. In the last section of chapter 4, we give an alternative approach to the problem that is more algorithmic in nature. Unfortunately this alternative approach is far from being an effective algorithm (essentially we cannot prove that it terminates, so technically speaking it is not an algorithm at all), which gives another justification of the need of Elkies' work to solve this problem.

Chapter 2

Modular curves

We begin our study of modular curves by reviewing some elementary theory of modular forms. Let $\mathbb{H} = \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$ denote the upper half plane in $\mathbb{C}$. Then we have that the modular group $\mathrm{SL}_2(\mathbb{Z})$ acts on $\mathbb{H}$ from the left as follows; take $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ and $\tau \in \mathbb{H}$, then $g \cdot \tau := \frac{a\tau+b}{c\tau+d}$. Notice that

$$\mathrm{Im}(g \cdot \tau) = \mathrm{Im}\left(\frac{a\tau+b}{c\tau+d} \cdot \frac{c\bar{\tau}+d}{c\bar{\tau}+d}\right) = \frac{1}{|c\tau+d|^2}\mathrm{Im}(ac|\tau|^2 + ad\tau + bc\bar{\tau} + bd)$$

$$= \frac{1}{|c\tau+d|^2}(ad-bc)\mathrm{Im}(\tau) = \frac{1}{|c\tau+d|^2}\mathrm{Im}(\tau) > 0.$$

Hence $g \cdot \tau \in \mathbb{H}$ and indeed one can easily check that the rest of the axioms for an action hold. Notice here that the element $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ acts trivially and as a result it is natural to consider the quotient $\mathrm{PSL}_2(\mathbb{Z}) := \mathrm{SL}_2(\mathbb{Z})/\{\pm\mathrm{Id}\}$ which acts faithfully on $\mathbb{H}$. Now define the subgroup $\Gamma(N)$ of $\mathrm{SL}_2(\mathbb{Z})$ for an integer N by

$$\Gamma(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \bmod N \right\}.$$

We say that a subgroup $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$ is a **congruence subgroup** when $\Gamma(N) \subseteq \Gamma$ for some $N \in \mathbb{N}$. It is easy to see that if Γ is a congruence subgroup then it is of finite index since $\Gamma(N)$ is the kernel of the natural reduction map $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ and $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ is finite (but there are finite index subgroups of $\mathrm{SL}_2(\mathbb{Z})$ that are not congruence subgroups; this is the so called "The congruence subgroup problem").

Two important congruence subgroups are the following:

$$\Gamma_0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} \bar{a} & \bar{b} \\ 0 & \bar{d} \end{pmatrix} \bmod N \right\}$$

$$\Gamma_1(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & \bar{b} \\ 0 & 1 \end{pmatrix} \bmod N \right\}.$$

Note that we have an inclusion of groups $\Gamma(N) \leq \Gamma_1(N) \leq \Gamma_0(N)$.

$\mathrm{SL}_2(\mathbb{Z})$ also acts on $\mathbb{P}^1_{\mathbb{Q}} = \mathbb{Q} \cup \{\infty\}$ from the left as follows; let $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$, $\frac{u}{v} \in \mathbb{Q}$. Then $g \cdot (\frac{u}{v}) := \frac{a\frac{u}{v}+b}{c\frac{u}{v}+d}$ and $g \cdot \infty := \frac{a}{c}$. Moreover, we define $g \cdot (\frac{u}{v}) = \infty$ when $c\frac{u}{v} + d = 0$. As in the case of the action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathbb{H}$, we have that $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ acts trivially and $\mathrm{PSL}_2(\mathbb{Z})$ acts faithfully. Furthermore, one can in fact show that $\mathrm{SL}_2(\mathbb{Z})$ acts transitively on $\mathbb{P}^1_{\mathbb{Q}}$ and for Γ a congruence subgroup, the set of orbits is finite. Hence we define the set of **cusps** of Γ to be the finite set of orbits of the left action of Γ on $\mathbb{P}^1_{\mathbb{Q}}$, $\Gamma \setminus (\mathbb{Q} \cup \{\infty\})$.

In general, the set of orbits of the action of a congruence subgroup $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$ on $\mathbb{H}$ is called the modular curve $Y(\Gamma)$.

Definition 2.1 - ***The modular curve*** $Y(\Gamma)$

$$Y(\Gamma) := \Gamma \setminus \mathbb{H} = \{\Gamma\tau : \tau \in \mathbb{H}\}.$$

A priori this set has no structure. However, as we will see later, a modular curve can be given a nice topology (which is Hausdorff, second countable) and a Riemann surface structure. In particular, we will also see that a modular curve being a Riemann surface, is also an algebraic curve. The modular curves corresponding to the congruence subgroups $\Gamma(N)$, $\Gamma_1(N)$, $\Gamma_0(N)$ are denoted by $Y(N)$, $Y_1(N)$, $Y_0(N)$. In particular notice that we get surjections $Y(N) \twoheadrightarrow Y_1(N) \twoheadrightarrow Y_0(N)$ given by $\Gamma(N)\tau \mapsto \Gamma_1(N)\tau \mapsto \Gamma_0(N)\tau$. One of the main important properties of a modular curve is that it serves as a moduli space to isomorphism classes of elliptic curves satisfying certain properties. This will be discussed more extensively in section 2.3, however it is worth noting here that the above surjections suggest that as we move up the surjections we get a finer parametrization (more properties) of isomorphism classes of elliptic curves.

The modular curves $Y(\Gamma)$ can be compactified by adding the set of cusps of Γ and form a compact modular curve denoted by $X(\Gamma)$.

Definition 2.2 ***The modular curve*** $X(\Gamma)$

$$X(\Gamma) := Y(\Gamma) \cup \Gamma \setminus (\mathbb{Q} \cup \{\infty\}) = \Gamma \setminus \mathbb{H}^*,$$

for $\mathbb{H}^* = \mathbb{H} \cup \mathbb{Q} \cup \{\infty\}$.

In particular $X(\Gamma)$ is a compact Riemann surface (section 2.1) and hence we can use the theory of compact Riemann surfaces (eg. Riemann-Hurwitz formula, Riemann-Roch theorem) to extract a lot of information regarding $X(\Gamma)$. Similarly, we write $X(N)$, $X_1(N)$, $X_0(N)$, for the compactified modular curves corresponding to the congruence subgroups $\Gamma(N)$, $\Gamma_1(N)$, $\Gamma_0(N)$.

Meromorphic functions defined on the modular curve $X(\Gamma)$ are called **modular functions** (of level Γ and weight 0). Unwinding this definition we see that for a function f to be defined on $X(\Gamma)$, f needs to be constant on the set of orbits of Γ acting on $\mathbb{H}^*$. (Note that everything we define here can be defined for an arbitrary finite index subgroup $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$). A generalization of these sort of functions are the **modular functions of level Γ and weight k**. These functions are still meromorphic functions $\mathbb{H}^* \to \mathbb{C}$, but now we introduce a **factor of automorphy**, $j(\gamma, \tau)$; if $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$, $\tau \in \mathbb{H}^*$, then a meromorphic function $f : \mathbb{H}^* \to \mathbb{C}$ is a modular function of weight k and level Γ if it satisfies $f(\gamma \cdot \tau) = j(\gamma, \tau)^k f(\tau)$, where $j(\gamma, \tau) = c\tau + d$. So modular functions of weight $k > 0$, are no longer functions defined on $X(\Gamma)$.

An important class of modular functions of level Γ and weight k is the class of modular forms. A **modular form of level Γ and weight k**, is a holomorphic modular function $\mathbb{H}^* \to \mathbb{C}$ of level Γ and weight k. We denote this space by $M_k(\Gamma)$. One can in fact show that this is a finite dimensional $\mathbb{C}$-vector space and deduce some explicit dimension formulae with respect to the topology of the modular curve $X(\Gamma)$ (for example, see [Dia & Shur], Theorem 3.5.1). $M_k(\Gamma)$ has an equally important subspace of functions, called cusp forms; a modular form f is a **cusp** form if $f\,|_{\mathbb{P}^1_{\mathbb{Q}}} \equiv 0$. The subspace of cusp forms is denoted by $S_k(\Gamma)$. As a last comment here, we remark that we cannot have a non-constant modular form defined on $X(\Gamma)$ (i.e. of level Γ and weight 0). To see this, notice that if $f : X(\Gamma) \to \mathbb{C}$ would be a non-constant modular form, then as we will see later, $X(\Gamma)$ is a compact Riemann surface and so f can be extended as a map $f : X(\Gamma) \to \mathbb{P}^1_{\mathbb{C}}$ of Riemann surfaces. But since f is holomorphic, its image omits ∞ and hence it is a proper subset of $\mathbb{P}^1_{\mathbb{C}}$. Also, open mapping theorem implies that the image of f is open. But the compactness of $X(\Gamma)$ implies that its image under f in the Hausdorff space $\mathbb{P}^1_{\mathbb{C}}$ is closed, contradicting the

fact that $\mathbb{P}^1_{\mathbb{C}}$ is connected. So we conclude that no such f can exist.

2.1 Modular curves as Riemann surfaces

2.1.1 Topology and a complex structure on $X(\Gamma)$

In this section we first discuss how we can give a nice Hausdorff, second countable topology on $X(\Gamma)$ that makes it a compact, connected topological space. The naive approach would be to equip $\mathbb{H}^*$ with the Euclidean topology. As pointed out in [Dia & Shur] 2.4, this topology contains too many points of $\mathbb{P}^1_{\mathbb{Q}}$ to be Hausdorff. Instead, we take as a base of our topology on $\mathbb{H}^*$ the sets of the form $\{g(U_M \cup \{\infty\})\}_{M>0, g\in \mathrm{SL}_2(\mathbb{Z})}$, where $U_M := \{\tau \in \mathbb{H} : \mathrm{Im}(\tau) > M\}$, together with the open subsets of $\mathbb{H}$ with respect to the Euclidean topology. Then for a congruence subgroup $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$, we equip $\Gamma \setminus \mathbb{H}^*$ with the quotient topology corresponding to the projection map $\pi : \mathbb{H}^* \to \Gamma \setminus \mathbb{H}^*$. Then $X(\Gamma) = \Gamma \setminus \mathbb{H}^*$ with this topology is Hausdorff, connected, second countable and compact (for a proof of this see for example [Dia & Shur], Proposition 2.4.2).

The next step is to give $\Gamma \setminus \mathbb{H}^*$ a complex structure. For a congruence subgroup $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$, let us denote by $\bar{\Gamma}$ the projective image of Γ, i.e. the image of Γ under the projection map $\mathrm{SL}_2(\mathbb{Z}) \twoheadrightarrow \mathrm{PSL}_2(\mathbb{Z})$, which equals to $\Gamma/\{\Gamma \cap \pm\mathrm{Id.}\}$. Then for points $\pi(\tau) \in Y(\Gamma)$, where $\tau \in \mathbb{H}$ and τ has trivial stabilizer in $\bar{\Gamma}$, any point in the fibre $\pi^{-1}(\pi(\tau))$ has multiplicity 1. Hence π is locally injective. Since Γ acts properly discontinuously on $\mathbb{H}$ (for a proof of this, see for instance [Dia & Shur], Proposition 2.1.1), we can find a neighbourhood U of τ in $\mathbb{H}$ such that for any $\gamma \in \Gamma$, $\gamma U \cap U = \emptyset$. Therefore $\pi\,|_U \colon U \to \pi(U)$ is a continuous bijection and being an open map makes it a homeomorphism.

However, the points in $\mathbb{H}$ which have non-trivial stabilizer in $\bar{\Gamma}$ pose a problem. These points are called the **elliptic points** for Γ. If τ is such a point, then there are points in the fibre $\pi^{-1}(\pi(\tau))$ where the multiplicity is greater than 1 and π can no longer be locally injective. To measure this discrepancy we introduce the notion of the **period** of $\tau \in \mathbb{H}$, denoted by $n_\Gamma(\tau)$ and defined as follows; let us call Γ **even** when $-\mathrm{Id.} \in \Gamma$ and **odd** otherwise. Then

$$n_\Gamma(\tau) := \mid \mathrm{Stab}_{\bar{\Gamma}}(\tau) \mid = \begin{cases} \frac{1}{2} \mid \mathrm{Stab}_\Gamma(\tau) \mid, & \text{if } \mathrm{Stab}_{\bar{\Gamma}}(\tau) \text{ is even} \\ \mid \mathrm{Stab}_\Gamma(\tau) \mid, & \text{if } \mathrm{Stab}_{\bar{\Gamma}}(\tau) \text{ is odd} \end{cases}$$

Then the elliptic points for Γ are the points with $n_\Gamma(\tau) > 1$. It is worth noting here that $n_\Gamma(\tau) = n_{g\Gamma g^{-1}}(g\tau)$ for $g \in \mathrm{SL}_2(\mathbb{Z})$ and hence any point in the fibre $\pi^{-1}(\pi(\tau))$

has the same period.

As in the previous case of points $\tau \in \mathbb{H}$ with $n_\Gamma(\tau) = 1$, since Γ acts properly discontinuously on $\mathbb{H}$, if $\tau \in \mathbb{H}$ is arbitrary then there exists a neighbourhood $U \subset \mathbb{H}$ such that if $\gamma \in \Gamma$ and $\gamma U \cap U \neq \emptyset$ then $\gamma \in \mathrm{Stab}_{\bar{\Gamma}}(\tau)$. Consequently, such a neighbourhood has no elliptic points except possibly τ. So for any $\tau \in \mathbb{H}$ (elliptic or not), take such a neighbourhood $U \subset \mathbb{H}$ and define a chart about $\pi(\tau)$ as follows: Consider the transformations $\delta_\tau := \begin{pmatrix} 1 & -\tau \\ 1 & -\bar{\tau} \end{pmatrix} \in \mathrm{GL}_2(\mathbb{C})$ (where $\mathrm{GL}_2(\mathbb{C})$ is viewed as a linear fractional transformation $\mathbb{H} \to \mathbb{C}$) and $\rho_\tau(z) := z^{n_\Gamma(\tau)}$ defined on $\mathbb{C}$. Set $U_\tau := \pi(U)$ (where $\pi : \mathbb{H} \to \Gamma\backslash\mathbb{H}$) and define $\psi_\tau : U \to V$ to be the composite $\psi_\tau(z) = \rho_\tau \circ \delta_\tau(z) = (\delta_\tau \cdot z)^{n_\Gamma(\tau)}$, $V := \psi_\tau(U)$. Then take $\phi_\tau : U_\tau \to V$ given by $\phi_\tau \circ \pi = \psi$ and finally take the chart to be the pair (U_τ, ϕ_τ). In [Dia & Shur] 2.2, the authors check that indeed the charts $\{(U_\tau, \phi_\tau)\}_{\tau \in \mathbb{H}}$ are compatible.

It now remains to find charts for the set of cusps of $X(\Gamma)$. As in the case of elliptic points, we want to attach to each cusp $c \in \Gamma \setminus \mathbb{P}^1_{\mathbb{Q}}$ a discrepancy-measuring number called the **width** of the cusp c, denoted by $h_\Gamma(c)$ (the width of a cusp measures how much the "behaviour" of the cusp deviates from that of the single cusp of $X(1)$). The width of a cusp $c \in \Gamma \setminus \mathbb{P}^1_{\mathbb{Q}}$ is defined as follows; consider the stabilizer of the point $\infty \in \mathbb{P}^1_{\mathbb{Q}}$ in $\mathrm{SL}_2(\mathbb{Z})$ given by $P_\infty := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : c = 0 \right\}$ and take $g \in \mathrm{SL}_2(\mathbb{Z})$ with $g \cdot \infty = c$ (such g exists since as noted previously $\mathrm{SL}_2(\mathbb{Z})$ acts transitively on $\mathbb{P}^1_{\mathbb{Q}}$). Then let $\Gamma_c := (g^{-1}\Gamma g) \cap P_\infty$ and define $h_\Gamma(c) := [\bar{P}_\infty : \bar{\Gamma}_c]$. One can easily check that $h_\Gamma(c)$ is independent of the choice of $g \in \mathrm{SL}_2(\mathbb{Z})$. Take an open set of the form $U := g(U_2 \cup \{\infty\})$ and write $\delta_c := g^{-1}$, $\rho_c(z) := e^{\frac{2\pi i z}{h_\Gamma(c)}}$. Let $\psi_c : U \to V$ be the composite $\rho_c \circ \delta_c(z) = e^{\frac{2\pi i \delta_c \cdot z}{h_\Gamma(c)}}$, where $V = \mathrm{Im}\psi_c$. Then a chart about $\pi(U) =: U_c$ ($\pi : \mathbb{H}^* \to \Gamma\backslash\mathbb{H}^*$) is defined by $\phi_c : U_c \to V$, where $\phi_c \circ \pi = \psi_c$. As in the case of elliptic points, the authors in [Dia & Shur] 2.4, check explicitly the compatibility of the charts as well as with the rest of the charts that we have already defined for $X(\Gamma)$.

2.1.2 The Riemann-Hurwitz formula and the genus of $X(\Gamma)$

We begin this section by examining more closely the local structure of the natural surjective map

$$f : X(\Gamma_1) \twoheadrightarrow X(\Gamma_2)$$

$$\Gamma_1\tau \mapsto \Gamma_2\tau$$

for $\Gamma_1 \subset \Gamma_2$ congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$. This type of map is a holomorphic map of Riemann surfaces and in particular the map $X(\Gamma_1) \twoheadrightarrow X(1)$ gives a very nice formula for computing the genus of $X(\Gamma_1)$. Let us commence with the study of the **degree of** f, which is by definition the size of the fibre $f^{-1}(\Gamma_2\tau)$, counting multiplicities. Notice that since Γ_1, Γ_2 are both congruence subgroups, the index $[\Gamma_2 : \Gamma_1]$ is finite. In particular, write $\{\Gamma_1\gamma_j : j = 1, ..., n\}$ for coset representatives of $\Gamma_1 \setminus \Gamma_2$. We would like to say that $f^{-1}(\Gamma_2\tau) = \{\Gamma_1\gamma_j\tau : j = 1, ..., n\}$, but this is not always true since $X(\Gamma) = X(\bar{\Gamma})$, for any congruence subgroup Γ. So to fix this we need to consider the cosets of $\bar{\Gamma}_1 \setminus \bar{\Gamma}_2$. Write $\{\bar{\Gamma_1}\gamma'_j : j = 1, ..., n'\}$ for the coset representatives. Then $f^{-1}(\Gamma_2\tau) = \{\Gamma_1\gamma'_j\tau : j = 1, ..., n'\}$. Thus $\deg(f) = [\bar{\Gamma}_2 : \bar{\Gamma}_1]$. It is easy to observe that since $\Gamma_1 \subset \Gamma_2$, the only case in which $[\bar{\Gamma}_2 : \bar{\Gamma}_1] \neq [\Gamma_2 : \Gamma_1]$ is the case where Γ_2 is even and Γ_1 is odd, in which case it actually equals to $\frac{1}{2}[\Gamma_2 : \Gamma_1]$.

We next want to study how does f ramify. Given $x \in X(\Gamma_1)$, we write e_x for the **ramification index of** f **at** x. Now suppose that $\tau \in \mathbb{H}$. Comparing charts about the points $\Gamma_1\tau$ and $f(\Gamma_1\tau)$, one sees that $e_{\Gamma_1\tau} = [\mathrm{Stab}_{\bar{\Gamma}_2}(\tau) : \mathrm{Stab}_{\bar{\Gamma}_1}(\tau)] = \frac{n_{\Gamma_2}(\tau)}{n_{\Gamma_1}(\tau)}$. Similarly, if $c \in \mathbb{P}^1_{\mathbb{Q}}$, comparing charts about $\Gamma_1 c$ and $f(\Gamma_1 c)$ gives

$$e_{\Gamma_1 c} = [\bar{\Gamma}_{2,c} : \bar{\Gamma}_{1,c}] = \frac{[\bar{P}_\infty : \bar{\Gamma}_{1,c}]}{[\bar{P}_\infty : \bar{\Gamma}_{2,c}]} = \frac{h_{\Gamma_1}(c)}{h_{\Gamma_2}(c)}.$$

An important tool in the study of Riemann surfaces that relates the genus of $X(\Gamma_1)$ and $X(\Gamma_2)$ with the degree of f and the ramification indices e_x is the **Riemann-Hurwitz formula**:

$$2g_{X(\Gamma_1)} - 2 = d(2g_{X(\Gamma_2)}) + \sum_{x \in X(\Gamma_1)} (e_x - 1).$$

Here $g_{X(\Gamma)}$ denotes the genus of $X(\Gamma)$ and d the degree of f. Notice that since the set of ramification points of a non-constant holomorphic function f on a connected Riemann surface is a discrete subset and since we are dealing with compact Riemann surfaces, the set of ramification points is finite and hence the sum in Riemann-Hurwitz formula is finite. Considering the map $X(\Gamma) \twoheadrightarrow X(1)$, we get a vey useful genus formula for $X(\Gamma)$:

Theorem 2.3 *Let $\Gamma \leq SL_2(\mathbb{Z})$ be a congruence subgroup and $X(\Gamma) \twoheadrightarrow X(1)$ the natural projection map of degree d. Then write ϵ_2 and ϵ_3 for the number of elliptic points of period 2 and 3 in $X(\Gamma)$ and ϵ_∞ the number of cusps of $X(\Gamma)$. Then*

$$g_{X(\Gamma)} = 1 + \frac{d}{12} - \frac{\epsilon_2}{4} - \frac{\epsilon_3}{3} - \frac{\epsilon_\infty}{2}.$$

Proof: This is Theorem 3.1.1 in [Dia & Shur]. □

It is worth noting here that since $X(1) = \mathrm{SL}_2(\mathbb{Z}) \setminus \mathbb{H}^*$, $d = [\mathrm{PSL}_2(\mathbb{Z}) : \bar{\Gamma}]$, the so called projective index of Γ that we denote by d_Γ.

2.1.3 Example: The modular curve $X(1)$

$X(1)$ is the compactified modular curve corresponding to the projective modular group $\mathrm{PSL}_2(\mathbb{Z})$. Since $\mathrm{PSL}_2(\mathbb{Z})$ acts transitively on $\mathbb{P}^1_{\mathbb{Q}}$, X(1) has only one cusp. Moreover, $\mathrm{PSL}_2(\mathbb{Z})$ is generated by the elements $\mathrm{S} := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $\mathrm{T} := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ ([Serre 1], Chapter VII). Note that geometrically the action of S on $\mathbb{H}$ is a reflection about the imaginary axis followed by inversion in the unit circle. The action of T is a translation by 1. A fundamental domain for the action of $\mathrm{PSL}_2(\mathbb{Z})$ on $\mathbb{H}$ is the region $D := \{z \in \mathbb{H} : \frac{-1}{2} \leq \mathrm{Re}(z) \leq \frac{1}{2}, |z| \geq 1\}$ and if $z \in D$, $g \in \mathrm{PSL}_2(\mathbb{Z})$, $g \cdot z \in D$ then either $g = 1$ or $z \in \partial D$ (for a justification of this, see for instance [Serre 1], Chapter VII, Theorem 1). Hence identifying the boundary points of D to a single point and adding the cusp as a point at ∞ gives topologically a sphere (the identification space is homeomorphic to $\mathbb{C}$ and together with the point at infinity it is homeomorphic to a sphere). As we saw before, one is able to define a complex structure on $X(1)$ and make it a Riemann surface, though extra care needs to be taken at the elliptic points $i, e^{\frac{2\pi i}{3}}$, that have a non-trivial stabilizer in $\mathrm{PSL}_2(\mathbb{Z})$ and at the cusp (or the point at ∞). As a Riemann surface $X(1)$ is the Riemann sphere, $\mathbb{P}^1_{\mathbb{C}}$.

In order to determine the function field $\mathbb{C}(X(1))$, we first need to find the meromorphic functions on $\mathbb{P}^1_{\mathbb{C}}$. In particular, since we allow for functions $f : \mathbb{P}^1_{\mathbb{C}} \to \mathbb{C}$ to have poles, we can extend them to holomorphic maps between Riemann surfaces, $\tilde{f} : \mathbb{P}^1_{\mathbb{C}} \to \mathbb{P}^1_{\mathbb{C}}$. From Riemann surfaces theory, we have that any such map $\tilde{f}$ is a rational function of the form $\tilde{f}(z) = \frac{p(z)}{q(z)}$, for polynomials p, q and if $\tilde{f}$ is non-constant, then it is surjective. Thus the function field $\mathbb{C}(\mathbb{P}^1_{\mathbb{C}})$ is generated by a single transcendental function, i.e. $\mathbb{C}(\mathbb{P}^1_{\mathbb{C}}) = \mathbb{C}(z)$, for z transcendental. Since $X(1)$ is analytically isomorphic to $\mathbb{P}^1_{\mathbb{C}}$ (since the two spaces are homeomorphic), we conclude that $\mathbb{C}(X(1))$ is also generated by a single transcendental function. So now it remains to find a generator of $\mathbb{C}(X(1))$. Consider the discriminant function $\Delta : \mathbb{H} \to \mathbb{C}$, given by $\Delta(\tau) = g_2(\tau)^3 - 27g_3(\tau)^2$, where $g_2(\tau) = 60G_4(\Lambda_\tau)$, $g_3(\tau) = 140G_6(\Lambda_\tau)$ and $\Lambda_\tau = \mathbb{Z} + \tau\mathbb{Z}$, $G_k(\Lambda) = \sum_{\lambda \in \Lambda} \frac{1}{\lambda^k}$ the weight k homogeneous Eisenstein series. In particular, the weight k Eisenstein series are modular forms of level $\mathrm{SL}_2(\mathbb{Z})$ (see for instance [Serre 1], Chapter VII, Proposition 4). Since $g_2(\tau)^3 = (60G_4(\Lambda_\tau))^3$

and $g_3(\tau)^2 = (140G_6(\Lambda_\tau))^2$ are both modular forms of weight 12, we have that Δ is a modular form of weight 12 and same level. In particular one can check ([Silverman 2], Chapter 1, Proposition 7.4) that Δ takes the value 0 at the cusp ∞ and hence $\Delta \in S_{12}(\mathrm{SL}_2(\mathbb{Z}))$. Now we can consider the function $j : \mathbb{H} \to \mathbb{C}$, given by $j(\tau) := \frac{1728 g_2(\tau)^3}{\Delta(\tau)}$. In this case we can see that both g_2^3 and Δ are of weight 12, so j is of weight 0 and therefore $\mathrm{SL}_2(\mathbb{Z})$-invariant. This means that we can consider j as a function on $X(1)$. Moreover, $j(\tau)$ has a q-expansion of the form $j(\tau) = \frac{1}{q} + 744 + 196884q + ...$, where $q = e^{2\pi i \tau}$ (for a justification of this, see[Silverman 2], Chapter 1, Remark 7.4.1). As a result, $j(\tau)$ has a simple pole at the cusp ∞. Thus $j : X(1) \to \mathbb{P}^1_{\mathbb{C}}$ is a locally injective, surjective map of Riemann surfaces that serves as an analytic isomorphism $X(1) \cong \mathbb{P}^1_{\mathbb{C}}$. As a result, we can take j to be the generator of the function field of $X(1)$.

2.1.4 Example: Elliptic curves as Riemann surfaces

Given a rank 2 lattice $\Lambda = \omega_1\mathbb{Z} + \omega_2\mathbb{Z} \subset \mathbb{C}$ (for $\omega_1, \omega_2 \in \mathbb{C}^*$ and $\mathrm{Im}(\frac{\omega_2}{\omega_1}) > 0$), the Weierstrass $\wp$- function given by

$$\wp_\Lambda : \mathbb{C}/\Lambda \to \mathbb{C}$$

such that

$$\wp_\Lambda(z) := \frac{1}{z^2} + \sum_{\lambda \in \Lambda \setminus \{0\}} \left(\frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2} \right)$$

together with its derivative, $\wp'_\Lambda(z) = -2\sum_{\lambda\in\Lambda} \frac{1}{(z-\lambda)^3}$, satisfy the relation $(\wp'_\Lambda(z))^2 = 4(\wp_\Lambda(z^3)) - g_2(\Lambda)\wp_\Lambda(z) - g_3(\Lambda)$ (for a proof of this see [Dia & Shur], Proposition 1.4.1). Moreover, the identification space $\mathbb{C}/\Lambda$ with the quotient topology is a torus. Additionally it can be equipped with a complex structure; given a point $z \in \mathbb{C}/\Lambda$, take a neighbourhood $U_z \subset \mathbb{C}/\Lambda$ small enough such that the projection map $\pi : \mathbb{C} \to \mathbb{C}/\Lambda$ is a homeomorphism when restricted to a connected component of $V_z := \pi^{-1}(U_z)$ and its image. Then the pair $(U_z, \pi^{-1} \mid_{U_z})$ is a coordinate chart about z and one can easily check that these charts give a Riemann surface structure. In particular we have the following theorem which gives an embedding $\mathbb{C}/\Lambda \hookrightarrow \mathbb{P}^1_{\mathbb{C}}$:

Theorem 2.4 *The map $F : \mathbb{C}/\Lambda \to \mathbb{P}^2_{\mathbb{C}}$ given by*

$$F : z \mapsto \begin{cases} \left[\wp_\Lambda(z) : \wp'_\Lambda(z) : 1\right], & z \notin \Lambda \\ \left[0 : 1 : 0\right], & z \in \Lambda \end{cases}$$

is holomorphic and bijects with $E(\mathbb{C})$ the plane curve given in affine form by $y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda)$.

Proof: This is Theorem 6.14 in [Knapp]. □

A priori, $E(\mathbb{C})$ need not be non-singular. However, $\wp'_\Lambda(z)$ is easily seen to be an odd function. Hence $\wp'_\Lambda(-z) = -\wp'_\Lambda(z)$ and at the points where $-z \equiv z \bmod \Lambda$, we have $-\wp'_\Lambda(z) = \wp'_\Lambda(z)$ and z is a zero of $\wp'_\Lambda(z)$. But $-z \equiv z \bmod \Lambda \iff z \in \frac{1}{2}\Lambda \iff z \in \{\frac{w_1}{2}, \frac{w_2}{2}, \frac{w_1+w_2}{2}\}$. So at the half lattice points, $(\wp'_\Lambda(z))^2 = 4\wp_\Lambda(z)^3 - g_2(\Lambda)\wp_\Lambda(z) - g_3(\Lambda) = 0$, i.e. $\wp_\Lambda(z_i)$ are the roots of $4x^3 - g_2(\Lambda)x - g_3(\Lambda)$ (for $z_1 := \frac{w_1}{2}, z_2 := \frac{w_2}{2}, z_3 := \frac{w_1+w_2}{2}$). Notice that $\wp_\Lambda(z)$ can be extended to a degree 2 holomorphic map between compact Riemann surfaces $\wp_\Lambda : \mathbb{C}/\Lambda \to \mathbb{P}^1_{\mathbb{C}}$. In particular, $\wp_\Lambda$ ramifies at $z \in \mathbb{C}/\Lambda \iff \wp'_\Lambda(z) = 0$. But $\wp'_\Lambda(z_i) = 0$ and therefore at z_i, $\wp_\Lambda$ is a 2-to-1 map. This implies that $\wp_\Lambda(z_i) \neq \wp_\Lambda(z_j)$, for $i \neq j$ and thus the polynomial $4x^3 - g_2(\Lambda)x - g_3(\Lambda)$ has no repeated roots. As a result, the plane curve $E(\mathbb{C})$ is non-singular. The converse also holds:

Proposition 2.5 *Given a non-singular plane curve defined by $y^2 = 4x^3 - a_2x - a_3$, there exists a lattice Λ such that $a_2 = g_2(\Lambda), a_3 = g_3(\Lambda)$.*

Proof: This is Proposition 1.4.3 in [Dia & Shur]. □

So we define an **elliptic curve over** $\mathbb{C}$ to be any non-singular plane curve given in affine form by $y^2 = 4x^3 - a_2x - a_3$, with a point at infinity (notice that an affine change of coordinates of the form $y \mapsto 2y'$, gives the Weierstrass equation of an elliptic curve). As a consequence, any genus 1, compact Riemann surface is an elliptic curve over $\mathbb{C}$ and any elliptic curve over $\mathbb{C}$ is a compact Riemann surface of genus 1.

2.2 Modular curves as algebraic curves

This section is devoted to the study of some important concepts and tools of algebraic curves. We refer to a smooth 1-dimensional projective algebraic variety as an **algebraic curve**. Serre's GAGA states that the category of compact Riemann surfaces is equivalent to the category of algebraic curves over $\mathbb{C}$. As we have seen, modular curves and elliptic curves are Riemann surfaces and hence by Serre's GAGA, they are algebraic curves over $\mathbb{C}$. So initially we can write them as 1-dimensional projective algebraic varieties over $\mathbb{C}$. However, this does not give us the freedom of defining modular curves or elliptic curves over an arbitrary field that does not have an embedding in $\mathbb{C}$.

The main difference between the two worlds of algebraic curves and Riemann surfaces is that the former can be defined over an arbitrary field, whereas the latter is always modelled in $\mathbb{C}$ (notice the analogue between Lie groups and algebraic groups; the former is defined over fields of characteristic 0 such as $\mathbb{R}$ or $\mathbb{C}$, whereas the latter is defined over an arbitrary field of any characteristic and thus one needs to redefine everything in the language of algebraic geometry). This is why we need to develop machinery that will be able to imitate the Riemann surface setting algebraically. This will give us the freedom to work with fields of any characteristic and not just the complex numbers.

2.2.1 Valuations

We begin with the study of the algebraic analogue of the order of vanishing for meromorphic functions of a Riemann surface, that is valuations. Suppose C is an algebraic curve over a field K. Then for a point $P \in C$ we can associate to it a subring of $\bar{K}(C)$ (the function field of C over the algebraic closure of K), denoted by $\mathcal{O}_P(C)$, called the **local ring of C over $\bar{K}$ at P**, defined by $\mathcal{O}_P(C) := \{\frac{f}{g} \in \bar{K}(C) : g(P) \neq 0\}$. Then this ring has an ideal $\mathfrak{m}_P(C) := \{F \in \mathcal{O}_P(C) : F(P) = 0\}$. This ideal is in fact maximal in $\mathcal{O}_P(C)$ since the evaluation map $\mathcal{O}_P(C) \to \bar{K}$ given by $\frac{f}{g} \mapsto \frac{f(P)}{g(P)}$ is obviously a surjective ring homomorphism that has kernel $\mathfrak{m}_P(C)$. Hence $\mathcal{O}_P(C)/\mathfrak{m}_P(C) \cong \bar{K}$ and $\mathfrak{m}_P(C)$ is a maximal ideal. In fact, we can say even more about $\mathcal{O}_P(C)$ and its maximal ideal $\mathfrak{m}_P$; since an element $F \in \mathcal{O}_P(C)$ is not a unit $\iff F \in \mathfrak{m}_P$, $\mathfrak{m}_P = \{$ non-units of $\mathcal{O}_P(C)\}$ and every proper ideal of $\mathcal{O}_P(C)$ is contained in $\mathfrak{m}_P$. Thus $\mathcal{O}_P(C)$ has a unique maximal ideal $\mathfrak{m}_P$ and it is therefore a local ring. Moreover, since we insist that our algebraic curve C is smooth, the ring $\mathcal{O}_P(C)$ is a discrete valuation ring (see [Silverman 1], II , Proposition 1.1), which is equivalent to saying that $\mathfrak{m}_P$ is a principal ideal and $\mathcal{O}_P(C)$ is Noetherian and

local. A generator t of $\mathfrak{m}_P$ is called a **uniformizer** (or local parameter) at P.

This whole setup now allows us to define a family of discrete valuations on the function field $\bar{K}(C)$, i.e. for $P \in C$ a map $v_P : \bar{K}(C) \to \mathbb{Z} \cup \{\infty\}$ satisfying the following:
For any $F, G \in \bar{K}(C)^*$

- $v_P(FG) = v_P(F) + v_P(G)$
- $v_P(F+G) \geq \min\{v_P(F), v_P(G)\}$, with equality $\iff v_P(F) \neq v_P(G)$

Let $F \in \mathcal{O}_P(C) \setminus \{0\}$ and t a uniformizer at P. Then $\mathfrak{m}_P = \langle t \rangle$ and either F is a unit or not. If F is a non-unit then $F \in \mathfrak{m}_P$ and $F = tF_1$ for some $F_1 \in \mathcal{O}_P(C) \setminus \{0\}$. We can proceed with the same argument for F_1, that is F_1 is either a unit or not. If not, then $F_1 = tF_2$ for some $F_2 \in \mathcal{O}_P(C) \setminus \{0\}$. Iterating, this process needs to terminate since $\mathcal{O}_P(C)$ is Noetherian and $\langle F \rangle \subsetneq \langle F_1 \rangle \subsetneq \langle F_2 \rangle \subsetneq ...$ is an ascending chain of ideals. Hence we may write $F = t^{e_P} F'$ for some unit $F' \in \mathcal{O}_P(C)$ and this expression is unique. Indeed, if $t^{e_P} u_1 = t^{e'_P} u_2$ for units $u_1, u_2 \in \mathcal{O}_P(C)$ and without loss of generality $e_P \geq e'_P$, then $u_2 = t^{e_P - e'_P} u_1$ which implies that $e_P = e'_P$ and $u_1 = u_2$. So we have a map $v_P : \mathcal{O}_P(C) \to \mathbb{N} \cup \{\infty\}$ defined by

$$v_P : F \mapsto \begin{cases} e_P, & F = t^{e_P} F' \\ \infty, & F = 0 \end{cases}$$

We extend v_P on $\bar{K}(C)$ as follows:

$$v_P : \bar{K}(C) \to \mathbb{Z} \cup \{\infty\}$$

$$v_P\left(\frac{f}{g}\right) := v_P(f) - v_P(g).$$

Building on our Riemann surface analogue, we can now extend a rational function $\frac{f}{g} \in \bar{K}(C)$ to a function $\frac{f}{g} : C \to \mathbb{P}^1_{\bar{K}}$ as follows: Let $P \in C$. Then

$$\frac{f}{g}(P) := \begin{cases} 0, & \text{if } v_P(\frac{f}{g}) > 0 \\ \infty, & \text{if } v_P(\frac{f}{g}) < 0 \\ \frac{f(P)}{g(P)}, & \text{if } v_P(\frac{f}{g}) = 0 \end{cases}$$

2.2.2 Divisors

Let C be an algebraic curve over a field K. Then a **divisor of** C (over $\bar{K}$) is a formal sum $\sum_{P\in C(\bar{K})} n_P(P)$, where $n_P \in \mathbb{Z}$ and $n_P = 0$ for all but finitely many $P \in C(\bar{K})$. The **degree of a divisor** $\sum_{P\in C(\bar{K})} n_P(P)$, is defined as the integer $\sum_{P\in C(\bar{K})} n_P$. The free Abelian group

$$\mathrm{Div}_{\bar{K}}(C) := \left\{ \sum_{P\in C(\bar{K})} n_P(P) : n_P \in \mathbb{Z},\ \ n_P = 0,\ \text{ for all but finitely many } P \in C(\bar{K}) \right\}$$

is called the **divisor group of** C. It is easy to see that the map $\deg : \mathrm{Div}_{\bar{K}}(C) \to \mathbb{Z}$ is a group homomorphism. Hence the set of degree 0 divisors, denoted by $\mathrm{Div}^0_{\bar{K}}(C)$ is a subgroup of $\mathrm{Div}_{\bar{K}}(C)$. If $f \in \bar{K}(C)^*$ is a non-zero element of the function field of C, then its divisor is defined by $(f) := \sum_{P\in C(\bar{K})} v_P(f)(P)$. Divisors of the form (f), for $f \in \bar{K}(C)^*$ are called **principal divisors**. In a more general setting, if $f : X \to Y$ is a non-constant map between algebraic curves, $P \in X$ and $t \in \mathcal{O}_{f(P)}(Y)$ a uniformizer at $f(P)$, then we define the **ramification index of** f **at** P to be the valuation at P of the pull-back of t under f, i.e. $e_P(f) := v_P(f^*t)$. Then notice that $e_P(f) \geq 1$ and we say f is **unramified at** P when $e_P(f) = 1$. Now take any $Q \in Y$; we define the **degree of the map** f to be $\sum_{P\in f^{-1}(Q)} e_P(f)$ and one can show (essentially because we insist that our algebraic curve C is projective) that this is independent of the choice of the point Q and thus well defined (see [Hartshorne], II, Proposition 6.9). Now going back to the case where $f \in \bar{K}(C)^*$, as in the case of Riemann surfaces theory, one can show that $(f) = \sum_{P\in f^{-1}(0)} e_P(f)(P) - \sum_{P\in f^{-1}(\infty)} e_P(f)(P)$. As a result, taking degrees, we get that $\deg(f) = \sum_{P\in f^{-1}(0)} e_P(f) - \sum_{P\in f^{-1}(\infty)} e_P(f) = \deg f - \deg f = 0$. Therefore, we have that the set of principal divisors, denoted by $\mathrm{Div}^l_{\bar{K}}(C)$ is a subset of $\mathrm{Div}^0_{\bar{K}}(C)$. In fact, since valuations satisfy $v_P(fg) = v_P(f) + v_P(g)$ for $f, g \in \bar{K}(C)^*$, we have that $(fg) = (f) + (g)$ and $(\frac{1}{f}) = -(f)$. Hence $\mathrm{Div}^l_{\bar{K}}(C)$, is in fact a subgroup of $\mathrm{Div}^0_{\bar{K}}(C)$. A consequence of this is that we can take their quotient and form a very important group, called the (degree 0) **Picard group of** C. We denote this group by $\mathrm{Pic}^0_{\bar{K}}(C)$, which is also called the divisor class group.

We now move on to give an ordering on the set of divisors of C: Let $D = \sum_{P\in C} n_P(P) \in \mathrm{Div}(C)$ be an arbitrary divisor of C. Then we say D is an **effective divisor** and denote it by $D \geq 0$, when $n_P \geq 0$, for all $P \in C$. Moreover, we can now attach to D an important $\bar{K}$-vector space, defined by $\mathfrak{L}(D) := \{f \in \bar{K}(C)^* : (f) + D \geq 0\}$. We denote the dimension of this vector space by $l(D)$. One of the most important tools used in the study of algebraic curves is the so called Riemann-

Roch theorem, that states an expression of $l(D)$ in terms of the (algebraic) genus of C, the degree of D and $l(K_C - D)$. K_C is the so called **canonical divisor**, which is the divisor of a differential of C. It is beyond the scope of this essay to give an exposition of the construction of differentials on algebraic curves, for reference see for instance [Silverman 1], II, §4. Instead we will just assume that a canonical divisor always exists for an algebraic curve C and any two canonical divisors are linearly equivalent in the quotient $\mathrm{Div}_{\bar{K}}(C)/\mathrm{Div}^{l}_{\bar{K}}(C)$, the class of which is called the **canonical class**. Thus, $l(K_C)$ is independent of the choice of a differential of C. So we are now ready to state the theorem:

Theorem 2.6 ***Riemann- Roch:*** *Let C be an algebraic curve over a field K. Then there is an integer $g \geq 0$, called the **genus** of C such that for every divisor $D \in Div_{\bar{K}}(C)$,*

$$l(D) - l(K_C - D) = degD + 1 - g$$

Proof: [Hartshorne], IV, Theorem 1.3. □

Notice here that we defined the genus of an algebraic curve to be this integer such that the above equality holds. When an algebraic curve C is defined over $\mathbb{C}$, then this integer is equal to the genus of C as a Riemann surface. We have only seen how to define elliptic curves over $\mathbb{C}$. The way we define an elliptic curve over an arbitrary field is as follows: An **elliptic curve over a field** K is a pair $(E, 0_E)$, where E is a curve of genus 1 defined over K and $0_E \in E(K)$. A priori, it is not so clear how this definition is related to the definition of an elliptic curve over $\mathbb{C}$. However, the following lemma gives that the two definitions agree when $K = \mathbb{C}$ and hence this new definition generalizes the previous one:

Lemma 2.7 *If C is a genus 1 algebraic curve defined over a field K with a K-rational point P, then we have an embedding $C \hookrightarrow \mathbb{P}^2_{\bar{K}}$, given by $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$.*

Proof: This is essentially Riemann-Roch at its best. Let P be a K-rational point in C. Then Riemann-Roch theorem states that $l(D) - l(K_C - D) = \mathrm{deg}D - g + 1$. However, we have that $\mathrm{deg}K_C = 2g - 2 = 0$ ([Silverman 1], II, Corollary 5.5). Thus for $t = 1, .., 6$, $\mathrm{deg}K_C - t(P) < 0$. If $f \in \mathfrak{L}(K_C - t(P))$ is non-zero, then by definition $(f) + K_C - t(P) \geq 0$. But taking degrees, we have that $\deg(f) + K_C - t(P) = \deg(f) + \mathrm{deg}K_C - t(P) < 0$ which is a contradiction. Hence $l(K_C - t(P)) = 0$. So for $t = 1, ..., 6$, Riemann-Roch reduces to $l(D) = \mathrm{deg}D - g + 1 = \mathrm{deg}D - 1 + 1 = \mathrm{deg}D$ and $l(t(P)) = t$. Moreover, notice the inclusion $\mathfrak{L}(P) \subseteq \mathfrak{L}(2(P)) \subseteq ... \subseteq \mathfrak{L}(6(P))$. Explicitly, we have that

- $\mathfrak{L}(P) = \langle 1 \rangle$, since $\mathfrak{L}(P)$ is 1-dimensional and includes the constant functions
- $\mathfrak{L}(2(P)) = \langle 1, x \rangle$ and the function x has a double pole at P
- $\mathfrak{L}(3(P)) = \langle 1, x, y \rangle$ and the function y has a pole of order 3 at P
- $\mathfrak{L}(4(P)) = \langle 1, x, y, x^2 \rangle$, since the function x^2 has a pole of order 4 at P
- $\mathfrak{L}(5(P)) = \langle 1, x, y, x^2, xy \rangle$, since the function xy has a pole of order 5 at P
- $\mathfrak{L}(6(P)) = \langle 1, x, y, x^2, xy, x^3 \rangle$, since the function x^3 has a pole of order 6 at P

However notice that the function y^2 has a pole of order 6 at P and hence it is an element of $\mathfrak{L}(6(P))$. Therefore there exists elements $a'_1, ..., a'_6 \in \bar{K}$ not all zero, such that $y^2 + a'_1xy + a'_2y = a'_3x^3 + a'_4x^2 + a'_5x + a'_6$. Under a change of variables the relation can be rewritten as $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, for some $a_1, ..., a_4, a_6 \in K$. As a result, $\mathfrak{L}(3(P))$ defines an embedding

$$C \hookrightarrow \mathbb{P}^2_{\bar{K}}$$

$$P \mapsto [1 : x(P) : y(P)]$$

given by $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$. □

If the characteristic of K is different from 2, then we can complete the square and under a change of variables reduce the equation $y^2+a_1xy+a_3y = x^3+a_2x^2+a_4x+a_6$ to $y^2 = x^3 + b_1x^2 + b_2x + b_3$. In addition, if characteristic of K is different from 2 and 3 then we can make a further change of variable $x \mapsto x + \frac{1}{3}b_1$ to get the equation $y^2 = x^3 + Ax + B$.

Defining an elliptic curve as an abstract algebraic curve, as it was stated at the beginning of this section, allows us to define it over arbitrary fields such as a finite field. In particular it allows us to reduce an elliptic curve defined over $\mathbb{Q}$ modulo a prime p of good reduction (i.e. $p \nmid 2\Delta$, Δ the discriminant of E) and get a reduced elliptic curve $\bar{E}/\mathbb{F}_p$. We can then count the number of points $\#\bar{E}(\mathbb{F}_p)$ and define a number $a_p(E) := p + 1 - \#\bar{E}(\mathbb{F}_p)$. This integer $a_p(E)$ is called the **trace of the Frobenius at p** and the choice of this name will become apparent in section 3.4, Theorem 3.9.

Until now, we have defined the whole setup over the algebraic closure of the field over which our algebraic curve is defined. It is important to see what happens when we restrict ourselves to divisors defined over the base field we are working with (where we assume the base field to be perfect). First we say what does it mean for **a divisor to be defined over the base field**: Let C/K be an algebraic curve and

take $D = \sum_{P \in C} n_P(P) \in \mathrm{Div}_{\bar{K}}(C)$. Then D is defined over K when it is fixed by the action of $\mathrm{Gal}(\bar{K}/K)$, i.e. for any $\sigma \in \mathrm{Gal}(\bar{K}/K)$, $D^\sigma = \sum_{P \in C} n_P(P^\sigma) = D$. We denote by $\mathrm{Div}_K(C)$ the free Abelian subgroup of $\mathrm{Div}_{\bar{K}}(C)$ that consists of divisors on C defined over K. We then have the following important proposition:

Proposition 2.8 *Let C/K be an algebraic curve and $D \in Div_K(C)$. Then $\mathfrak{L}(D)$ has a basis that consists of functions in $K(C)$.*

Proof: [Silverman 1], II, Proposition 5.8. □

This theorem essentially implies that the vector spaces $\mathfrak{L}_{\bar{K}}(D) := \{f \in \bar{K}(C)^* : (f) + D \geq 0\}$ and $\mathfrak{L}_K(D) := \{f \in K(C)^* : (f) + D \geq 0\}$ defined over $\bar{K}$ and K respectively have the same dimensions. Hence the Riemann-Roch theorem still works even when we are considering divisors D defined over the base field K, with associated vector spaces $\mathfrak{L}_K(D) := \{f \in K(C)^* : (f) + D \geq 0\}$.

2.2.3 The Weil pairing

In this section we briefly discuss an important map, called the Weil pairing. This is a bilinear map $E[N] \times E[N] \to \mu_N$, μ_N the group of N-th roots of unity that satisfies properties of an inner product. It will provide a very useful tool throughout this essay.

We first give a theorem that will help us in the construction of the Weil pairing. Let $h : X \to Y$ be a non-constant morphism between algebraic curves. Then we can define forward and reverse maps on the (degree 0) Picard groups of X and Y as follows:

$h_* : \mathrm{Pic}^0_{\bar{K}}(X) \to \mathrm{Pic}^0_{\bar{K}}(Y), \qquad h_*([\sum_P n_P(P)]) := [\sum_P n_P(h(P))]$ and

$h^* : \mathrm{Pic}^0_{\bar{K}}(Y) \to \mathrm{Pic}^0_{\bar{K}}(X), \qquad h^*([\sum_Q n_Q(Q)]) := [\sum_Q n_Q \sum_{P \in h^{-1}(Q)} e_P(h)(P)]$.

Considering the case where C is an elliptic curve E, we have the following powerful theorem:

Theorem 2.9 *The map*

$$Div_{\bar{K}}(E) \to E(\bar{K})$$

$$\sum n_P(P) \mapsto \sum [n_p]P$$

(where $[n_P]$ is the multiplication by n_P map in End(E)), induces an isomorphism $Pic^0_{\bar{K}}(E) \cong E(\bar{K})$. Moreover $\sum n_P(P)$ is principal $\iff$ $\sum n_P = 0$ and $\sum [n_P]P = 0_E$.

Proof: [Dia & Shur], Theorem 7.3.3. □

Let us fix a field K of characteristic 0 and denote by μ_N the group of N-th roots of unity in $\bar{K}$. Let E denote an elliptic curve over K and $E[N] := \{P \in \bar{K} : [N]P = 0_E\}$ the N-torsion subgroup of E. The structure theorem of Abelian groups and the separability of the multiplication by N map give $E[N] \cong \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$. Take two points $P, Q \in E[N]$, not necessarily distinct. Notice that since $[N]P = 0_E$, then $[N]P + [N]0_E = 0_E$ and we can invoke Theorem 2.9; there exists $f \in \bar{K}(E)$ with divisor $(f) = N(P) - N(0_E)$. Moreover, the map $[N] : E(\bar{K}) \to E(\bar{K})$ is unramified (this is [Silverman 1], III, Theorem 4.10(c)) and thus pulling back the divisor of f by $[N]$ gives $[N]^*(f) = N\sum_{R\in[N]^{-1}(P)}(R) - N\sum_{S\in[N]^{-1}(0_E)}(S) = (f \circ [N])$. Elements of the fibre $[N]^{-1}(P)$ have the property that they live in the kernel of the $[N^2]$ map. Hence $[N]^{-1}(P) \subseteq E[N^2]$ and $[N]^{-1}(0_E) = E[N]$. In particular, fixing an element $R \in [N]^{-1}(P)$, the map $E[N] \to [N]^{-1}(P)$ given by $S \to R + S$ is a bijection. So we can rewrite $[N]^*(f) = N\sum_{S\in E[N]}(R + S) - (S)$. Moreover the divisor $\alpha = \sum_{S\in E[N]}(R + S) - (S)$ has degree 0 and since $\#E[N] = N^2$, we have that $\sum_{S\in E[N]} R + S - S = [N^2]R = 0_E$. Invoking Theorem 2.9 again, there exists $g \in \bar{K}(E)$ such that $(g) = \alpha$. Therefore $N(g) = (g^N) = N\alpha = [N]^*(f) = (f \circ [N])$ and possibly after rescaling g if necessary, $f \circ [N] = g^N$. But notice that from this deduction it follows that g^N is constant. Indeed fixing some point $x \in E(\bar{K})$, $g(x + Q)^N = f([N]x + [N]Q) = f([N]x) = g(x)^N$. Consequently, the function $\frac{g(x+Q)}{g(x)} \in \bar{K}(E)$ satisfies $(\frac{g(x+Q)}{g(x)})^N = \frac{g(x+Q)^N}{g(x)^N} = 1$, i.e. it is an Nth root of unity in $\bar{K}(E)$ (the group of which we denote by μ_N).

Definition 2.10 - ***Weil pairing***
The Weil pairing of two points $P, Q \in E[N]$ is the function

$$e_N(Q, P) := \frac{g(x + Q)}{g(x)} \in \mu_N$$

for any point $x \in E(\bar{K})$.

We deduce some important properties:

Proposition 2.11 *The Weil pairing is:*

1. *Bilinear:* $e_N(Q_1 + Q_2, P) = e_N(Q_1, P)e_N(Q_2, P)$;
2. *Alternating:* $e_N(Q, Q) = 1$, $e_N(Q, P) = e_N(P, Q)^{-1}$;
3. *Non-degenerate: If* $e_N(Q, P) = 1$ *for all* $Q \in E[N]$, *then* $P = 0_E$;
4. *Galois equivariant:* $e_N(Q^\sigma, P^\sigma) = e_N(Q, P)^\sigma$, *for all* $\sigma \in Gal(\bar{K}/K)$;
5. *Invariant under isomorphisms of elliptic curves*

Proof: [Dia & Shur], Proposition 7.4.1. □

Hence we have a map $e_N : E[N] \times E[N] \to \mu_N$ that is bilinear and non-degenerate. In particular we have the following lemma:

Lemma 2.12 *Given an elliptic curve* E *over a field* K *we have that the Weil pairing is surjective and* $K(E[N]) \supseteq \mu_N$ *(where* μ_N *is the group of* N*-th roots of unity).*

Proof: The image of e_N on the product $E[N] \times E[N]$ is a subgroup of μ_N, i.e. it is the group of N'-th roots of unity, for some $N' \mid N$. So for any points $P, Q \in E[N]$, $e_N(Q, P)^{N'} = 1 = e_N(Q, N'P) = e_N(N'Q, P)$. So fixing P and varying Q in $E[N]$, by the non-degeneracy of e_N we see that $N'P = 0_E$. But P was arbitrary and since $E[N]$ contains points of order N, we conclude that we must have $N' = N$. This proves e_N is surjective.

For the second part of the theorem we make use of the Galois equivariance property of the Weil pairing. Consider $P, Q \in E[N]$ which have coordinates in $K(E[N])$. Then for any $\sigma \in \mathrm{Gal}(\bar{K}/K(E[N]))$, P, Q are fixed by the action of σ and thus $e_N(P^\sigma, Q^\sigma) = e_N(P, Q)^\sigma = e_N(P, Q)$. As a result, $e_N(P, Q) \in \mu_N$ is also fixed by σ and since e_N is surjective, we have that $\mu_N \subseteq K(E[N])$. □

2.3 Modular curves as moduli spaces

We begin our study of this section by revisiting our archetypical example of $X(1)$ and demonstrating how it can serve as a moduli space to the set $\mathrm{Ell}(\mathbb{C})$, the set of isomorphism classes of elliptic curves over $\mathbb{C}$. This example also provides motivation as follows; since orbits of the action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathbb{H}$ correspond to isomorphism classes of elliptic curves over $\mathbb{C}$, then one would expect that the inclusion $\Gamma(N) \subseteq \Gamma_1(N) \subseteq \Gamma_0(N) \subseteq \mathrm{SL}_2(\mathbb{Z})$ would imply that orbits under these congruence subgroups would correspond to finer parametrizations of elliptic curves over $\mathbb{C}$.

2.3.1 Example 1.1 revisited: $X(1)$ as a moduli space

Let us denote by $\mathrm{Ell}(\mathbb{C})$ the set of elliptic curves over $\mathbb{C}$ of the form $y^2 = 4x^3+Ax+B$. We define two elliptic curves $y^2 = 4x^3 + A_1x + B_1$, $y^2 = 4x^3 + A_2x + B_2$ over a field K to be isomorphic over K when there exists $\alpha \in K^*$ such that $\alpha^4 A_1 = A_2$ and $\alpha^6 B_1 = B_2$. The isomorphism is given by the morphism $(x, y) \mapsto (\alpha^2 x, \alpha^3 y)$. Given $E \in \mathrm{Ell}(\mathbb{C})$, there exists a rank 2 lattice $\Lambda \subset \mathbb{C}$ such that $\mathbb{C}/\Lambda$ corresponds to E under the map F of Theorem 2.4 (this is guaranteed by Proposition 2.5). Moreover, suppose E' is another element of $\mathrm{Ell}(\mathbb{C})$ with corresponding lattice Λ'. To ask whether E and E' are isomorphic over $\mathbb{C}$ is equivalent to ask whether there exists $\alpha \in \mathbb{C}^*$ such that $\Lambda' = \alpha\Lambda$ (in this case Λ and Λ' are said to be **homothetic**). To see this, notice that E' is given in affine form by $y^2 = 4x^3 - g_2(\Lambda') - g_3(\Lambda')$. But $g_2(\Lambda') = g_2(\alpha\Lambda) = 60G_4(\alpha\Lambda) = 60\sum_{\lambda\in\alpha\Lambda} \frac{1}{\lambda^4} = 60\sum_{\lambda\in\Lambda} \frac{1}{\frac{1}{\alpha^4}\lambda^4} = 60\sum_{\lambda\in\Lambda} \frac{\alpha^4}{\lambda^4} = \alpha^4 g_2(\Lambda)$. Similarly $g_3(\Lambda') = g_3(\alpha\Lambda) = \alpha^6 g_3(\Lambda)$. Thus $y^2 = 4x^3 - g_2(\Lambda') - g_3(\Lambda') = 4x^3 - \alpha^4 g_2(\Lambda) - \alpha^6 g_3(\Lambda)$ and $y^2 = 4x^3 - g_2(\Lambda) - g_3(\Lambda)$ is the affine form of E. Hence E and E' are isomorphic over $\mathbb{C}$.

So we can now restrict our attention to rank 2 lattices in $\mathbb{C}$ up to homothety. A canonical form of this would be the lattice $\Lambda_\tau = \mathbb{Z} + \tau\mathbb{Z}$; given $\Lambda = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$ we take the homothetic lattice $\frac{1}{\omega_1}\Lambda = \mathbb{Z} + \frac{\omega_2}{\omega_1}\mathbb{Z}$ (recall that Λ is a rank 2 lattice and $\omega_1 \neq 0$). A $\mathbb{Z}$-basis of Λ_τ is given by $\{1, \tau\}$. Any other basis is given by a transformation under a matrix $G := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z})$. Since we ask for the basis of our lattice to live in the upper half plane $\mathbb{H}$, we insist that the determinant of the matrix is $+1$, i.e. $G \in \mathrm{SL}_2(\mathbb{Z})$. Also, another basis of Λ_τ would be $\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 \\ \tau \end{pmatrix} = \begin{pmatrix} a+b\tau \\ c+d\tau \end{pmatrix}$ and in fact all basis of Λ_τ are given by the set $\{(a+b\tau, c+d\tau) : a, b, c, d \in \mathbb{Z}, ad-bc = 1\}$. So $\Lambda_\tau = (a+b\tau)\mathbb{Z} + (c+d\tau)\mathbb{Z}$ which is homothetic to $\mathbb{Z} + \frac{a+b\tau}{c+d\tau}\mathbb{Z}$ ($c + d\tau \neq 0$, otherwise if $c = 0$, then $d = 0$ which is a contradiction. If $d = 0$ then $c = 0$ which is also a contradiction. If both $c, d \neq 0$, then $\tau = \frac{-c}{d} \notin \mathbb{H}$). But $\frac{a+b\tau}{c+d\tau} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \tau$ and as a result Λ_τ and $\Lambda_{\gamma\cdot\tau}$ (for $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$) are homothetic. In particular this also shows that if τ and τ' are in the same $\mathrm{SL}_2(\mathbb{Z})$ orbit, then Λ_τ and $\Lambda_{\tau'}$ are homothetic and therefore the elliptic curves E_τ and $E_{\tau'}$ are isomorphic. Conversely, if we are given that $E_\tau \cong E_{\tau'}$, for corresponding lattices $\Lambda_\tau = \mathbb{Z} + \tau\mathbb{Z}$, $\Lambda_{\tau'} = \mathbb{Z} + \tau'\mathbb{Z}$, then there exists $\alpha \in \mathbb{C}^*$ such that $\alpha(\mathbb{Z} + \tau\mathbb{Z}) = \alpha\mathbb{Z} + \alpha\tau\mathbb{Z} = \mathbb{Z} + \tau'\mathbb{Z}$. So there exists a change of basis matrix $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$, with $\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} \tau' \\ 1 \end{pmatrix} = \begin{pmatrix} \alpha\tau \\ \alpha \end{pmatrix}$. This

implies that $\alpha = c\tau' + d$ and $\alpha\tau = a\tau' + b$, thus $\frac{\alpha\tau}{\alpha} = \frac{a\tau'+b}{c\tau'+d} = \tau$. In other words, $\gamma \cdot \tau' = \tau$.

To conclude, the orbits of the action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathbb{H}$ correspond bijectively to isomorphism classes of elliptic curves over $\mathbb{C}$. Since we are interested in the compactified modular curve $X(1) = \mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H} \cup \{\infty\}$ we identify the cusp ∞ with a generalised elliptic curve of level 1 structure. As a final remark, observe that since the points of $X(1)$ correspond to isomorphism classes of elliptic curves over $\mathbb{C}$, we can attach to an isomorphism class $\{E : y^2 = 4x^3 - g_2(\alpha\Lambda)x - g_3(\alpha\Lambda) : \alpha \in \mathbb{C}^*\}$ an invariant called the j-invariant which is the value of the function $j(\tau) = \frac{1728 g_2(\tau)^3}{\Delta(\tau)}$ (recall that the j-function is $\mathrm{SL}_2(\mathbb{Z})$ invariant - see example 2.1.3) for $\Lambda = \mathbb{Z} + \tau\mathbb{Z}$ being the lattice corresponding to the above isomorphism class.

2.3.2 The main theorem

The first notion we need to consider is the notion of an isogeny. As we have seen in Theorem 2.4 and Proposition 2.5, an elliptic curve over $\mathbb{C}$ corresponds to a rank 2 lattice $\Lambda \subset \mathbb{C}$, which is in fact a subgroup of the additive group $\mathbb{C}$. Given two elliptic curves $E_1/\mathbb{C}, E_2/\mathbb{C}$ with corresponding lattices Λ_1, Λ_2, an **isogeny** between them is a non-zero holomorphic homomorphism $\phi : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$. The following lemma gives structural information of an isogeny:

Lemma 2.13 *Suppose $\phi : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$ is an isogeny. Then there exists $\alpha \in \mathbb{C}^*$ such that $\phi(z + \Lambda_1) = \alpha z + \Lambda_2$.*

Proof: This is Proposition 1.3.2 and Corollary 1.3.3 in [Dia & Shur]. □

So two elliptic curves $E_1/\mathbb{C}, E_2/\mathbb{C}$ are isomorphic over $\mathbb{C}$ when there exists an isogeny $\phi : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$ that is an isomorphism. What we next consider is the notion of a modular pair of level N. We define a **modular pair of level** N to be the pair (E, E_N) where $E/\mathbb{C}$ is an elliptic curve and E_N is some data of the N-torsion subgroup $E[N]$. We will refer to two modular pairs $(E, E_N), (E', E'_N)$ as being isomorphic when there exists an isogeny $\phi : E \to E'$ that is an isomorphism, taking E_N to E'_N. In the case of $X(1)$, $\mathrm{SL}_2(\mathbb{Z})$ is a large arithmetic group and hence its action on $\mathbb{H}$ identifies too many points. As a result, the quotient $X(1)$ is not fine enough to distinguish between elliptic curves with different torsion data. However, if we consider a smaller congruence subgroup Γ of $\mathrm{SL}_2(\mathbb{Z})$, the resulting identification space $Y(\Gamma)$ is finer and more interesting.

Before we move on to the main theorem that will give us a moduli interpretation of the modular curves $Y_0(N), Y_1(N), Y(N)$, let us first investigate how

the N-torsion subgroup $E[N]$ of an elliptic curve $E/\mathbb{C}$ with corresponding lattice $\Lambda = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$, sits in the torus $\mathbb{C}/\Lambda$. Suppose $P \in E[N]$ with corresponding point on $\mathbb{C}/\Lambda$, $z + \Lambda$ (recall from Theorem 2.4 the bijection $F : \mathbb{C}/\Lambda \to E(\mathbb{C})$). Then

$$[N]P = 0_E \iff N(z + \Lambda) = \Lambda$$

$$\iff Nz \in \Lambda$$

$$\iff z \in \frac{\omega_1}{N}\mathbb{Z} + \frac{\omega_2}{N}\mathbb{Z}.$$

Hence $E[N]$ corresponds to the subgroup $(\frac{\omega_1}{N}\mathbb{Z} + \frac{\omega_2}{N}\mathbb{Z}) + \Lambda \subseteq \mathbb{C}/\Lambda$. In particular, if C is a subgroup of $E[N]$, then C corresponds to a subgroup of $(\frac{\omega_1}{N}\mathbb{Z} + \frac{\omega_2}{N}\mathbb{Z}) + \Lambda$. We are now ready to move on to the main theorem of this section that describes the parametrized spaces for the modular curves $Y_0(N), Y_1(N), Y(N)$ (this is Theorem 1.5.1 in [Dia & Shur]):

Theorem 2.14 *Let N be a positive integer, $\tau \in \mathbb{H}$ and E_τ the elliptic curve over $\mathbb{C}$ corresponding to the lattice $\Lambda_\tau = \mathbb{Z} + \tau\mathbb{Z}$. Then we have the following:*

1. *The moduli space for $Y_0(N)$ is the set of modular pairs*

$$S_0(N) := \{(E_\tau, \frac{1}{N}\mathbb{Z} + \Lambda_\tau) : \tau \in \mathbb{H}\}.$$

In particular, two pairs $(E_\tau, \frac{1}{N}\mathbb{Z} + \Lambda_\tau)$ and $(E_{\tau'}, \frac{1}{N}\mathbb{Z} + \Lambda_{\tau'})$ are isomorphic if and only if $\Gamma_0(N)\tau = \Gamma_0(N)\tau'$. Thus there is a bijection $\psi_0 : S_0(N) \longrightarrow Y_0(N)$ given by $(E_\tau, \frac{1}{N}\mathbb{Z} + \Lambda_\tau) \mapsto \Gamma_0(N)\tau$.

2. *The moduli space for $Y_1(N)$ is the set of modular pairs*

$$S_1(N) := \{(E_\tau, \frac{1}{N} + \Lambda_\tau) : \tau \in \mathbb{H}\}.$$

Two pairs $(E_\tau, \frac{1}{N} + \Lambda_\tau)$ and $(E_{\tau'}, \frac{1}{N} + \Lambda_{\tau'})$ are isomorphic if and only if $\Gamma_1(N)\tau = \Gamma_1(N)\tau'$. So there is a bijection $\psi_1 : S_1(N) \longrightarrow Y_1(N)$ given by $(E_\tau, \frac{1}{N} + \Lambda_\tau) \mapsto \Gamma_1(N)\tau$.

3. *The moduli space for $Y(N)$ is the set of modular pairs*

$$S(N) := \{(E_\tau, (\frac{\tau}{N} + \Lambda_\tau, \frac{1}{N} + \Lambda_\tau)) : \tau \in \mathbb{H}\}.$$

Moreover, the pairs $(E_\tau, (\frac{\tau}{N} + \Lambda_\tau, \frac{1}{N} + \Lambda_\tau))$ and $(E_{\tau'}, (\frac{\tau'}{N} + \Lambda_{\tau'}, \frac{1}{N} + \Lambda_{\tau'}))$ are isomorphic if and only if $\Gamma(N)\tau = \Gamma(N)\tau'$ and thus there is a bijection $\psi : S(N) \longrightarrow Y(N)$, $(E_\tau, (\frac{\tau}{N} + \Lambda_\tau, \frac{1}{N} + \Lambda_\tau)) \mapsto \Gamma(N)\tau$.

We summarize the content of this theorem:

- $Y_0(N)$ parametrizes modular pairs $(E/\mathbb{C}, C)$, where C is a cyclic subgroup of $E[N]$ of order N.
- $Y_1(N)$ parametrizes modular pairs $(E/\mathbb{C}, Q)$, where Q is a point in $E[N]$ of order N.
- Suppose (P, Q) is a $\mathbb{Z}/N\mathbb{Z}$-basis of $E[N]$. Recall that the Weil pairing $e_N(P, Q)$ has image in the group of N-th roots of unity in $\mathbb{C}$, that we denote by μ_N. So $e_N(P, Q) = e^{\frac{2\pi ik}{N}}$ for some $k \in \mathbb{Z}$ and under normalization we may take $k = 1$. Then $Y(N)$ parametrizes modular pairs $(E/\mathbb{C}, (P, Q))$ where (P, Q) is a $\mathbb{Z}/N\mathbb{Z}$-basis of $E[N]$ with $e_N(P, Q) = e^{\frac{2\pi i}{N}}$.

The proof of the theorem is in [Dia & Shur], Theorem 1.5.1. However, since the techniques employed are important, we reproduce it here:

Proof of Theorem 2.14:

1. Take any modular pair (E, C) where $E/\mathbb{C}$ is an elliptic curve and C a cyclic subgroup of $E[N]$ of order N. Then E corresponds to a rank 2 lattice $\Lambda = \omega_1\mathbb{Z}+\omega_2\mathbb{Z}$ and C to a sublattice $\Lambda' = \frac{c\omega_1+d\omega_2}{N}\mathbb{Z}$, for some $c, d \in \mathbb{Z}$. But $\frac{1}{\omega_2}\Lambda = \mathbb{Z} + \frac{\omega_1}{\omega_2}\mathbb{Z} =: \Lambda_\tau$, where $\tau := \frac{\omega_1}{\omega_2} \in \mathbb{H}$ and $\frac{1}{\omega_2}\Lambda' = \frac{c\tau+d}{N}\mathbb{Z} =: \Lambda'_\tau$. Then the elliptic curve E_τ corresponding to Λ_τ is isomorphic to E over $\mathbb{C}$, since Λ and Λ_τ are homothetic (see section 2.3.1). However, since $\frac{c\tau+d}{N}$ has order equal to N in the torus $\mathbb{C}/\Lambda_\tau$, we have that $\gcd(c, d, N) = 1$. Hence by Euclid's algorithm there exists $k, a, b \in \mathbb{Z}$ such that $ad - bc - kN = 1$. But then the matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ has determinant 1 mod N and thus reduces to $\begin{pmatrix} \bar{a} & \bar{b} \\ \bar{c} & \bar{d} \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ mod N.

Since the map $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ mod N is surjective (see Lemma 6.1), we may lift the matrix $\begin{pmatrix} \bar{a} & \bar{b} \\ \bar{c} & \bar{d} \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ to $\gamma := \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$. However, since $\Lambda'_\tau = \frac{c\tau+d}{N}\mathbb{Z}$ and in the torus $\mathbb{C}/\Lambda_\tau$ we are interested in the points with

$c, d \bmod N$, we may take without loss of generality $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$. Let $\tau' := \gamma \cdot \tau$ and consider

$$\begin{aligned} \Lambda_\tau = \mathbb{Z} + \tau\mathbb{Z} &= (a\tau + b)\mathbb{Z} + (c\tau + d)\mathbb{Z} \quad \text{(under change of basis)} \\ &= (c\tau + d)(\tfrac{a\tau+b}{c\tau+d}\mathbb{Z} + \mathbb{Z}) \\ &= (c\tau + d)(\gamma \cdot \tau\mathbb{Z} + \mathbb{Z}) = (c\tau + d)\Lambda_{\tau'}. \end{aligned}$$

As a result, $\Lambda_{\tau'}$ is homothetic to Λ_τ and $E_{\tau'}$ is isomorphic to E_τ. We also have that $\Lambda'_\tau = \frac{c\tau+d}{N}\mathbb{Z} = (c\tau + d)\frac{1}{N}\mathbb{Z} = (c\tau + d)\Lambda'_{\tau'}$ (where we define $\Lambda'_{\tau'} := \frac{1}{N}\mathbb{Z}$). Thus the modular pair (E, C) is isomorphic to $(E_{\tau'}, \frac{1}{N}\mathbb{Z} + \Lambda_{\tau'})$.

Now suppose we have 2 pairs $(E_\tau, \frac{1}{N}\mathbb{Z}+\Lambda_\tau)$ and $(E_{\tau'}, \frac{1}{N}\mathbb{Z}+\Lambda_{\tau'})$, with $\tau, \tau' \in \mathbb{H}$ in the same $\Gamma_0(N)$-orbit, i.e. $\gamma \cdot \tau = \tau'$ for some $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$. Then as before, $(c\tau+d)\Lambda_{\tau'} = \Lambda_\tau$ and E_τ is isomorphic to $E_{\tau'}$. Moreover, $(c\tau+d)(\frac{1}{N}\mathbb{Z}+\Lambda_{\tau'}) = \frac{c\tau+d}{N}\mathbb{Z}+\Lambda_\tau = \frac{d}{N}\mathbb{Z}+\Lambda_\tau$, since $c \equiv 0 \bmod N$. But since $h :=\gcd(d, N) = 1$ (otherwise if $h > 1$, then $h \mid \det\gamma$ and $\det\gamma$ is not a unit in $\mathbb{Z}/N\mathbb{Z}$), $\frac{d}{N}\mathbb{Z} + \Lambda_\tau$ is an order N subgroup of $E_\tau[N]$ isomorphic to $\frac{1}{N}\mathbb{Z} + \Lambda_\tau$. Hence the two modular pairs are isomorphic.

Conversely, suppose we have two isomorphic modular pairs $(E_\tau, \frac{1}{N}\mathbb{Z} + \Lambda_\tau)$, $(E_{\tau'}, \frac{1}{N}\mathbb{Z} + \Lambda_{\tau'})$. Then the lattices $\Lambda_\tau, \Lambda_{\tau'}$ are homothetic and there exists $\alpha \in \mathbb{C}^*$ such that $\alpha\Lambda_\tau = \alpha\mathbb{Z} + \alpha\tau\mathbb{Z} = \Lambda_{\tau'} = \mathbb{Z} + \tau'\mathbb{Z}$ and $\alpha(\frac{1}{N}\mathbb{Z} + \Lambda_\tau) = \frac{\alpha}{N}\mathbb{Z} + \Lambda_{\tau'} = \frac{1}{N}\mathbb{Z}+\Lambda_{\tau'}$. So there exists a change of basis matrix $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ such that $\gamma \begin{pmatrix} \tau' \\ 1 \end{pmatrix} = \begin{pmatrix} a\tau' + b \\ c\tau' + d \end{pmatrix} = \begin{pmatrix} \alpha\tau \\ \alpha \end{pmatrix}$. Thus $\alpha = c\tau' + d$. Replacing this into the equation $\frac{\alpha}{N}\mathbb{Z} + \Lambda_{\tau'} = \frac{1}{N}\mathbb{Z} + \Lambda_{\tau'}$, gives $\frac{c\tau'+d}{N}\mathbb{Z} + \Lambda_{\tau'} = \frac{1}{N}\mathbb{Z} + \Lambda_{\tau'}$. This implies that $c \equiv 0 \bmod N$ and $\gcd(d, N) = 1 \implies \gamma \in \Gamma_0(N)$. From $\begin{pmatrix} a\tau' + b \\ c\tau' + d \end{pmatrix} = \begin{pmatrix} \alpha\tau \\ \alpha \end{pmatrix}$ we get that $\frac{a\tau'+b}{c\tau'+d} = \tau$, i.e. $\gamma \cdot \tau' = \tau$ and τ, τ' are in the same $\Gamma_0(N)$-orbit.

2. This is exactly as in case *(1)*, though extra care needs to be taken for $d \equiv 1 \bmod N$ (for $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_1(N)$).

3. Take a modular pair $(E, (P, Q))$ where $E/\mathbb{C}$ is an elliptic curve and P, Q generators of $E[N]$ with Weil pairing $e^{\frac{2\pi i}{N}}$. Let $\Lambda = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$ be the lattice corresponding to E, $P = \frac{a\omega_1+b\omega_2}{N} + \Lambda$, $Q = \frac{c\omega_1+d\omega_2}{N} + \Lambda$ (for some integers a, b, c, d). Then as in case *(1)*, Λ is homothetic to the lattice Λ_τ and E is isomorphic to E_τ (for $\tau = \frac{\omega_1}{\omega_2}$). Under this isomorphism we have that P, Q get mapped to the points $P_\tau = \frac{a\tau+b}{N} + \Lambda_\tau$ and $Q_\tau = \frac{c\tau+d}{N} + \Lambda_\tau$ respectively. Moreover isomorphisms of elliptic curves preserve the Weil pairing (see Proposition 2.11) and hence $e_N(P_\tau, Q_\tau) = e^{\frac{2\pi i}{N}}$. But

$$\begin{aligned} e_N(P_\tau, Q_\tau) &= e_N(\tfrac{a\tau+b}{N}, \tfrac{c\tau+d}{N}) \\ &= e_N(\tfrac{a\tau}{N}, \tfrac{c\tau}{N}) e_N(\tfrac{a\tau}{N}, \tfrac{d}{N}) e_N(\tfrac{b}{N}, \tfrac{c\tau}{N}) e_N(\tfrac{b}{N}, \tfrac{d}{N}) \\ &= e_N(\tfrac{\tau}{N}, \tfrac{1}{N})^{ad} e_N(\tfrac{\tau}{N}, \tfrac{1}{N})^{-bc} \\ &= e_N(\tfrac{\tau}{N}, \tfrac{1}{N})^{ad-bc} = e^{(\frac{2\pi i}{N})(ad-bc)} \end{aligned}$$

.

Thus $ad - bc \equiv 1 \bmod N$ and the matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ reduces to $\begin{pmatrix} \bar{a} & \bar{b} \\ \bar{c} & \bar{d} \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ mod N. As in case *(1)*, we can take without loss of generality the lift of $\begin{pmatrix} \bar{a} & \bar{b} \\ \bar{c} & \bar{d} \end{pmatrix}$ to be $\gamma := \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ in $\mathrm{SL}_2(\mathbb{Z})$ and define $\tau' := \gamma \cdot \tau$. Then as before, $\Lambda_\tau = (c\tau + d)\Lambda_{\tau'}$. Hence $E_{\tau'}$ is isomorphic to E_τ. Moreover letting $\alpha := c\tau + d$, we get that $\gamma \begin{pmatrix} \tau \\ 1 \end{pmatrix} = \begin{pmatrix} a\tau + b \\ c\tau + d \end{pmatrix} = \begin{pmatrix} \alpha\tau' \\ \alpha \end{pmatrix}$ and $\alpha\tau' = a\tau + b$. So $P_\tau = \frac{a\tau+b}{N} + \Lambda_\tau = \alpha\frac{\tau'}{N} + \alpha\Lambda_{\tau'} = \alpha(\frac{\tau'}{N} + \Lambda_{\tau'})$ and $Q_\tau = \frac{\alpha}{N} + \Lambda_\tau = \alpha(\frac{1}{N} + \Lambda_\tau)$. As a result the modular pair $(E, (P, Q))$ is isomorphic to $(E_{\tau'}, (\frac{\tau'}{N} + \Lambda_{\tau'}, \frac{1}{N} + \Lambda_{\tau'}))$.

Now suppose for two arbitrary pairs $(E_\tau, (\frac{\tau}{N} + \Lambda_\tau, \frac{1}{N} + \Lambda_\tau))$, $(E_{\tau'}, (\frac{\tau'}{N} + \Lambda_{\tau'}, \frac{1}{N} + \Lambda_{\tau'}))$, τ and τ' are in the same $\Gamma(N)$-orbit. Then there exists $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(N)$ such that $\gamma \cdot \tau = \tau'$. So $(c\tau + d)\Lambda_{\tau'} = \Lambda_\tau$ and $E_\tau \cong E_{\tau'}$. Also $(c\tau + d)(\frac{1}{N} + \Lambda_{\tau'}) = \frac{c\tau+d}{N} + \Lambda_\tau = \frac{1}{N} + \Lambda_\tau$, since $c \equiv 0$, $d \equiv 1 \bmod N$ and $(c\tau + d)(\frac{\tau'}{N} + \Lambda_{\tau'}) = \frac{a\tau+b}{N} + \Lambda_\tau = \frac{\tau}{N} + \Lambda_\tau$, since $a \equiv 1$, $b \equiv 0 \bmod N$.

Conversely, suppose $(E_\tau, (\frac{\tau}{N} + \Lambda_\tau, \frac{1}{N} + \Lambda_\tau))$, $(E_{\tau'}, (\frac{\tau'}{N} + \Lambda_{\tau'}, \frac{1}{N} + \Lambda_{\tau'}))$ are isomorphic. Then there exists $\alpha \in \mathbb{C}^*$ such that $\alpha\Lambda_\tau = \Lambda_{\tau'}$ and $\alpha(\frac{\tau}{N} + \Lambda_\tau) = \frac{\tau'}{N} + \Lambda_{\tau'}$, $\alpha(\frac{1}{N} + \Lambda_\tau) = \frac{1}{N} + \Lambda_{\tau'}$. We have a change of basis matrix $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ such that $\gamma \begin{pmatrix} \tau' \\ 1 \end{pmatrix} = \begin{pmatrix} a\tau' + b \\ c\tau' + d \end{pmatrix} = \begin{pmatrix} \alpha\tau \\ \alpha \end{pmatrix} \implies \alpha = c\tau' + d$ and $\alpha\tau = a\tau' + b$. Replacing into the previous equations gives $\frac{\alpha\tau}{N} + \Lambda_{\tau'} = \frac{a\tau'+b}{N} + \Lambda_{\tau'} = \frac{\tau'}{N} + \Lambda_{\tau'}$, which implies that $a \equiv 1$, $b \equiv 0 \bmod N$ and $\frac{\alpha}{N} + \Lambda_{\tau'} = \frac{c\tau'+d}{N} + \Lambda_{\tau'} = \frac{1}{N} + \Lambda_{\tau'}$ and in turn gives that $c \equiv 0$, $d \equiv 1 \bmod N$. Therefore $\gamma \in \Gamma(N)$. But $\gamma \cdot \tau' = \frac{a\tau'+b}{c\tau'+d} = \tau$ and hence τ, τ' are in the same $\Gamma(N)$-orbit. □

Chapter 3

Galois representations attached to elliptic curves over $\mathbb{Q}$

In this section we study the so called l-adic representation attached to an elliptic curve E over $\mathbb{Q}$. This representation essentially arises from the action of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ on the torsion subgroups of E. These representations are ubiquitous in modern number theory since they can give a great deal of arithmetic information of an elliptic curve. Similarly, we have l-adic representations attached to modular curves given by the action of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ on the torsion subgroups of the degree zero Picard group of modular curves. The study of the connection between these two classes of l-adic representations has been extremely fruitful. A classical example of the crucial role of these representations is the proof of Fermat's last theorem.

3.1 The l-adic representation

We start by reviewing how does the absolute Galois group $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ acts on the $\bar{\mathbb{Q}}$ points of an algebraic curve defined over $\mathbb{Q}$. Throughout this chapter we will denote by $G_{\mathbb{Q}}$ the Galois group $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. Suppose $C/\mathbb{Q}$ is a (smooth, projective) algebraic curve and $(x,y) \in C(\bar{\mathbb{Q}})$ in some affine chart. Then for $\sigma \in G_{\mathbb{Q}}$, we set $(x,y)^\sigma := (x^\sigma, y^\sigma)$. To deduce that this gives an action we need to check that $(x^\sigma, y^\sigma) \in C(\mathbb{Q})$, since the rest of the axioms of an action follow trivially. Indeed, if $C = V(f_1, ..., f_s) \subseteq \mathbb{A}^2_{\mathbb{Q}}$ in some affine chart (where $f_1, ..., f_s \in \mathbb{Q}[x,y]$), then writing $f_i = \sum_{j,k\in\mathbb{N}} a_{jk}x^j y^k$, we see that $f_i^\sigma(x,y) = (\sum_{j,k} a_{jk}x^j y^k)^\sigma = \sum_{j,k} a_{jk}^\sigma (x^j)^\sigma (y^k)^\sigma = \sum_{j,k} a_{jk}(x^\sigma)^j (y^\sigma)^k = f_i(x^\sigma, y^\sigma)$. Hence if $(x,y) \in C(\bar{\mathbb{Q}})$, then $f_i^\sigma(x,y) = 0 = f_i(x^\sigma, y^\sigma)$. But this holds for any $i \in \{1, ..., s\}$. Thus for any polynomial $f = \sum_{i=1}^s g_i f_i \in \langle f_1, ..., f_s\rangle$, $f(x^\sigma, y^\sigma) = \sum_{i=1}^s g_i(x^\sigma, y^\sigma) f_i(x^\sigma, y^\sigma) = \sum_{i=1}^s g_i^\sigma(x,y) f_i^\sigma(x,y) =$

0. So we conclude that $(x^\sigma, y^\sigma) \in C(\bar{\mathbb{Q}})$.

Since we have defined an elliptic curve $E/\mathbb{Q}$ to be a genus 1 algebraic curve over $\mathbb{Q}$ with a $\mathbb{Q}$-rational point (that we call the point at infinity), we have that $G_\mathbb{Q}$ acts on $E(\bar{\mathbb{Q}})$. Recall that we have defined the N-torsion points of $E/\mathbb{Q}$ as the subgroup $E[N] = \{P \in E(\bar{\mathbb{Q}}) : [N]P = 0_E\}$. This set is in fact the kernel of the multiplication by N map. By the separability of the map $[N]$, we have that $\#E[N] = \deg[N] = N^2$ and by the structure theorem of Abelian groups, $E[N] \cong \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$. So $E[N]$ is a $\mathbb{Z}/N\mathbb{Z}$-module. To fix such an isomorphism, one needs to fix a basis of $E[N]$. Our next task is to show that $G_\mathbb{Q}$ acts on $E[N]$. To see this, we first need to prove that the action of $G_\mathbb{Q}$ respects the group law of the elliptic curve. Recall that the group law on an elliptic curve is defined via the so called "chord-tangent" construction; suppose we choose an affine chart not including the point at infinity. If $P, Q \in E(\bar{\mathbb{Q}})$ and L is a line passing through the two points then by Bezoút's theorem, L intersects E at a third point R'. Then one defines $P + Q := R$, where R is the point of intersection of the vertical line through R' with E. So if in this affine chart L is given by $ax + by = c$ (for $a, b \in \bar{\mathbb{Q}}$), then L^σ is given by $a^\sigma(x^\sigma) + b^\sigma(y^\sigma) = c^\sigma$ which is still a line. This line passes through P^σ and Q^σ and following through the definition of the group law we see that indeed $P^\sigma + Q^\sigma = R^\sigma$. Thus the action of $G_\mathbb{Q}$ indeed respects the group law. Consequently if $P \in E[N]$ then $[N]P = 0_E$ and acting by $\sigma \in G_\mathbb{Q}$ gives $[N]P^\sigma = 0_E^\sigma = 0_E$ ($0_E = 0_E^\sigma$ since an elliptic curve has only one point at infinity, which is preserved). So $G_\mathbb{Q}$ acts on $E[N]$.

In fact we see that the action of $G_\mathbb{Q}$ on $E[N]$ is far from being faithful and factors through the Galois group $\mathrm{Gal}(\mathbb{Q}(E[N])/\mathbb{Q})$. So picking a basis P, Q of $E[N]$ we have a representation $\bar{\rho}_{E,N} : G_\mathbb{Q} \to \mathrm{Gal}(\mathbb{Q}(E[N])/\mathbb{Q}) \hookrightarrow \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ and can write down matrices explicitly as follows; let $\sigma \in \mathrm{Gal}(\mathbb{Q}(E[N])/\mathbb{Q})$, then $P^\sigma = aP + cQ$, $Q^\sigma = bP + dQ$ and $\bar{\rho}_{E,N}(\sigma) = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$.

From now on we shift from an arbitrary integer N (in order to follow the standard notation in the literature) and fix a prime l. We have seen that $G_\mathbb{Q}$ has an action on $E[N]$ for an arbitrary $N \in \mathbb{N}$ and so we can consider torsion subgroups of powers of l, $E[l^n]$. For any element $P \in E[l^n]$, we have that $[l]P \in E[l^{n-1}]$ and so we have a map $[l] : E[l^n] \to E[l^{n-1}]$. Moreover the sequence $(E[l^n], [l])$ defines an inverse limit

$$E[l] \xleftarrow{[l]} E[l^2] \xleftarrow{[l]} E[l^3] \xleftarrow{[l]} \ldots$$

and we define this inverse limit to be the **l-adic Tate module of** E, denoted by

$$\mathrm{Ta}_l(E) := \varprojlim_n E[l^n].$$

We also have another inverse system defined by the pairs $(\mathbb{Z}/l^n\mathbb{Z}, [l])$, where $[l] : \mathbb{Z}/l^n\mathbb{Z} \to \mathbb{Z}/l^{n-1}\mathbb{Z}$. Taking the inverse limit of this sequence we get the ring of **l-adic integers** $\mathbb{Z}_l := \varprojlim_n \mathbb{Z}/l^n\mathbb{Z}$. Now for any $a \in \mathbb{Z}/l^n\mathbb{Z}$, $P \in E[l^n] \cong \mathbb{Z}/l^n\mathbb{Z} \times \mathbb{Z}/l^n\mathbb{Z}$, we have that $[l](aP) = a[l]P$ and so we have a commutative diagram

$$\begin{array}{ccc} E[l^n] & \xrightarrow{[l]} & E[l^{n-1}] \\ \downarrow{\scriptstyle a} & & \downarrow{\scriptstyle a} \\ E[l^n] & \xrightarrow{[l]} & E[l^{n-1}] \end{array}$$

Therefore $\mathrm{Ta}_l(E)$ is a $\mathbb{Z}_l$-module. We also have that the action of $G_\mathbb{Q}$ commutes with the multiplication by l map; for any $\sigma \in G_\mathbb{Q}$, $P \in E[l^n]$, $([l]P)^\sigma = [l]P^\sigma$ (since the action of $G_\mathbb{Q}$ respects the group law of E). Thus we have another commutative diagram

$$\begin{array}{ccc} E[l^n] & \xrightarrow{[l]} & E[l^{n-1}] \\ \downarrow{\scriptstyle \sigma} & & \downarrow{\scriptstyle \sigma} \\ E[l^n] & \xrightarrow{[l]} & E[l^{n-1}] \end{array}$$

and $\mathrm{Ta}_l(E)$ is also a $G_\mathbb{Q}$-module. This action gives the **l-adic representation of** $G_\mathbb{Q}$ attached to an elliptic curve over $\mathbb{Q}$,

$$\rho_{l,E} : G_\mathbb{Q} \to \mathrm{GL}_2(\mathbb{Z}_l).$$

Given the l-adic representation $\rho_{l,E}$ of $G_\mathbb{Q}$ attached to $E/\mathbb{Q}$, we can compose it with the reduction mod l^n map (for some positive integer n), $\mathrm{GL}_2(\mathbb{Z}_l) \to \mathrm{GL}_2(\mathbb{Z}/l^n\mathbb{Z})$ and get the mod l^n representation

$$\bar{\rho}_{l,E} : G_\mathbb{Q} \to \mathrm{Gal}(\mathbb{Q}(E[l^n])/\mathbb{Q}) \hookrightarrow \mathrm{GL}_2(\mathbb{Z}/l^n\mathbb{Z}).$$

So the determinant of a matrix with respect to $\bar{\rho}_{l,E}$ mod l^n gives a map

$$\det : G_{\mathbb{Q}} \to \mathrm{Gal}(\mathbb{Q}(E[l^n])/\mathbb{Q}) \to (\mathbb{Z}/l^n\mathbb{Z})^*,$$

which is the composite $\mathrm{Gal}(\mathbb{Q}(E[l^n])/\mathbb{Q}) \xrightarrow{\bar{\rho}_{l,E}} \mathrm{GL}_2(\mathbb{Z}/l^n\mathbb{Z}) \xrightarrow{\det} (\mathbb{Z}/l^n\mathbb{Z})^*$. Since $\mathbb{Q}(E[l^n]) \supseteq \mu_{l^n}$ (see Lemma 2.12), we have a character

$$\bar{\chi} : G_{\mathbb{Q}} \to \mathrm{Gal}(\mathbb{Q}(E[l^n])/\mathbb{Q}) \to (\mathbb{Z}/l^n\mathbb{Z})^*,$$

called the **cyclotomic character mod** l^n given by the action of $G_{\mathbb{Q}}$ on μ_{l^n} (the group of l^n roots of unity in $\bar{\mathbb{Q}}$) that factors through $\mathrm{Gal}(\mathbb{Q}(E[l^n])/\mathbb{Q})$. Any generator ζ of μ_{l^n} is a primitive l^n-th root of unity. Hence for $\sigma \in \mathrm{Gal}(\mathbb{Q}(E[l^n])/\mathbb{Q})$, $\zeta^\sigma = \zeta^{\chi(\sigma)}$, where $\zeta^{\chi(\sigma)}$ is another primitive l^n-th root of unity (since the action of $\mathrm{Gal}(\mathbb{Q}(E[l^n])/\mathbb{Q})$ sends a primitive l^n-th root of unity to another one) and thus $\bar{\chi}(\sigma) \in (\mathbb{Z}/l^n\mathbb{Z})^*$. We then have the following lemma:

Lemma 3.1 *The cyclotomic character $\bar{\chi}$ is in fact the determinant map $det(\bar{\rho}_{l,E})$.*

Proof: Let $P, Q \in E[l^n]$ be a basis and $\sigma \in \mathrm{Gal}(\mathbb{Q}(E[l^n])/\mathbb{Q})$. Then write $P^\sigma = aP + bQ$, $Q^\sigma = cP + dQ$ $(a, b, c, d \in \mathbb{Z})$, for the action of $\mathrm{Gal}(\mathbb{Q}(E[l^n])/\mathbb{Q})$ on the basis of $E[l^n]$. This gives $\bar{\rho}_{l,E}(\sigma) = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$ and $\det(\bar{\rho}_{l,E}(\sigma)) = ad - bc$. Applying the Weil pairing to their images we have that

$$\begin{aligned} e_N(P^\sigma, Q^\sigma) &= e_N(aP + bQ, cP + dQ) \\ &= e_N(P, cP + dQ)^a e_N(Q, cP + dQ)^b \\ &= e_N(P, P)^{ac} e_N(P, Q)^{ad} e_N(Q, P)^{bc} e_N(Q, Q)^{bd} \\ &= e_N(P, Q)^{ad} e_N(P, Q)^{-bc} \\ &= e_N(P, Q)^{ad-bc}, \end{aligned}$$

i.e.

$$e_N(P^\sigma, Q^\sigma) = e_N(P, Q)^{\det(\bar{\rho}_{l,E}(\sigma))}.$$

But the Weil pairing is Galois equivariant and hence $e_N(P^\sigma, Q^\sigma) = e_N(P, Q)^\sigma = e_N(P, Q)^{\chi(\sigma)}$ which gives $\bar{\chi}(\sigma) = \det(\bar{\rho}_{l,E}(\sigma))$. □

As a consequence of this, if we replace $\mathbb{Q}$ with a field K that contains μ_l^n, then $\bar{\rho}_{l,E}$ mod l^n has image in $\mathrm{SL}_2(\mathbb{Z}/l^n\mathbb{Z})$ since the action of $\mathrm{Gal}(K(E[l^n])/K)$ on μ_l^n is trivial.

What we further notice is that the action of $G_{\mathbb{Q}}$ on μ_{l^n} in fact commutes with the multiplication by l map $\zeta \mapsto \zeta^l$, for $\zeta \in \mu_{l^n}$. Moreover, if ζ is primitive in μ_{l^n},

then ζ^l is primitive in $\mu_{l^{n-1}}$. Fixing a generator of μ_{l^n} gives an isomorphism with $\mathbb{Z}/l^n\mathbb{Z}$ and so the ring of l-adic integers $\mathbb{Z}_l$ is a $G_\mathbb{Q}$-module, giving the **cyclotomic character** $\chi : G_\mathbb{Q} \to \mathbb{Z}_l^*$, (where $\mathbb{Z}_l^* = \varprojlim_n (\mathbb{Z}/l^n\mathbb{Z})^*$). Therefore we conclude that the two maps, the cyclotomic character and the determinant map with respect to the above actions, are equal.

3.2 Galois theory of number fields

In this section we review some of the basic material regarding the Galois theory of number fields, since this theory is naturally related to the l-adic representation of $G_\mathbb{Q}$. The reason behind this is that, as we have already seen, one can get a representation of the absolute Galois group of $\mathbb{Q}$, by considering its action on the l-adic Tate module of an elliptic curve $E/\mathbb{Q}$. But the Tate module is defined as the inverse limit of the l^n torsion subgroups of E and the action of $G_\mathbb{Q}$ on each term of a sequence of the Tate module factors through the Galois number fields $\mathbb{Q}(E[l^n])/\mathbb{Q}$. So let us start by fixing a Galois number field $K/\mathbb{Q}$ with Galois group $G := \mathrm{Gal}(K/\mathbb{Q})$. Take $p \in \mathbb{Z}$ prime. Then we have that the ideal (p) in $\mathcal{O}_K$, the ring of integers of K, decomposes into a product of prime ideals of $\mathcal{O}_K$, that we say that that they **lie over** p. Moreover the image of a prime ideal $\wp \in \mathcal{O}_K$ under $\sigma \in G$, is again a prime ideal. In addition we have that σ acts transitively on prime ideals of $\mathcal{O}_K$ lying over p, i.e. for any $\wp, \wp' \in \mathcal{O}_K$ lying over p, there exists an element $\sigma \in G$ such that $\wp^\sigma = \wp'$. To see this, suppose $\wp$ and $\wp'$ are two distinct prime ideals lying over $p \in \mathbb{Z}$. Let $x \in \mathcal{O}_K$ such that $x \equiv 0 \bmod \wp$ and $x \not\equiv 0 \bmod \wp'$ (the existence of such an element is guaranteed by the Chinese remainder theorem). Then the element $y := \prod_{\sigma \in \mathrm{Gal}(K/\mathbb{Q})} x^\sigma \in \wp \cap \mathcal{O}_\mathbb{Q}$ (since the element y is fixed by the action of $\mathrm{Gal}(K/\mathbb{Q})$). But $\wp \cap \mathcal{O}_\mathbb{Q} = \wp \cap \mathbb{Z} = p \in \wp'$. Since $\wp'$ is a prime ideal, it follows that there exists an element $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ such that $x^\sigma \equiv 0 \bmod \wp'$. This in turn implies that $x \equiv 0 \bmod \wp'^{\sigma^{-1}}$ and since we have chosen $x \equiv 0 \bmod \wp$, $\wp'^{\sigma^{-1}} = \wp$ or $\wp^\sigma = \wp'$. As a result, it follows that if

$$p\mathcal{O}_K = \wp_1^{e_1} ... \wp_g^{e_g}$$

then $e_i = e_j =: e$ for any $i, j \in \{1, ..., g\}$. We call this number e the **ramification index of** p. What we notice here is that since $\mathcal{O}_K$ is a Dedekind domain, $\mathcal{O}_K/\wp_i$ is a finite field for any prime ideal $\wp_i$ lying over p. Therefore $\mathcal{O}_K/\wp_i$ is isomorphic to $\mathbb{F}_{p^f}$, for some $f \in \mathbb{N}$ that we call the **degree of inertia**. One can also view $\mathcal{O}_K/\wp_i$ as a vector space over $\mathbb{Z}/p\mathbb{Z}$. Then this vector space has dimension equal to f. We call the quotient $\mathcal{O}_K/\wp_i$ the **residue field**.

Let us denote by n the degree of the extension $K/\mathbb{Q}$. Then one has that $n = efg$. We say that a prime p

- **splits** in $\mathcal{O}_K$ if $g > 1$
- **ramifies** in $\mathcal{O}_K$ if $e > 1$
- **remains inert** in $\mathcal{O}_K$ if $g = e = 1$

Another result that we have from algebraic number theory is that a prime p ramifies in $\mathcal{O}_K$ if and only if p divides the discriminant of $K/\mathbb{Q}$ (this is in [Neukirch], Chapter 3, Corollary 2.12). Hence it follows that only finitely many primes ramify in $\mathcal{O}_K$. To be able to make use of the full force of the following machinery we have developed we also need the following two constructions. Suppose we have the same setting as before, i.e. $p\mathcal{O}_K = \wp_1^{e_1}...\wp_g^{e_g}$ and let us fix a prime ideal $\wp$ lying over p. Then we define the following:

Definition 3.2 *The **decomposition group** of the prime ideal $\wp$ is defined to be the subgroup of the Galois group $Gal(K/\mathbb{Q})$, which fixes the prime ideal $\wp$ as a set. Explicitly,*

$$D_\wp := \{\sigma \in Gal(K/\mathbb{Q}) : \wp^\sigma = \wp\}.$$

In fact, this group has order equal to ef. This is because the Orbit-Stabilizer theorem gives that the order of $\mathrm{Gal}(K/\mathbb{Q})$ equals to the product of the size of the orbit of the action of this group on $\wp$ with the size of its stabilizer. The latter of the two is the order of $D_\wp$ and since the action is transitive, $|\mathrm{Gal}(K/\mathbb{Q})| = n = |D_\wp|g$. But we also have that $n = efg$ and so $|D_\wp| = ef$. Now notice that if we take $\sigma \in D_\wp$ and $x + \wp \in \mathcal{O}_K/\wp$, then $(x+\wp)^\sigma = x^\sigma + \wp$. Thus $D_\wp$ is acting on the residue field $\mathcal{O}_K/\wp$. The kernel of this action is defined to be the set of elements $\sigma \in D_\wp$ such that for any $x + \wp \in \mathcal{O}_K/\wp$, $(x+\wp)^\sigma = x + \wp$. This gives a normal subgroup of $D_\wp$, that we call the inertia group.

Definition 3.3 *The **inertia group** of the prime ideal $\wp$, is the subgroup of $D_\wp$ defined by*

$$I_\wp := \{\sigma \in D_\wp : (x+\wp)^\sigma = x + \wp, \ \textit{for all } x + \wp \in \mathcal{O}_K/\wp\}$$

Shifting our attention now back to the residue field $\mathcal{O}_K/\wp \cong \mathbb{F}_{p^f}$, we have that $\mathrm{Gal}((\mathcal{O}_K/\wp)/\mathbb{F}_p)$ is cyclic and generated by the Frobenius automorphism $\sigma_p : x \mapsto x^p$. The punchline of this machinery lies in the isomorphism $D_\wp/I_\wp \cong \mathrm{Gal}((\mathcal{O}_K/\wp)/\mathbb{F}_p) = \langle\sigma_p\rangle$ and the theorem of Čebotarev that we will soon state

explicitly. We also remark that since $|\mathrm{Gal}((\mathcal{O}_K/\wp)/\mathbb{F}_p)| = f$ and $|D_\wp/I_\wp| = ef/|I_\wp|$, the order of the inertia group of $\wp$ equals to e.

Definition 3.4 *Any lift of σ_p to a generator of $D_\wp/I_\wp$ is called a* ***Frobenius element at*** *$\wp$ and denoted by* $\mathrm{Frob}_\wp$.

Since $\mathrm{Frob}_\wp \in \mathrm{Gal}(K/\mathbb{Q})$ is the lift in the quotient $D_\wp/I_\wp$, then it is unique up to inertia, i.e. it is a coset in $D_\wp/I_\wp$. However, in the case when p is unramified, $|I_\wp| = e = 1$, $I_\wp$ is trivial and $\mathrm{Frob}_\wp$ is no longer a coset and does not depend on inertia.

Theorem 3.5 ***Čebotarev's density theorem (weak form):*** *Let $K/\mathbb{Q}$ be a Galois number field. Then every element of $Gal(K/\mathbb{Q})$ takes the form* $\mathrm{Frob}_\wp$ *for infinitely many prime ideals $\wp$ of $\mathcal{O}_K$.*

Proof: This is a consequence of [Neukirch], §3, Theorem 13.4. □

Thus any element of $\mathrm{Gal}(K/\mathbb{Q})$ is equal to $\mathrm{Frob}_\wp$ for some prime ideal $\wp$ of $\mathcal{O}_K$, up to conjugacy. Now if $\wp_i$, $\wp_j$ are two prime ideals lying over p, the following lemma gives a way of relating the decomposition and inertia groups as well as the Frobenius elements at the two prime ideals:

Proposition 3.6 *For any $\sigma \in Gal(K/\mathbb{Q})$ we have the following relations:*

$$\sigma^{-1} D_\wp \sigma = D_{\wp^\sigma}$$

$$\sigma^{-1} I_\wp \sigma = I_{\wp^\sigma}$$

$$\sigma^{-1} \mathrm{Frob}_\wp \sigma = \mathrm{Frob}_{\wp^\sigma}$$

Proof: $\tau \in D_{\wp^\sigma} \iff (\wp^\sigma)^\tau = \wp^\sigma \iff \wp^{\sigma\tau\sigma^{-1}} = \wp \iff \sigma\tau\sigma^{-1} \in D_\wp$. So $D_{\wp^\sigma} = \sigma^{-1} D_\wp \sigma$ and similarly $I_{\wp^\sigma} = \sigma^{-1} I_\wp \sigma$. As a result, it follows that if $\mathrm{Frob}_{\wp^\sigma}$ is a lift of $\sigma_p \in \mathrm{Gal}((\mathcal{O}_K/\wp)/\mathbb{F}_p)$ in $D_{\wp^\sigma}/I_{\wp^\sigma} = \sigma^{-1}(D_\wp/I_\wp)\sigma$ then $\sigma \mathrm{Frob}_{\wp^\sigma} \sigma^{-1}$ is a lift of σ_p in $D_\wp/I_\wp$, i.e. $\sigma \mathrm{Frob}_{\wp^\sigma} \sigma^{-1} = \mathrm{Frob}_\wp$. □

This gives us a well-defined notion of ramification of the extension $K/\mathbb{Q}$ at a prime $p \in \mathbb{Z}$ in the following sense; for a prime ideal $\wp$ lying over p, since $\sigma^{-1} I_\wp \sigma = I_{\wp^\sigma}$ we have that $|I_\wp| = |I_{\wp^\sigma}|$. Thus $I_\wp$ is trivial if and only if $I_{\wp^\sigma}$ is trivial. But $\mathrm{Gal}(K/\mathbb{Q})$ acts transitively on the prime ideals lying over p and hence we say that the extension $K/\mathbb{Q}$ is **unramified at** p when $I_\wp$ is trivial for any prime ideal $\wp$ lying over p.

3.3 Galois theory of $\bar{\mathbb{Q}}/\mathbb{Q}$

In the previous section we have developed the machinery that gives a nice link between the Galois group of a number field and the arithmetic of this field. In this section we study how this machinery can carry over to the case of the field extension $\bar{\mathbb{Q}}/\mathbb{Q}$ which is of course not a finite extension. As a result, it does not belong to the case of number fields and the classical Galois theory of number fields here breaks down. There is a nice way to extend this theory of Galois number fields to the infinite case, which is based on choosing an appropriate topology for the infinite Galois group $G_{\mathbb{Q}}$. In particular, the topology chosen here is the so called **Krull topology**. What is fundamental to the construction of this topology is to observe that fixing a Galois number field K the homomorphism $G_{\mathbb{Q}} \to \mathrm{Gal}(K/\mathbb{Q})$ given by restricting the action to the field K, has kernel the normal subgroup $M(K) := \{\sigma \in G_{\mathbb{Q}} : \sigma \mid_K = 1\}$. Then the corresponding cosets of the quotient $G_{\mathbb{Q}}/M(K)$ are sets of the form $U_\sigma(K) = \{\sigma\tau : \tau \in M(K)\}$, where $\sigma \in G_{\mathbb{Q}}$. We choose as a basis for the Krull topology on $G_{\mathbb{Q}}$ the sets of the form $U_\sigma(K)$, for $\sigma \in G_{\mathbb{Q}}$ and K a Galois number field.

The next step in our construction is a categorical description of $G_{\mathbb{Q}}$. In particular, for any Galois number fields K, K' ordered by inclusion, i.e. $K \subset K'$, one associates their corresponding Galois groups. Then there is a surjective homomorphism $\phi_{K',K} : \mathrm{Gal}(K'/\mathbb{Q}) \to \mathrm{Gal}(K/\mathbb{Q})$. Moreover if $K \subset L \subset M$, then the homomorphism $\phi_{M,K}$ factors through $\phi_{M,L} \circ \phi_{L,K}$. Hence this setup actually defines an inverse system and taking the inverse limit over all Galois number fields we have that $G_{\mathbb{Q}}$ is a pro-finite group

$$G_{\mathbb{Q}} = \varprojlim_{K} \mathrm{Gal}(K/\mathbb{Q}).$$

$G_{\mathbb{Q}}$ equipped with the Krull topology satisfies the following Galois correspondence: The map

$$N \mapsto \mathrm{Gal}(\bar{\mathbb{Q}}/N)$$

gives a 1 to 1 inclusion reversing correspondence between subextensions $N/\mathbb{Q}$ and closed subgroups of $G_{\mathbb{Q}}$. Conversely, the map

$$H \mapsto \bar{\mathbb{Q}}^H$$

gives an inverse correspondence to the previous map, where H is a closed subgroup of $G_{\mathbb{Q}}$ and $\bar{\mathbb{Q}}^H$ denotes its fixed field.

Now the main definitions of the previous section carry over to the case of $G_{\mathbb{Q}}$. The "ring of integers" of $\bar{\mathbb{Q}}$ is now the ring of algebraic integers over $\mathbb{Q}$ which we denote by $\bar{\mathbb{Z}}$. Since $\bar{\mathbb{Z}}$ is not a Dedekind domain, we cannot expect to have the factorisation of a prime $p \in \mathbb{Z}$ into finitely many prime ideals of $\bar{\mathbb{Z}}$. However we can always pick a prime ideal $\wp \subset \bar{\mathbb{Z}}$ lying over p, which is equivalent to a compatible system of primes lying over p in all number fields. As in the case of Galois number fields, we define the decomposition group of $\wp$ as the subgroup of $G_{\mathbb{Q}}$ that fixes $\wp$ as a set, $D_{\wp} := \{\sigma \in G_{\mathbb{Q}} : \wp^{\sigma} = \wp\}$. Thus $D_{\wp}$ has an action on $\bar{\mathbb{Z}}/\wp \cong \bar{\mathbb{F}}_p$ defined by $(x+\wp)^{\sigma} = x^{\sigma} + \wp$, for $\sigma \in D_{\wp}$ and $x + \wp \in \bar{\mathbb{Z}}/\wp$. The inertia group of $\wp$ is similarly defined to be the kernel of this action, $I_{\wp} := \{\sigma \in D_{\wp} : (x+\wp)^{\sigma} = x + \wp, \text{ for all } x + \wp \in \bar{\mathbb{F}}_p\}$. So $D_{\wp}/I_{\wp} \cong \mathrm{Gal}((\bar{\mathbb{Z}}/\wp)/\mathbb{F}_p) = \mathrm{Gal}(\bar{\mathbb{F}}_p/\mathbb{F}_p)$. $\mathrm{Gal}(\bar{\mathbb{F}}_p/\mathbb{F}_p)$ contains Frobenius automorphisms of the form $\sigma_p : x \mapsto x^p$ and any lift of σ_p to an element of $D_{\wp}/I_{\wp}$ is called the **absolute Frobenius element at** $\wp$ (or simply the Frobenius element at $\wp$ for simplicity) which again depends as a coset on $I_{\wp}$. Similarly as in the case of Galois number fields, we have the following relations: For any $\sigma \in G_{\mathbb{Q}}$,

$$\sigma^{-1} D_{\wp} \sigma = D_{\wp^{\sigma}}$$

$$\sigma^{-1} I_{\wp} \sigma = I_{\wp^{\sigma}}$$

$$\sigma^{-1} \mathrm{Frob}_{\wp} \sigma = \mathrm{Frob}_{\wp^{\sigma}}.$$

This analogue from Galois number fields carries over to the case of $G_{\mathbb{Q}}$ because $G_{\mathbb{Q}}$ acts transitively on the prime ideals lying over p in $\bar{\mathbb{Z}}$. Čebotarev's density theorem generalizes to the case of $G_{\mathbb{Q}}$ as well with respect to the Krull topology:

Theorem 3.7 ***Čebotarev's density theorem:*** *For each prime $p \in \mathbb{Z}$ choose a prime ideal $\wp \subset \bar{\mathbb{Z}}$ lying over p and an absolute Frobenius element at $\wp$, $Frob_{\wp}$. Then the set $\{Frob_{\wp}\}_{p,\ prime}$ is a dense subset of $G_{\mathbb{Q}}$.*

Proof: See [Neukirch], §3, Theorem 13.4. □

Moving our attention back to the l-adic representation $\rho_{l,E}$ attached to an elliptic curve $E/\mathbb{Q}$, given any prime $p \neq l$, we say that $\rho_{l,E}$ **is unramified at** p when the inertia subgroup $I_{\wp}$ of any prime ideal $\wp$ lying over p acts trivially on $\mathrm{Ta}_l(E)$. Notice that the definition is well defined because of the property $I_{\wp^{\sigma}} = \sigma^{-1} I_{\wp} \sigma$ for $\sigma \in G_{\mathbb{Q}}$ and since $G_{\mathbb{Q}}$ acts transitively on the prime ideals over p, any prime ideal over p is conjugate to $\wp$.

3.4 A taste of modularity

In this section we show how does a number being attached to an elliptic curve $E/\mathbb{Q}$ called its conductor can serve as the tipping point of another bridge between the two worlds of elliptic curves and modular curves (other than the one of modular curves as moduli spaces of elliptic curves). So far, we have seen how does $G_{\mathbb{Q}}$ acts on the Tate module $\mathrm{Ta}_l(E)$ of an elliptic curve $E/\mathbb{Q}$. We have also seen that $\mathrm{Ta}_l(E)$ is a $\mathbb{Z}_l$-module. In fact one can do even better and turn $\mathrm{Ta}_l(E)$ into a 2-dimensional vector space over $\mathbb{Q}_l$ (the field of fractions of $\mathbb{Z}_l$) by taking the tensor product $V_l := \mathrm{Ta}_l(E) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$, which is still a $G_{\mathbb{Q}}$-module. hence we get an extended representation

$$\rho_{l,E} : G_{\mathbb{Q}} \to \mathrm{Aut}(V_l) \cong \mathrm{GL}_2(\mathbb{Q}_l).$$

At a prime $p \neq l$, we can take an ideal $\wp \subset \bar{\mathbb{Z}}$ lying over p and consider the action of $I_\wp$ on V_l. Write $V_l^{I_\wp}$ for the vector subspace fixed by the action of $I_\wp$ and define

$$\mathrm{tame}_p := 2 - \dim(V_l^{I_\wp}).$$

The next part we want to define is slightly more technical; let $\wp'$ be an ideal of $\mathbb{Q}(E[l])$ lying over p and consider the higher ramification groups of $\mathrm{Gal}(\mathbb{Q}(E[l])/\mathbb{Q})$ given by

$$G_i := \{\sigma \in \mathrm{Gal}(\mathbb{Q}(E[l])/\mathbb{Q}) : x^\sigma \equiv x \mod(\wp')^{i+1} \text{ for all } x \in \mathcal{O}_{\mathbb{Q}(E[l])}\}.$$

Then define

$$\mathrm{wild}_p := \sum_{i=1}^{\infty} \frac{\dim(E[l]/E[l]^{G_i})}{[G_0 : G_i]},$$

where $E[l]^{G_i}$ is the submodule fixed by the action of G_i on $E[l]$ and G_0 actually equals to $I_{\wp'}$. Notice here that the above sum is in fact a finite sum since for large enough i, G_i is trivial and $\dim(E[l]/E[l]^{G_i})$ is eventually 0. Finally, set

$$e_p := \mathrm{tame}_p + \mathrm{wild}_p.$$

If at a prime p, $E/\mathbb{Q}$ has good reduction then the Néron-Ogg-Shafarevich criterion (see for example [Silverman 1], §7, Theorem 7.1) gives that $\rho_{l,E}$ is unramified at p and so the action of $I_\wp$ is trivial. Hence $\mathrm{tame}_p = \mathrm{wild}_p = 0$. The conductor of the elliptic curve $E/\mathbb{Q}$ is defined as the product

$$N_E := \prod_p p^{e_p}.$$

One notices that since $E/\mathbb{Q}$ has bad reduction at a finite set of primes, by the above discussion, finitely many terms that are not equal to 1 appear in the above product and thus N_E is a finite product.

In the celebrated paper [B C D T], the authors prove that any elliptic curve $E/\mathbb{Q}$ is modular, the so called **Modularity theorem**. This is one of the most remarkable results in the mathematics of the 20-th century. A special case of it for the class of semistable elliptic curves was originally proved by Andrew Wiles and opened the way for the proof of Fermat's last theorem. One interpretation of the Modularity theorem is the following ([Dia & Shur], Theorem 7.7.2):

Theorem 3.8 *Let $E/\mathbb{Q}$ be an elliptic curve, with conductor N_E. Then there exists a surjective morphism over $\mathbb{Q}$ between the algebraic curves $X_0(N_E)/\mathbb{Q}$ to $E/\mathbb{Q}$.*

Now that we have the notion of the conductor of an elliptic curve in hand, we state another important theorem that gives a more hands-on description of how the absolute Frobenius elements of $G_{\mathbb{Q}}$ act on $\mathrm{Ta}_l(E)$.

Theorem 3.9 *Let l be a rational prime and $E/\mathbb{Q}$ an elliptic curve with conductor N_E. Then the Galois representation $\rho_{l,E}$ is unramified at every prime $p \nmid lN_E$. For any such p let $\wp \subset \bar{\mathbb{Z}}$ be a prime ideal lying over p. Then*

$$det\, \rho_{l,E}(Frob_{\wp}) = p$$

$$tr\, \rho_{l,E}(Frob_{\wp}) = a_p(E)$$

where $a_p(E) = p + 1 - \#\bar{E}(\mathbb{F}_p)$ as defined in section 2.2.2 and tr denotes the trace. Thus the characteristic equation of $\rho_{l,E}(Frob_{\wp})$ is $x^2 - a_p(E)x + p$.

Proof: This is [Dia & Shur], Theorem 9.4.1. □

What there is to observe here is that $\det \rho_{l,E}(\mathrm{Frob}_{\wp})$ and $\mathrm{tr}\ \rho_{l,E}(\mathrm{Frob}_{\wp})$ in fact do not depend on the choice of a prime ideal $\wp \subset \bar{\mathbb{Z}}$ lying over p. The reason behind this is essentially the fact that $\rho_{l,E}$ is unramified at every prime $p \nmid lN_E$ and so the action of the inertia subgroup for any prime ideal lying over p is trivial. Also, by the properties of the trace and $\sigma^{-1}\mathrm{Frob}_{\wp}\sigma = \mathrm{Frob}_{\wp^{\sigma}}$ we have that $\mathrm{tr}\ \rho_{l,E}(\mathrm{Frob}_{\wp^{\sigma}}) = \mathrm{tr}\ \rho_{l,E}(\sigma^{-1}\mathrm{Frob}_{\wp}\sigma) = \mathrm{tr}\ \rho_{l,E}(\mathrm{Frob}_{\wp})$. As a result, in this situation we omit the choice of a prime ideal $\wp$ lying over p and write $\det \rho_{l,E}(\mathrm{Frob}_p)$ and $\mathrm{tr}\ \rho_{l,E}(\mathrm{Frob}_p)$ instead.

Another incarnation of the Modularity theorem states that given an elliptic curve $E/\mathbb{Q}$ of conductor N_E, there exists a normalised new eigenform $f = \sum_{n=1}^{\infty} a_n q^n$ of weight 2 and level $\Gamma_0(N_E)$ such that $\mathrm{tr}\ \rho_{l,E}(\mathrm{Frob}_p) = a_p$ (this is

in [Dia & Shur], Theorem 8.8.1). As an example, let's consider the elliptic curve $E/\mathbb{Q} : y^2 + y = x^3 - x^2 - 10x - 20$. This is a curve of conductor 11 obtained from Cremona's tables of elliptic curves with conductor up to 10000. The computations in this example were done in SAGE and an attachment of the code can be found in Appendix - section 6.1, code 1 and 2. Considering the 3-adic representation attached to E, $\rho_{3,E}$, we compute the trace of the Frobenius at primes $p \nmid 33$ up to 50. We also consider the space of the cusp forms of weight 2 and level $\Gamma_0(11)$. It turns out that this space is 1-dimensional and has a basis vector the cusp form $f = \sum_{n=1}^{\infty} a_n q^n$ whose q-expansion up to the q^{50} term can be found in Appendix - section 6.1, code 1. The results are summarised in the following table:

Prime p	tr $\rho_{3,E}(\text{Frob}_p)$	a_p
2	7	7
5	1	1
7	7	7
13	4	4
17	7	7
19	0	0
23	8	8
29	0	0
31	7	7
37	3	3
41	1	1
43	3	3
47	8	8

Chapter 4

Surjectivity of Galois representations of elliptic curves over $\mathbb{Q}$

Recall, from the previous section, that given an elliptic curve E over $\mathbb{Q}$, we can always associate a representation of the Galois group $G_{\mathbb{Q}}$, using the action of $G_{\mathbb{Q}}$ on the l-adic Tate module of E. A natural question would be whether this representation, $\rho_{l,E} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}_l)$, is surjective. To make the question more precise, one could ask for which elliptic curve E over a field K and for which integer $l \in \mathbb{Z}$ the representation $\rho_{l,E}$ is surjective. This question is in general hard to answer (see for example [Greicius] for the general case). However, the case where E is defined over $\mathbb{Q}$ is very well understood and the aim of this section is to provide a satisfactory answer.

In [Serre 2], Serre observes a property $\mathrm{SL}_2(\mathbb{Z}_l)$ has, which will be the main tool used in answering this question. Explicitly, Serre states it as a lemma:

Lemma 4.1 *Let X be a closed subgroup of $SL_2(\mathbb{Z}_l)$ whose image under the reduction mod l map in $SL_2(\mathbb{Z}/l\mathbb{Z})$ is surjective. Assume $l \geq 5$. Then $X = SL_2(\mathbb{Z}_l)$.*

Proof: [Serre 2], IV, 3.4, Lemma 3. □

As we have seen in Lemma 3.1, for an elliptic curve $E/\mathbb{Q}$ and $\sigma \in \mathrm{Gal}(\mathbb{Q}(E[l^n])/\mathbb{Q})$, $\det(\bar{\rho}_{l,E}(\sigma)) = \chi(\sigma)$, where $\chi : \mathrm{Gal}(\mathbb{Q}(E[l^n])/\mathbb{Q}) \to (\mathbb{Z}/l^n\mathbb{Z})^*$ is the cyclotomic character. However, we have also seen that $\mathbb{Q}(E[l^n]) \supseteq \mu_{l^n}$ (see Lemma 2.12) and $\mathbb{Q}$ does not contain any elements of μ_{l^n} apart from 1 or ± 1 if l is odd or even respectively. Hence χ is surjective mod l^n and the determinant map is surjective. If

the image of $\bar{\rho}_{l,E}$ mod l^n contains $\mathrm{SL}_2(\mathbb{Z}/l^n\mathbb{Z})$ and an element of every determinant mod l^n, then it must contain all the elements of $\mathrm{GL}_2(\mathbb{Z}/l^n\mathbb{Z})$. Therefore we conclude that if $\bar{\rho}_{l,E} : \mathrm{Gal}(\mathbb{Q}(E[l^n])/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}/l^n\mathbb{Z})$ mod l^n is surjective on $\mathrm{SL}_2(\mathbb{Z}/l^n\mathbb{Z})$, then it is surjective on $\mathrm{GL}_2(\mathbb{Z}/l^n\mathbb{Z})$.

Now if $\rho_{l,E} : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}_l)$ is surjective mod l then $\bar{\rho}_{l,E}$ is surjective on $\mathrm{SL}_2(\mathbb{Z}/l\mathbb{Z})$. Above lemma implies that for $l \geq 5$, $\rho_{l,E}$ is surjective on $\mathrm{SL}_2(\mathbb{Z}_l)$ and by previous observation, $\rho_{l,E}$ is surjective on $\mathrm{GL}_2(\mathbb{Z}_l)$. However, for $l < 5$, the above phenomenon no longer occurs. In [Serre 2],IV, 3.4, Exercise 3, Serre gives a recipe on how to construct a lift G of $\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$ in $\mathrm{SL}_2(\mathbb{Z}/9\mathbb{Z})$, such that G is a proper subgroup of $\mathrm{SL}_2(\mathbb{Z}/9\mathbb{Z})$. This suggests the existence of elliptic curves with image of $\bar{\rho}_{3,E}(\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}))$ mod 9 in $\mathrm{SL}_2(\mathbb{Z}/9\mathbb{Z})$ equal to G. These elliptic curves will be then surjective mod 3 and not mod 9 making $\rho_{3,E}$ not surjective. Elkies (in [Elkies]) uses the theory of modular curves and their property that they serve as moduli spaces to classify all elliptic curves with the above property. In this section we give an overview of Elkies approach and fill in some details omitted in [Elkies].

4.1 The group G

The group $\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$, which has order 24, is generated by the elements $S := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ and $T := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ (notice that here, in order to keep up with Elkies notation, S is the transpose of the matrix we called S in section 2.1.3). The relations that they satisfy are the following: $S^2 = -1, (ST)^3 = T^3 = 1$ (notice the misprint in [Elkies]). A computation using the computer package GAP (see Appendix - section 6.1, code 3), shows that $\mathrm{SL}_2(\mathbb{Z}/9\mathbb{Z})$ has 3 conjugacy classes of maximal subgroups, of which only 1 of them has order 24. In fact, this subgroup indeed reduces to $\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$ mod 3. This is the group G we are searching for.

As Elkies notes, to lift $\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$ to a subgroup G of $\mathrm{SL}_2(\mathbb{Z}/9\mathbb{Z})$ it is enough to lift S, T to matrices $\tilde{S}, \tilde{T}$ modulo 9 satisfying the relations $S^2 = -1, (ST)^3 = T^3 = 1$. Moreover, Elkies claims that there are 27 such lifts all conjugate in the automorphism group of the modular curve $X(9)$. We choose $\tilde{S} = \begin{pmatrix} 0 & 4 \\ 2 & 0 \end{pmatrix}$ and $\tilde{T} = \begin{pmatrix} 4 & 1 \\ -3 & 4 \end{pmatrix}$ (notice here that $\tilde{S}$ is the transpose of Elkies $\tilde{S}$, since the latter does not satisfy the desired relations). In turn we set $G = \langle \tilde{S}, \tilde{T} \rangle$.

4.2 The modular curve $X(9)/G$

As we saw in section 2.3, modular curves can serve as a moduli space for isomorphism classes of elliptic curves with some extra properties. We start with the modular curve $X(9)$ which parametrizes modular pairs $(E,(P,Q))$ where P,Q are generators of $E[9]$ satisfying $e_9(P,Q)=e^{\frac{2\pi i}{9}}$. The cusps of $\Gamma(9)$ correspond to generalized elliptic curves with level 9 structure. Roughly speaking, these are pairs of generators of the group $(\mathbb{Z}/9\mathbb{Z})\times\mu_9$. Picking a generator of μ_9 gives an isomorphism $(\mathbb{Z}/9\mathbb{Z})\times\mu_9\cong(\mathbb{Z}/9\mathbb{Z})^2$ and hence we have an obvious action of $\mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z})$. For the purpose of this essay, these generalized elliptic curves serve no purpose and thus we say no more about them. However, the cusps of $\Gamma(9)$ do have a significant role and we will study them in detail in succeeding sections. Notice that fixing a basis $P,Q\in E[9]$ gives an isomorphism $E[9]\cong\mathbb{Z}/9\mathbb{Z}\times\mathbb{Z}/9\mathbb{Z}$. Now it is clear that $\mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z})$ has a natural action on $E[9]$. We also have an action of $\mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z})$ on the group of 9-th roots of unity, μ_9, via the determinant map; for $g\in\mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z})$, $\zeta\in\mu_9$, $g\cdot\zeta:=\zeta^{\det(g)}$. As a result, restricting this action to the subgroup $\mathrm{SL}_2(\mathbb{Z}/9\mathbb{Z})$, the action is trivial and therefore $\mathrm{SL}_2(\mathbb{Z}/9\mathbb{Z})$ respects the Weil pairing. In particular, we get an action of $\mathrm{SL}_2(\mathbb{Z}/9\mathbb{Z})$ on $Y(9)(\mathbb{C})$. Since $G\subset\mathrm{SL}_2(\mathbb{Z}/9\mathbb{Z})$, G also acts on $Y(9)(\mathbb{C})$. In particular, we view a G-orbit as the pair $(E/\mathbb{C},\{$ equivalence class of (P,Q) mod $G\})$. G also has an action on the cusps of $X(9)(\mathbb{C})$ (see section 4.4).

The next step is that we want to make sense of a G-orbit to be "defined over a field extension $K/\mathbb{Q}$", where K contains μ_9. We say that a G-orbit $(E,\,[P,Q]$ mod $G)$ is defined over K if

1. the elliptic curve E is defined over K
2. for any $\sigma\in\mathrm{Gal}(K(E[9])/K)$, $(P,Q)^\sigma\in[P,Q]$ mod G.

Hence $(E,\,[P,Q]$ mod $G)$ is defined over K if and only if E is defined over K and for any $\sigma\in\mathrm{Gal}(K(E[9])/K)$ there exists an element $g\in G$ such that $P^\sigma=g\cdot P$ and $Q^\sigma=g\cdot Q$. But then this implies that $\bar{\rho}_{3,E}(\sigma)\mod 9\in G$. Therefore, we conclude that an orbit $(E,\,[P,Q]$ mod $G)$ is defined over K if and only if E is defined over K and the image of $\mathrm{Gal}(\bar{K}/K(\zeta_9))$ on 9-torsion in basis given by P,Q is contained in G.

As we saw in section 3.1, Lemma 3.1, if an elliptic curve E is defined over a field K which contains μ_l, then $\bar{\rho}_{l,E}$ mod l has image contained in $\mathrm{SL}(\mathbb{Z}/l\mathbb{Z})$. Since we are interested in elliptic curves over $\mathbb{Q}$, $\rho_{l,E}(\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}))\subseteq\mathrm{SL}(\mathbb{Z}_l)$ can no longer be guaranteed. So instead of using the group G we consider a subgroup $G'\subseteq\mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z})$ satisfying $G'\cap\mathrm{SL}_2(\mathbb{Z}/9\mathbb{Z})=G$ and elliptic curves over $\mathbb{Q}$ with

$\bar{\rho}_{3,E} \subseteq G'$ mod 9. Recall that the action of $\mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z})$ on the 9-th roots of unity is via the determinant map. Since $\det(\mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z})) \subseteq (\mathbb{Z}/9\mathbb{Z})^*$, $\mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z})$ also acts on the primitive 9-th roots of unity. But the action of $\mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z})$ on 9-torsion no longer preserves the Weil pairing and as a result we are forced to consider the disconnected modular curve $\tilde{X}(9)(\mathbb{C}) = \{(E, P, Q, \zeta) : e_9(P, Q) = \zeta, \zeta \in \mu_9^*\} \cup \{(c, \zeta) : c \in C(X(9)), \zeta \in \mu_9^*\}$ (where μ_9^* denotes the primitive 9-th roots of unity). In fact, $\tilde{X}(9)(\mathbb{C})$ is equal to 6 copies of $X(9)(\mathbb{C})$, the number of primitive 9-th roots of unity. Then we have an action of $\mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z})$ on $\tilde{X}(9)(\mathbb{C})$ defined as follows; for $g \in \mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z})$, $g \cdot (E, P, Q, \zeta) = (g \cdot (E, P, Q), \zeta^{\det g})$ (the action $g \cdot (E, P, Q)$ is the same as in the case of $\mathrm{SL}_2(\mathbb{Z}/9\mathbb{Z})$ acting on $Y(9)$). It is worth noting here that $\mathrm{SL}_2(\mathbb{Z}/9\mathbb{Z})$ stabilizes the components of $\tilde{X}(9)(\mathbb{C})$ and hence when we restrict its action to each component, the orbits remain the same as in the case of the action of $\mathrm{SL}_2(\mathbb{Z}/9\mathbb{Z})$ on $Y(9)$.

4.3 The group G'

As pointed out in previous section, our next task now is to find a group $G' \subseteq \mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z})$ satisfying $G = G' \cap \mathrm{SL}_2(\mathbb{Z}/9\mathbb{Z})$. Let s denote the index of the subgroup $\det(G')$ in the group $(\mathbb{Z}/9\mathbb{Z})^*$, which is the number of orbits of the action of G' on the primitive 9-th roots of unity. Then we see that $\tilde{X}(9)(\mathbb{C})/G' = s$ copies of $X(9)/G$. In particular, if we insist that our choice of the group G' makes the determinant map $G'/G \to (\mathbb{Z}/9\mathbb{Z})^*$ an isomorphism, then $s = 1$ and $\tilde{X}(9)/G' = X(9)/G$. What would also follow is that G is normal in G', since $\mathrm{SL}_2(\mathbb{Z}/9\mathbb{Z}) \lhd \mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z})$ (being the kernel of the determinant map) and $G \subseteq \mathrm{SL}_2(\mathbb{Z}/9\mathbb{Z})$, $G' \subseteq \mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z})$.

In our case we can find a group G' that makes the determinant map $G'/G \to (\mathbb{Z}/9\mathbb{Z})^*$ an isomorphism and for which we have $s = 1$. The way we construct this group G' is using the determinant map $G'/G \to (\mathbb{Z}/9\mathbb{Z})^*$ to lift elements in $\mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z})$ that normalize G. As suggested by Elkies, for the squares of $(\mathbb{Z}/9\mathbb{Z})^* = \{-4, -2, -1, 1, 2, 4\}$ we use invertible multiples of the identity. The squares of $(\mathbb{Z}/9\mathbb{Z})^*$ are the elements $\{-2, 1, 4\}$ for which we choose the matrices $\begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix}$, $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$ respectively. Notice that the matrices we've chosen are elements of the center of $\mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z})$ and hence normalize G. For -1, take the matrix $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ for which one can check explicitly that it does normalize G.

Thus for the element 2, we take $\begin{pmatrix}-1 & 0\\ 0 & 1\end{pmatrix}\cdot\begin{pmatrix}4 & 0\\ 0 & 4\end{pmatrix}=\begin{pmatrix}-4 & 0\\ 0 & 4\end{pmatrix}$ and for -4, take $\begin{pmatrix}-1 & 0\\ 0 & 1\end{pmatrix}\cdot\begin{pmatrix}2 & 0\\ 0 & 2\end{pmatrix}=\begin{pmatrix}-2 & 0\\ 0 & 2\end{pmatrix}$. Then the coset representatives for G'/G are

$$\left\{\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix},\begin{pmatrix}2 & 0\\ 0 & 2\end{pmatrix},\begin{pmatrix}4 & 0\\ 0 & 4\end{pmatrix},\begin{pmatrix}-1 & 0\\ 0 & 1\end{pmatrix},\begin{pmatrix}-4 & 0\\ 0 & 4\end{pmatrix},\begin{pmatrix}-2 & 0\\ 0 & 2\end{pmatrix}\right\}.$$

One can check explicitly that G'/G is indeed a group and the determinant map $G'/G\to(\mathbb{Z}/9\mathbb{Z})^*$ is well defined on classes. In particular, we can easily see that the map is an isomorphism. It is worth noting here, that since $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})\cong(\mathbb{Z}/9\mathbb{Z})^*$, we have an isomorphism $G'/G\cong\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$. As pointed out by Elkies, we now have a model $\tilde{X}(9)/G'$ of $X(9)/G$ over $\mathbb{Q}$, which means we can ask for points on $\tilde{X}(9)/G'(\mathbb{Q})$ that correspond to elliptic curves $E/\mathbb{Q}$, with $\bar{\rho}_{3,E}$ equal to G' mod 9.

4.4 The cusps of $X(9)/G$

In this section we investigate the cusps of $X(9)/G$ in a two step process: we first find the cusps of $X(9)$, i.e. the set of orbits of the action of $\Gamma(9)$ on $\mathbb{P}^1_{\mathbb{Q}}$ (that we denote by $C(\Gamma(9))$) and then the orbits of the action of G on $C(\Gamma(9))$. A priori, it is not clear how does G act on $C(\Gamma(9))$. The following lemma ([Dia & Shur], Proposition 3.8.3) gives an explicit description of elements of $C(\Gamma(9))$ as pairs of integers mod 9 satisfying a certain condition.

Lemma 4.2 *Let $s=\frac{a}{c}$, $s'=\frac{a'}{c'}\in\mathbb{P}^1_{\mathbb{Q}}$ in lowest terms. Then*

$$\begin{aligned}\Gamma(N)s'=\Gamma(N)s &\iff \begin{pmatrix}a'\\ c'\end{pmatrix}=\pm\gamma\begin{pmatrix}a\\ c\end{pmatrix}\ \textit{for some}\ \gamma\in\Gamma(N)\\ &\iff \begin{pmatrix}a'\\ c'\end{pmatrix}=\pm\begin{pmatrix}a\\ c\end{pmatrix}\ \ \textit{mod } N.\end{aligned}$$

Proof: Suppose $s'=\gamma\cdot s$ for some $\gamma\in\Gamma(N)$. Write $\gamma=\begin{pmatrix}w & x\\ y & z\end{pmatrix}$. Then if $s,s'\neq\infty$, $s'=\gamma\cdot s\iff\frac{a'}{c'}=\frac{w\frac{a}{c}+x}{y\frac{a}{c}+z}\iff\frac{a'}{c'}=\frac{wa+xc}{ya+zc}=\frac{-(wa+xc)}{-(ya+zc)}=\frac{(-w)a+(-x)c}{(-y)a+(-z)c}$. Notice that $\gcd(wa+xc,ya+zc)=1$ since both the numerator and denominator

linearly combine back to a and c under γ^{-1}. Hence $\frac{a'}{c'} = \frac{wa+xc}{ya+zc} \iff \begin{pmatrix} a' \\ c' \end{pmatrix} = \begin{pmatrix} wa+xc \\ ya+zc \end{pmatrix} = \gamma \begin{pmatrix} a \\ c \end{pmatrix}$ or $\begin{pmatrix} a' \\ c' \end{pmatrix} = \begin{pmatrix} (-w)a+(-x)c \\ (-y)a+(-z)c \end{pmatrix} = -\gamma \begin{pmatrix} a \\ c \end{pmatrix}$.

In the case where $c = 0$, $s = \infty$ we have

$$\frac{a'}{c'} = \begin{pmatrix} w & x \\ y & z \end{pmatrix} \cdot \infty = \frac{w}{y} = \frac{-w}{-y} \iff a' = w, c' = y$$

(since $\gcd(w, y) = 1$, otherwise $1 < \gcd(w, y) \mid \det(\gamma)$ which is a contradiction)

$$\iff \begin{pmatrix} a' \\ c' \end{pmatrix} = \begin{pmatrix} a' & x \\ c' & z \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} \text{ or } \begin{pmatrix} a' \\ c' \end{pmatrix} = - \begin{pmatrix} a' & x \\ c' & z \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

(where we take $a = 1$ so that $gcd(a, 0) = 1$)

$$\iff \begin{pmatrix} a' \\ c' \end{pmatrix} = \pm\gamma \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

Similarly if $c' = 0$, $s' = \infty$, $a' = 1$, we have

$$\infty = \begin{pmatrix} w & x \\ y & z \end{pmatrix} \cdot \frac{a}{c} = \frac{wa+xc}{ya+zc} \iff ya + zc = 0$$

$$\iff \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} w & x \\ y & z \end{pmatrix} \begin{pmatrix} a \\ c \end{pmatrix} \text{ or } \begin{pmatrix} 1 \\ 0 \end{pmatrix} = - \begin{pmatrix} w & x \\ y & z \end{pmatrix} \begin{pmatrix} a \\ c \end{pmatrix}$$

$$\iff \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \pm\gamma \begin{pmatrix} a \\ c \end{pmatrix}.$$

Now suppose $\begin{pmatrix} a' \\ c' \end{pmatrix} = \pm\gamma \begin{pmatrix} a \\ c \end{pmatrix}$, where $\gamma = \begin{pmatrix} w & x \\ y & z \end{pmatrix} \in \Gamma(N)$, i.e. $w, z \equiv 1 \bmod N$ and $x, y \equiv 0 \bmod N$. So $\begin{pmatrix} a' \\ c' \end{pmatrix} = \pm \begin{pmatrix} wa + xc \\ ya + zc \end{pmatrix} = \pm \begin{pmatrix} a \\ c \end{pmatrix} \bmod N$.

Conversely suppose $\begin{pmatrix} a' \\ c' \end{pmatrix} = \pm \begin{pmatrix} a \\ c \end{pmatrix} \bmod N$. Then there exists integers b, d such that $\gamma := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$. We have that $\gamma \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} a \\ c \end{pmatrix} = \begin{pmatrix} a' \\ c' \end{pmatrix} \bmod N$. This implies that $\gamma^{-1} \begin{pmatrix} a \\ c \end{pmatrix} = \gamma^{-1} \begin{pmatrix} a' \\ c' \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \bmod N$ (†). Write $\begin{pmatrix} \alpha N + 1 \\ \beta N \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \bmod N$. Since $\gcd(\alpha N + 1, \beta N) = 1$, using Euclid's algorithm we can find integers A, B such that $A(\alpha N + 1) + B\beta N = 1$ and $(-\alpha A)(\alpha N + 1) + (-\alpha B)(\beta N) = -\alpha$. Let $y := -\alpha A$, $x := -\alpha B$ and $\gamma' := \begin{pmatrix} \alpha N + 1 & xN \\ \beta N & 1 + yN \end{pmatrix}$. We have that $\det\gamma' = (\alpha N + 1)(yN + 1) - \beta x N^2 = ((\alpha N + 1)y - \beta x N)N + \alpha N + 1 = -\alpha N + \alpha N + 1 = 1$ and hence $\gamma' \in \Gamma(N)$. Moreover, $\gamma' \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \alpha N + 1 \\ \beta N \end{pmatrix}$ and $(\gamma)'^{-1} \begin{pmatrix} \alpha N + 1 \\ \beta N \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$. We had that (†) $\gamma^{-1} \begin{pmatrix} a' \\ c' \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \bmod N = \begin{pmatrix} \alpha N + 1 \\ \beta N \end{pmatrix}$ which implies that $(\gamma')^{-1}\gamma^{-1} \begin{pmatrix} a' \\ c' \end{pmatrix} = (\gamma')^{-1} \begin{pmatrix} \alpha N + 1 \\ \beta N \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$. Finally applying γ gives $\gamma(\gamma')^{-1}\gamma^{-1} \begin{pmatrix} a' \\ c' \end{pmatrix} = \begin{pmatrix} a \\ c \end{pmatrix}$. Notice that $\Gamma(N)$ is the kernel of the reduction mod N map $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ which implies that $\Gamma(N) \lhd \mathrm{SL}_2(\mathbb{Z})$ and thus $\delta := \gamma(\gamma')^{-1}\gamma^{-1} \in \Gamma(N)$ gives $s' = \delta \cdot s$.

□

Since there are a lot of lifts of $\pm \begin{pmatrix} a \\ c \end{pmatrix}$ mod N in $\mathbb{Z}^2$ and we insist on the ones of the form $\begin{pmatrix} a' \\ c' \end{pmatrix}$ such that $\gcd(a', c') = 1$ (since we want $\frac{a'}{c'}$ to be in lowest terms) we make use of the following lemma:

Lemma 4.3 *Define an element* $\begin{pmatrix} a \\ c \end{pmatrix} \in \mathbb{Z}^2$ *as primitive when* $gcd(a, c) = 1$ *and denote by* $\begin{pmatrix} \bar{a} \\ \bar{c} \end{pmatrix} := \begin{pmatrix} a \\ c \end{pmatrix}$ *mod N. Then* $\begin{pmatrix} \bar{a} \\ \bar{c} \end{pmatrix}$ *has a primitive lift in* $\mathbb{Z}^2$ *if and only if* $gcd(a, c, N) = 1$.

Proof: If $\begin{pmatrix} a' \\ c' \end{pmatrix} \in \mathbb{Z}^2$ is a primitive lift of $\begin{pmatrix} \bar{a} \\ \bar{c} \end{pmatrix}$, then $a' = \bar{a} + t'N$, $c' = \bar{c} + k'N$, for integers t', k'. Moreover, $a = \bar{a} + tN$, $c = \bar{c} + kN$, for $t, k \in \mathbb{Z}$. Since $\gcd(a', c') = 1$, we can find integers x, y such that $xa' + yc' = 1$. But $a' = a + (t' - t)N$ and $c' = c + (k' - k)N$. Therefore $x(a + (t' - t)N) + y(c + (k' - k)N) = 1$. Rearranging this gives $xa+yc+N(x(t'-t)+y(k'-k)) = 1$ and hence $\gcd(a, c, N) = 1$. Conversely, if $\gcd(a, c, N) = 1$, then there exists $x, y, z \in \mathbb{Z}$ such that $xa + yc + zN = 1$. So the matrix given by $\begin{pmatrix} a & -y \\ c & x \end{pmatrix}$ has determinant congruent to 1 mod N, as a result its reduction mod N lives in $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. Using the fact that the reduction mod N map $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ is surjective (see Lemma 6.1), we can find a lift $A := \begin{pmatrix} a' & -y' \\ c' & x' \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ of $\begin{pmatrix} \bar{a} & -\bar{y} \\ \bar{c} & \bar{x} \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. But then $\det(A) = x'a' + y'c' = 1$ and thus $\gcd(a', c') = 1$. □

We are now in good shape finding the cusps of $\Gamma(9)$. We first list all the pairs $\begin{pmatrix} a \\ c \end{pmatrix} \in \mathbb{Z}^2$ with $a, c \in \{0, 1, ..., 8\}$ and $\gcd(a, c, 9) = 1$;

$$\left\{ \begin{pmatrix} a \\ c \end{pmatrix} : a \in \{1, 2, 4, 5, 7, 8\}, c \in \{0, 3, 6\} \right\} \cup \left\{ \begin{pmatrix} a \\ c \end{pmatrix} : a \in \{0, 1, ..., 8\}, c \in \{1, 2, 4, 5, 7, 8\} \right\}.$$

Notice that we have 72 elements in total. Next we collect them in pairs of the form $\pm \begin{pmatrix} a \\ c \end{pmatrix}$ mod 9;

$$\pm\begin{pmatrix}1\\0\end{pmatrix}, \pm\begin{pmatrix}2\\0\end{pmatrix}, \pm\begin{pmatrix}4\\0\end{pmatrix}$$

$$\pm\begin{pmatrix}a\\c\end{pmatrix} : a \in \{0,1,...,8\}, c \in \{1,2,4\}$$

$$\pm\begin{pmatrix}a\\3\end{pmatrix} : a \in \{1,2,4,5,7,8\}.$$

This gives 36 pairs, half of the 72 elements of the previous step. For each of these pairs we then find a good lift $\begin{pmatrix}a'\\c'\end{pmatrix} \in \mathbb{Z}^2$ (whose existence is now guaranteed by the above lemma) satisfying $\gcd(a', c') = 1$ and corresponding to the cusp $\frac{a'}{c'} \in \mathbb{P}^1_{\mathbb{Q}}$;

$\pm\begin{pmatrix}a\\c\end{pmatrix}$ mod 9	**Lift**	**Cusp**	$\pm\begin{pmatrix}a\\c\end{pmatrix}$ mod 9	**Lift**	**Cusp**
$\pm\begin{pmatrix}1\\0\end{pmatrix}$	$\begin{pmatrix}1\\0\end{pmatrix}$	∞	$\pm\begin{pmatrix}6\\2\end{pmatrix}$	$\begin{pmatrix}6\\11\end{pmatrix}$	$\frac{6}{11}$
$\pm\begin{pmatrix}2\\0\end{pmatrix}$	$\begin{pmatrix}2\\9\end{pmatrix}$	$\frac{2}{9}$	$\pm\begin{pmatrix}7\\2\end{pmatrix}$	$\begin{pmatrix}7\\2\end{pmatrix}$	$\frac{7}{2}$
$\pm\begin{pmatrix}4\\0\end{pmatrix}$	$\begin{pmatrix}4\\9\end{pmatrix}$	$\frac{4}{9}$	$\pm\begin{pmatrix}8\\2\end{pmatrix}$	$\begin{pmatrix}8\\11\end{pmatrix}$	$\frac{8}{11}$
$\pm\begin{pmatrix}0\\1\end{pmatrix}$	$\begin{pmatrix}0\\1\end{pmatrix}$	0	$\pm\begin{pmatrix}1\\3\end{pmatrix}$	$\begin{pmatrix}1\\3\end{pmatrix}$	$\frac{1}{3}$
$\pm\begin{pmatrix}1\\1\end{pmatrix}$	$\begin{pmatrix}1\\1\end{pmatrix}$	1	$\pm\begin{pmatrix}2\\3\end{pmatrix}$	$\begin{pmatrix}2\\3\end{pmatrix}$	$\frac{2}{3}$
$\pm\begin{pmatrix}2\\1\end{pmatrix}$	$\begin{pmatrix}2\\1\end{pmatrix}$	2	$\pm\begin{pmatrix}4\\3\end{pmatrix}$	$\begin{pmatrix}4\\3\end{pmatrix}$	$\frac{4}{3}$
$\pm\begin{pmatrix}3\\1\end{pmatrix}$	$\begin{pmatrix}3\\1\end{pmatrix}$	3	$\pm\begin{pmatrix}5\\3\end{pmatrix}$	$\begin{pmatrix}5\\3\end{pmatrix}$	$\frac{5}{3}$
$\pm\begin{pmatrix}4\\1\end{pmatrix}$	$\begin{pmatrix}4\\1\end{pmatrix}$	4	$\pm\begin{pmatrix}7\\3\end{pmatrix}$	$\begin{pmatrix}7\\3\end{pmatrix}$	$\frac{7}{3}$
$\pm\begin{pmatrix}5\\1\end{pmatrix}$	$\begin{pmatrix}5\\1\end{pmatrix}$	5	$\pm\begin{pmatrix}8\\3\end{pmatrix}$	$\begin{pmatrix}8\\3\end{pmatrix}$	$\frac{8}{3}$
$\pm\begin{pmatrix}6\\1\end{pmatrix}$	$\begin{pmatrix}6\\1\end{pmatrix}$	6	$\pm\begin{pmatrix}0\\4\end{pmatrix}$	$\begin{pmatrix}9\\4\end{pmatrix}$	$\frac{9}{4}$
$\pm\begin{pmatrix}7\\1\end{pmatrix}$	$\begin{pmatrix}7\\1\end{pmatrix}$	7	$\pm\begin{pmatrix}1\\4\end{pmatrix}$	$\begin{pmatrix}1\\4\end{pmatrix}$	$\frac{1}{4}$
$\pm\begin{pmatrix}8\\1\end{pmatrix}$	$\begin{pmatrix}8\\1\end{pmatrix}$	8	$\pm\begin{pmatrix}2\\4\end{pmatrix}$	$\begin{pmatrix}11\\4\end{pmatrix}$	$\frac{11}{4}$
$\pm\begin{pmatrix}0\\2\end{pmatrix}$	$\begin{pmatrix}9\\2\end{pmatrix}$	$\frac{9}{2}$	$\pm\begin{pmatrix}3\\4\end{pmatrix}$	$\begin{pmatrix}3\\4\end{pmatrix}$	$\frac{3}{4}$
$\pm\begin{pmatrix}1\\2\end{pmatrix}$	$\begin{pmatrix}1\\2\end{pmatrix}$	$\frac{1}{2}$	$\pm\begin{pmatrix}4\\4\end{pmatrix}$	$\begin{pmatrix}4\\13\end{pmatrix}$	$\frac{4}{13}$
$\pm\begin{pmatrix}2\\2\end{pmatrix}$	$\begin{pmatrix}2\\11\end{pmatrix}$	$\frac{2}{11}$	$\pm\begin{pmatrix}5\\4\end{pmatrix}$	$\begin{pmatrix}5\\4\end{pmatrix}$	$\frac{5}{4}$
$\pm\begin{pmatrix}3\\2\end{pmatrix}$	$\begin{pmatrix}3\\2\end{pmatrix}$	$\frac{3}{2}$	$\pm\begin{pmatrix}6\\4\end{pmatrix}$	$\begin{pmatrix}6\\13\end{pmatrix}$	$\frac{6}{13}$
$\pm\begin{pmatrix}4\\2\end{pmatrix}$	$\begin{pmatrix}4\\11\end{pmatrix}$	$\frac{4}{11}$	$\pm\begin{pmatrix}7\\4\end{pmatrix}$	$\begin{pmatrix}7\\4\end{pmatrix}$	$\frac{7}{4}$

continued on next page

continued from previous page

$\pm\begin{pmatrix}a\\c\end{pmatrix}$ mod 9	**Lift**	**Cusp**	$\pm\begin{pmatrix}a\\c\end{pmatrix}$ mod 9	**Lift**	**Cusp**
$\pm\begin{pmatrix}5\\2\end{pmatrix}$	$\begin{pmatrix}5\\2\end{pmatrix}$	$\frac{5}{2}$	$\pm\begin{pmatrix}8\\4\end{pmatrix}$	$\begin{pmatrix}8\\13\end{pmatrix}$	$\frac{8}{13}$

Since we have found a bijection between the cusps of $\Gamma(9)$ and elements of the set $\left\{\pm\begin{pmatrix}a\\c\end{pmatrix} \mod 9\right\}$, the action of $G \subseteq \mathrm{SL}_2(\mathbb{Z}/9\mathbb{Z})$ is the one given by matrix multiplication on the elements of the second set. In particular, it turns out that this action has 3 set of orbits which are summarized in the following table:

Orbit of 0 *under* G		*Orbit of* 1 *under* G		*Orbit of* ∞ *under* G	
$\pm\begin{pmatrix}a\\c\end{pmatrix}$ mod 9	C($\Gamma(9)$)	$\pm\begin{pmatrix}a\\c\end{pmatrix}$ mod 9	C($\Gamma(9)$)	$\pm\begin{pmatrix}a\\c\end{pmatrix}$ mod 9	C($\Gamma(9)$)
$\pm\begin{pmatrix}4\\0\end{pmatrix}$	$\frac{4}{9}$	$\pm\begin{pmatrix}2\\0\end{pmatrix}$	$\frac{2}{9}$	$\pm\begin{pmatrix}1\\0\end{pmatrix}$	∞
$\pm\begin{pmatrix}0\\1\end{pmatrix}$	0	$\pm\begin{pmatrix}1\\1\end{pmatrix}$	1	$\pm\begin{pmatrix}2\\1\end{pmatrix}$	2
$\pm\begin{pmatrix}1\\2\end{pmatrix}$	$\frac{1}{2}$	$\pm\begin{pmatrix}4\\1\end{pmatrix}$	4	$\pm\begin{pmatrix}3\\1\end{pmatrix}$	3
$\pm\begin{pmatrix}2\\2\end{pmatrix}$	$\frac{2}{11}$	$\pm\begin{pmatrix}5\\1\end{pmatrix}$	5	$\pm\begin{pmatrix}6\\1\end{pmatrix}$	6
$\pm\begin{pmatrix}7\\2\end{pmatrix}$	$\frac{7}{2}$	$\pm\begin{pmatrix}8\\1\end{pmatrix}$	8	$\pm\begin{pmatrix}7\\1\end{pmatrix}$	7
$\pm\begin{pmatrix}8\\2\end{pmatrix}$	$\frac{8}{11}$	$\pm\begin{pmatrix}3\\2\end{pmatrix}$	$\frac{3}{2}$	$\pm\begin{pmatrix}0\\2\end{pmatrix}$	$\frac{9}{2}$
$\pm\begin{pmatrix}2\\3\end{pmatrix}$	$\frac{2}{3}$	$\pm\begin{pmatrix}4\\2\end{pmatrix}$	$\frac{4}{11}$	$\pm\begin{pmatrix}4\\3\end{pmatrix}$	$\frac{4}{3}$
$\pm\begin{pmatrix}7\\3\end{pmatrix}$	$\frac{7}{3}$	$\pm\begin{pmatrix}5\\2\end{pmatrix}$	$\frac{5}{2}$	$\pm\begin{pmatrix}5\\3\end{pmatrix}$	$\frac{5}{3}$
$\pm\begin{pmatrix}1\\4\end{pmatrix}$	$\frac{1}{4}$	$\pm\begin{pmatrix}6\\2\end{pmatrix}$	$\frac{6}{11}$	$\pm\begin{pmatrix}2\\4\end{pmatrix}$	$\frac{11}{4}$
$\pm\begin{pmatrix}3\\4\end{pmatrix}$	$\frac{3}{4}$	$\pm\begin{pmatrix}1\\3\end{pmatrix}$	$\frac{1}{3}$	$\pm\begin{pmatrix}4\\4\end{pmatrix}$	$\frac{4}{13}$

continued on next page

continued from previous page

Orbit of 0 *under* G		*Orbit of* 1 *under* G		*Orbit of* ∞ *under* G	
$\pm\begin{pmatrix}a\\c\end{pmatrix}$ mod 9	C($\Gamma(9)$)	$\pm\begin{pmatrix}a\\c\end{pmatrix}$ mod 9	C($\Gamma(9)$)	$\pm\begin{pmatrix}a\\c\end{pmatrix}$ mod 9	C($\Gamma(9)$)
$\pm\begin{pmatrix}6\\4\end{pmatrix}$	$\frac{6}{13}$	$\pm\begin{pmatrix}8\\3\end{pmatrix}$	$\frac{8}{3}$	$\pm\begin{pmatrix}5\\4\end{pmatrix}$	$\frac{5}{4}$
$\pm\begin{pmatrix}8\\4\end{pmatrix}$	$\frac{8}{13}$	$\pm\begin{pmatrix}0\\4\end{pmatrix}$	$\frac{9}{4}$	$\pm\begin{pmatrix}7\\4\end{pmatrix}$	$\frac{7}{4}$

We conclude that $X(9)/G$ has 3 cusps, of which we choose representatives $\{0, 1, \infty\}$.

4.5 The field of definition of the cusps of $X(9)/G$

What we want to understand now is how the absolute Galois group of $\mathbb{Q}$ acts on the cusps of $X(9)/G$. In particular we want to consider the model of $X(9)/G$ over $\mathbb{Q}$, given by $\tilde{X}(9)/G'$. This will give us an indication of whether the cusps are indeed defined over $\mathbb{Q}$ or not (i.e. whether the corresponding generalised elliptic curves are defined over $\mathbb{Q}$ or not). Recall that we gave a description of $\tilde{X}(9)$ as the set $\{(E, P, Q, \zeta) : e_9(P, Q) = \zeta\}$, where ζ is a primitive 9-th root of unity, $E/\mathbb{C}$ an elliptic curve and P, Q generators of $E[9]$. Given an element $(E, P, Q, \zeta) \in \tilde{X}(9)$, take $a \in (\mathbb{Z}/9\mathbb{Z})^*$ such that $\zeta^a = e^{\frac{2\pi i}{9}}$. This gives $e_9(P, Q)^a = e_9(P, aQ) = e^{\frac{2\pi i}{9}}$ and we identify (E, P, Q, ζ) with the pair $(\tau, e^{\frac{2\pi i a}{9}})$ where $E/\mathbb{C}$ corresponds to the lattice $\Lambda = \mathbb{Z} + \tau\mathbb{Z}$ and $\frac{1}{9}, \frac{\tau}{9}$ get mapped to P, aQ. So we can rewrite $\tilde{X}(9)$ as the set $\{(\tau, \zeta) : \tau \in X(9),\ \zeta \in \mu_9^*\}$ (where μ_9^* denotes the set of primitive 9-th roots of unity). Then the action of $\mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z})$ on the new realisation of $\tilde{X}(9)$ is given as follows; for $\gamma \in \mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z})$, $\gamma \cdot (\tau, \zeta) := (\gamma' \cdot \tau, \zeta^{\det\gamma})$, where $\gamma' = \gamma \begin{pmatrix}1 & 0\\0 & a\end{pmatrix}$, $a = (\det\gamma)^{-1}$ (notice here that $\det\gamma' = a\ \det\gamma = 1$ and hence $\gamma' \in \mathrm{SL}_2(\mathbb{Z}/9\mathbb{Z})$ giving an action on the elements of $X(9)$). The action on the cusps is similarly given by $\gamma \cdot (c, \zeta) := (\gamma \cdot c, \zeta^{\det\gamma})$, where $c \in C(X(9))$ are being considered as elements of $(\mathbb{Z}/9\mathbb{Z})^2$ (see Lemma 4.2). Notice that again the stabilizer of each component of $\tilde{X}(9)$ is given by $\mathrm{SL}_2(\mathbb{Z}/9\mathbb{Z})$ and thus the orbits are preserved.

Now that we can realise $\tilde{X}(9)$ as the set $\{(\tau, \zeta) : \tau \in X(9), \zeta \in \mu_9^*\}$, we can view the cusps of $\tilde{X}(9)$ as the set $\{(c, \zeta) : c \in C(X(9)), \zeta \in \mu_9^*\}$. Then we have an action of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ on $C(\tilde{X}(9))$ defined by $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, $(c, \zeta) \in C(\tilde{X}(9))$,

$(c,\zeta)^\sigma := (c,\zeta^\sigma)$ and as a consequence the action factors through $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$. However, the G'-orbits of $C(\tilde{X}(9))$ are not Galois invariant under this action of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$; given $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, (c,ζ) a representative of a G'-orbit of $C(\tilde{X}(9))$, we have that $(c,\zeta)^\sigma = (c,\zeta^\sigma)$. We can find an element $\gamma \in G'$ such that $(\zeta^\sigma)^{\det\gamma} = \zeta$ (since $\det : G'/G \to (\mathbb{Z}/9\mathbb{Z})^*$ is an isomorphism), but we can't always find $\gamma \in G'$ such that $\gamma \cdot c = c$ and $(\zeta^\sigma)^{\det\gamma} = \zeta$. Hence$(c,\zeta)$ and $(c,\zeta)^\sigma$ are not always in the same G'-orbit. As a result, the cusps of $\tilde{X}(9)/G'$ and therefore of $X(9)/G$ are not $\mathbb{Q}$-rational.

In our attempt to find the field of definition of the cusps of $\tilde{X}(9)/G'$, we observe the following; for the cusp $\infty \in C(\tilde{X}(9)/G')$, if $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ maps $(\infty,\zeta) \mapsto (\infty,\zeta^a)$, then (∞,ζ) and (∞,ζ^a) are in the same G'-orbit if and only if there exists a matrix $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G'$ such that $g \cdot (\infty,\zeta) = (\infty,\zeta^a) \iff (g\cdot\infty, \zeta^{\det g}) = (\infty,\zeta^a)$. Recall that ∞ corresponds to the pair $\pm\begin{pmatrix} 1 \\ 0 \end{pmatrix} \in (\mathbb{Z}/9\mathbb{Z})^2$. Thus, $(g\cdot\infty,\zeta^{\det g}) = (\infty,\zeta^a) \iff \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} \pm 1 \\ 0 \end{pmatrix} = \pm\begin{pmatrix} a \\ c \end{pmatrix} = \pm\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $\det g = a \iff g = \begin{pmatrix} \pm 1 & b \\ 0 & 1 \end{pmatrix}$ and $a = \det g = \pm 1$. Using GAP (see Appendix - section 6.1, code 4) we find that the only matrices in G of the form $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$ are $\begin{pmatrix} \pm 1 & 0 \\ 0 & 1 \end{pmatrix}$. The determinants of these matrices are $\pm 1 \in (\mathbb{Z}/9\mathbb{Z})^*$ and under the isomorphism $(\mathbb{Z}/9\mathbb{Z})^* \cong \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$, they correspond to the automorphisms $\zeta \mapsto \zeta$ and $\zeta \mapsto \zeta^{-1}$. The fixed field of the subgroup of these two automorphisms in $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ is the field $K := \mathbb{Q}(\zeta+\zeta^{-1})$. Notice that $(\zeta+\zeta^{-1})^3 = \zeta^3 + 3(\zeta+\zeta^{-1}) - \zeta^3 - 1$ (since the minimal polynomial of ζ^6 is $\Phi_9(x) = x^6+x^3+1$). So $(\zeta+\zeta^{-1})^3 = 3(\zeta+\zeta^{-1}) - 1$ and $\zeta+\zeta^{-1}$ satisfies the polynomial $x^3 - 3x + 1$ which is easily seen to be irreducible over $\mathbb{Q}$ and consequently it is the minimal polynomial. Therefore $K/\mathbb{Q}$ is a degree 3 extension. We conclude that the cusp ∞ is defined over K and the other two cusps of $\tilde{X}(9)/G'$ (and hence of $X(9)/G$) are the conjugates of the cusp ∞ under the action of $\mathrm{Gal}(K/\mathbb{Q})$. As pointed out by Elkies, the fact that the cusps are not defined over $\mathbb{Q}$ will make the case of finding rational functions on $X(9)/G$ trickier, since these will no longer have coefficients in $\mathbb{Q}$, but in K.

4.6 The genus of $X(9)/G$

So far, we have only seen a moduli description of $X(9)/G$. Recall that we viewed a point on $X(9)/G$ as the modular pair $(E/\mathbb{C}, \{$ equivalence class of (P,Q) mod $G\})$ with $e_9(P,Q) = \zeta_9$. However, it is also useful (for example in computing the genus of $X(9)/G$) to see how does $X(9)/G$ looks like as a Riemann surface. So we are looking for a congruence subgroup Γ such that $X(9)/G = X(\Gamma)$. Let $\Gamma_G := \{g \in \mathrm{SL}_2(\mathbb{Z}) : g \in G \mod 9\}$. Notice that $\Gamma(9) \subseteq \Gamma_G$ and as a result, Γ_G is a congruence subgroup.

Claim: $X(9)/G = X(\Gamma_G)$.

Proof: To prove this, we show that the two modular curves give the same moduli space. We follow the same line of argument as in the proof of Theorem 2.14. Take a modular pair $(E/\mathbb{C}, \{$equivalence class of (P,Q) mod $G\})$ with $e_9(P,Q) = \zeta_9$. Then as pointed out in the proof of Proposition 2.5, E corresponds to a lattice Λ and is homothetic to Λ_τ for some $\tau \in \mathbb{H}$. Moreover, in the proof of Theorem 2.14 we saw that the modular pair $(E,(P,Q))$ (where (P,Q) are representatives of the equivalence class) is isomorphic to $(E_{\tau'}, (\frac{\tau'}{9} + \Lambda_{\tau'}, \frac{1}{9} + \Lambda_{\tau'}))$ and the Weil pairing is preserved. Take two arbitrary pairs $(E_\tau, (\frac{\tau}{9} + \Lambda_\tau, \frac{1}{9} + \Lambda_\tau))$, $(E_{\tau'}, (\frac{\tau'}{9} + \Lambda_{\tau'}, \frac{1}{9} + \Lambda_{\tau'}))$ and suppose τ and τ' are in the same Γ_G-orbit. So there exists $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_G$ such that $\gamma \cdot \tau = \tau'$. Therefore $(c\tau+d)\tau' = a\tau+b$, $(c\tau+d)\Lambda_{\tau'} = \Lambda_\tau$ and $E_\tau \cong E_{\tau'}$ (see the proof of Theorem 2.14 for the omitted details). Moreover, $(c\tau + d)(\frac{1}{9} + \Lambda_{\tau'}) = \frac{c\tau+d}{9} + \Lambda_\tau$ and $(c\tau+d)(\frac{\tau'}{9} + \Lambda_{\tau'}) = \frac{a\tau+b}{9} + \Lambda_\tau$ Choosing an isomorphism with $(\mathbb{Z}/9\mathbb{Z})^2$, $\frac{\tau}{9} + \Lambda_\tau \mapsto (1,0)$, $\frac{1}{9} + \Lambda_\tau \mapsto (0,1)$ we have that for $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_G$ (denote by $\bar{\gamma} = \begin{pmatrix} \bar{a} & \bar{b} \\ \bar{c} & \bar{d} \end{pmatrix}$ its image mod 9 which lies in G),

$$(1,0)\bar{\gamma} = (\bar{a}, \bar{b}) \mapsto \frac{\bar{a}\tau + \bar{b}}{9} + \Lambda_\tau$$

$$(0,1)\bar{\gamma} = (\bar{c}, \bar{d}) \mapsto \frac{\bar{c}\tau + \bar{d}}{9} + \Lambda_\tau.$$

Hence $\bar{\gamma} : (\frac{\tau}{9} + \Lambda_\tau, \frac{1}{9} + \Lambda_\tau) \mapsto (\frac{\bar{a}\tau+\bar{b}}{9} + \Lambda_\tau, \frac{\bar{c}\tau+\bar{d}}{9} + \Lambda_\tau)$ and $(E_\tau, (\frac{\tau}{9} + \Lambda_\tau, \frac{1}{9} + \Lambda_\tau))$, $(E_\tau, (\frac{\bar{a}\tau+\bar{b}}{9} + \Lambda_\tau, \frac{\bar{c}\tau+\bar{d}}{9} + \Lambda_\tau))$ are in the same G-orbit. As a result, the modular pairs $(E_\tau, (\frac{\tau}{9} + \Lambda_\tau, \frac{1}{9} + \Lambda_\tau) \mod G)$ and $(E_{\tau'}, (\frac{\tau'}{9} + \Lambda_{\tau'}, \frac{1}{9} + \Lambda_{\tau'}) \mod G)$ are isomorphic.

Conversely, suppose $(E_\tau, (\frac{\tau}{9} + \Lambda_\tau, \frac{1}{9} + \Lambda_\tau) \mod G)$, $(E_{\tau'}, (\frac{\tau'}{9} + \Lambda_{\tau'}, \frac{1}{9} + \Lambda_{\tau'}) \mod G)$

are isomorphic. Then there exists $\alpha \in \mathbb{C}^*$ such that $\alpha\Lambda_{\tau'} = \Lambda_\tau$ and $\alpha(\frac{\tau'}{9} + \Lambda_{\tau'}) = \frac{a\tau+b}{9} + \Lambda_\tau$, $\alpha(\frac{1}{9} + \Lambda_{\tau'}) = \frac{c\tau+d}{9} + \Lambda_\tau$, for $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$ (here we use the same isomorphism as before). We have a change of basis matrix $\gamma = \begin{pmatrix} w & x \\ y & z \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ such that $\gamma \begin{pmatrix} \tau \\ 1 \end{pmatrix} = \begin{pmatrix} w\tau + x \\ y\tau + z \end{pmatrix} = \begin{pmatrix} \alpha\tau' \\ \alpha \end{pmatrix} \implies \alpha = y\tau + z$ and $\alpha\tau' = w\tau + x$. Replacing into the previous equations gives $\frac{\alpha\tau'}{9} + \Lambda_\tau = \frac{a\tau+b}{9} + \Lambda_\tau = \frac{w\tau+x}{9} + \Lambda_\tau$ and $\frac{\alpha}{9} + \Lambda_\tau = \frac{c\tau'+d}{9} + \Lambda_\tau = \frac{y\tau+z}{9} + \Lambda_\tau$. This implies that $\gamma \equiv \begin{pmatrix} a & b \\ c & d \end{pmatrix} \bmod 9$ and thus $\gamma \in \Gamma_G$. But $\gamma \cdot \tau = \frac{w\tau+x}{y\tau+z} = \tau'$ and hence τ, τ' are in the same Γ_G-orbit. □

We would now like to compute the genus of $X(9)/G$ as a Riemann surface, using the genus formula $g_{X(\Gamma_G)} = 1 + \frac{d_{\Gamma_G}}{12} - \frac{\epsilon_2}{4} - \frac{\epsilon_3}{3} - \frac{\epsilon_\infty}{2}$. This involves computing the following unknowns; d_{Γ_G} which is the projective index of Γ_G, ϵ_2, ϵ_3 and ϵ_∞ which are the elliptic points of period 2 and 3 in $X(\Gamma_G)$ and the number of cusps of $X(\Gamma_G)$. We have already computed the last unknown in the list and we have found that $\epsilon_\infty = 3$. Unfortunately, the computations regarding the rest of the unknowns are very large to be done by hand and we use the aid of the computer program SAGE to compute them. The code can be found in Appendix - section 6.1, code 5. It turns out that the projective index of $X(\Gamma_G)$ is 27 and $X(\Gamma_G)$ has 3 elliptic points of period 2 and 3 of period 3. Plugging these into the formula gives

$$g_{X(\Gamma_G)} = 1 + \frac{27}{12} - \frac{3}{4} - \frac{3}{3} - \frac{3}{2} = 0.$$

Consequently, $X(\Gamma_G)$ is a genus 0, compact Riemann surface. By the classification of compact Riemann surfaces, $X(\Gamma_G)$ is analytically isomorphic to the Riemann sphere $\mathbb{P}^1_{\mathbb{C}}$.

However, in our case we are interested in the $\mathbb{Q}$-structure of $X(9)/G$. In section 4.3, we have found a $\mathbb{Q}$-model of $X(9)/G$, namely $\tilde{X}(9)/G'$. In general though, a projective non-singular algebraic curve C defined over $\mathbb{Q}$ of genus 0, need not be algebraically isomorphic over $\mathbb{Q}$ with $\mathbb{P}^1_{\mathbb{Q}}$. As an example, consider the projective subvariety of $\mathbb{P}^2_{\mathbb{Q}}$, given by $C := \{[x : y : z] \in \mathbb{P}^1_{\mathbb{Q}} : x^2+y^2+2z^2 = 0\}$. Then the map $[x : y] \to [\sqrt{2}(x^2 - y^2) : 2\sqrt{2}xy : i(x^2 + y^2)]$ gives an algebraic isomorphism of C with $\mathbb{P}^1_{\mathbb{Q}}$ over $\mathbb{Q}(i, \sqrt{2})$. It is clear that the equation $x^2 + y^2 + 2z^2 = 0$ has no solution over $\mathbb{R}$ and hence no solution over $\mathbb{Q}$. As a result C has no $\mathbb{Q}$-rational points and therefore no algebraic isomorphism of C with $\mathbb{P}^1_{\mathbb{Q}}$ over $\mathbb{Q}$ can exist. A theorem that gives a sufficient condition for an algebraic curve of genus 0 defined

over $\mathbb{Q}$ to be algebraically isomorphic to $\mathbb{P}^1_{\mathbb{Q}}$ states the following:

Theorem 4.4 ***Max Noether:*** *If $C/\mathbb{Q}$ is a genus 0 projective non-singular algebraic curve that has a $\mathbb{Q}$-rational divisor of odd degree, then $C \cong \mathbb{P}^1_{\mathbb{Q}}$.*

Proof: Let D be a divisor of C of odd degree, say $2n+1$, defined over $\mathbb{Q}$. Then denote, as usual, by K_C a canonical divisor of C defined over $\mathbb{Q}$. We have that $\deg(K_C) = 2\text{genus}(C) - 2 = -2$ ([Silverman 1], II, Corollary 5.5(b)) and as a result, the divisor $D' := D + nK_C$ has degree 1. In particular, D' is fixed by the action of $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ and thus it is defined over $\mathbb{Q}$. Riemann-Roch theorem states that $l(D') - l(K_C - D') = \deg(D') - \text{genus}(C) + 1 = 1 - 0 + 1 = 2$. Hence $l(D') \geq 2$. Since $\mathfrak{L}(D')$ has a basis of functions in $\mathbb{Q}(C)$ (see Proposition 2.8), we can take $f \in \mathbb{Q}(C) \cap \mathfrak{L}(D')$, which has $(f)+D' \geq 0$ and $\deg((f)+D') = \deg(f)+\deg D' = 0+1 = 1$. But an effective divisor of degree 1 is necessarily a point, i.e. $(f) + D' =: (P)$ is a $\mathbb{Q}$-rational point on C. Similarly, as in the case of D', Riemann-Roch gives $l(P) \geq 2$ and consequently $\mathfrak{L}(P)$ has a non-constant element $g \in \mathbb{Q}(C)$ that has a simple pole at P (and is in fact locally injective) and can serve as an isomorphism $C \cong \mathbb{P}^1_{\mathbb{Q}}$ (by projecting about the point P via g). □

The natural cover $X(\Gamma_G) \to X(1)$ is of degree 27 which is odd (the index $[\text{SL}_2(\mathbb{Z}) : \Gamma_G]$ is equal to 27; see Appendix - section 6.1, code 5 for the computation). Hence the preimage of the cusp ∞ of $X(1)$ under the natural cover is a $\mathbb{Q}$-rational divisor of odd degree. Therefore, Theorem 4.4 now tells us that indeed $X(\Gamma_G)$ is algebraically isomorphic to $\mathbb{P}^1_{\mathbb{Q}}$. This is indeed great news since we now stand a chance of finding this isomorphism, that will allows us to read off the $\mathbb{Q}$-rational points of $X(9)/G$.

4.7 Modular units and Siegel functions

Definition 4.5 - *A **modular unit** on a modular curve $X(\Gamma)$ is a modular function (i.e. an element of its function field) whose divisor is supported at the cusps of $X(\Gamma)$.*

Definition 4.6 - *Let $a = (a_1, a_2) \in \mathbb{Z}^2$, $q_\tau = e^{2\pi i\tau}$, $q_z = e^{2\pi iz}$. Then the **Siegel function** corresponding to the vector a is defined to be the function on $\mathbb{H}$ given by $g_a(\tau) := -q_\tau^{\frac{1}{2}B_2(a_1)} e^{2\pi i a_2 \frac{a_1-1}{2}} (1-q_z) \prod_{n=1}^{\infty} (1-q_\tau^n q_z)(1-\frac{q_\tau^n}{q_z})$, where $B_2(x) = x^2 - x + \frac{1}{6}$ is the second Bernoulli polynomial.*

We can also express a Siegel function as a product of **Klein forms**

$$\mathfrak{k}_{(a_1,a_2)}(\tau) := e^{\pi i a_2(a_1-1)} q_\tau^{\frac{1}{2}a_1(a_1-1)}(1-q_z)\prod_{n=1}^{\infty}(1-q_\tau^n q_z)(1-q_\tau^n q_z^{-1})(1-q_\tau^n)^{-2}$$

and $\Delta^{\frac{1}{12}} = 2\pi i q_z^{\frac{1}{12}}\prod_{n=1}^{\infty}(1-q_z^n)^2$. In particular, we have $g_a(\tau) = \mathfrak{k}_a(\tau)\Delta^{\frac{1}{12}}$ (see [Kub & Lang] p.29, for a proof of this). We know that $\Delta(\tau)$ is a modular form of level $\mathrm{SL}_2(\mathbb{Z})$ (and thus of level $\Gamma(N)$, for all $N \geq 1$) and weight 12. It follows that $\Delta(\tau)^{\frac{1}{12}}$ is also of level $\mathrm{SL}_2(\mathbb{Z})$ and weight 1 .

The Siegel functions satisfy some nice properties that serve for our purpose, that is:

Theorem 4.7 *Assume that $a \in \mathbb{Z}^2$ has denominator dividing N. Then the Siegel function g_a is a modular function of level $SL_2(\mathbb{Z})$ and g_a^{12N} is of level $\Gamma(N)$. Furthermore, g_a has no zeroes or poles on $\mathbb{H}$ and hence its divisor is supported at the cusps (i.e. it is a modular unit).*

Proof: This is [Kub & Lang], Chapter 2, Theorem 1.2. □

As a result, we can think of the Siegel functions as generalizations of the modular form Δ which is also a modular unit, with a simple zero at the cusp ∞ of $X(1)$. For our purpose though, g_a^{12N} is quite restrictive since the theorem requires that $a = (a_1, a_2)$ has $a_2 \mid N$. To be more precise, since the cusps of $X(9)$ correspond bijectively to $\pm(a, b)$ mod 9, such that a, b are coprime (see Lemma 4.3), we need to find a modular function of level $\Gamma(9)$ that is also a modular unit, such that the restriction $a_2 \mid N$ is no longer there. For this, we make use of the following theorem:

Theorem 4.8 *A product $f = \prod_r \mathfrak{k}_r^{m(r)}$ of Klein forms is modular of level $\Gamma(N)$ $\iff$ the family $\{m(r)\}$ satisfies the following "quadratic" relations:*
N odd: $\sum m(r)r_1^2 \equiv \sum m(r)r_2^2 \equiv \sum m(r)r_1r_2 \equiv 0$ mod N
N even: $\sum m(r)r_1^2 \equiv \sum m(r)r_2^2 \equiv 0$ mod $2N$ and $\sum m(r)r_1r_2 \equiv 0$ mod N

Proof: This is [Kub & Lang], Chapter 3, Theorem 4.1. □

Since we want to keep the property of Siegel functions being modular units, we consider the product $F := \prod_r g_{(a_r,b_r)}^{m(r)} = \prod_r \mathfrak{k}_{(a_r,b_r)}^{m(r)}\Delta^{\frac{m(r)}{12}}$ such that $\sum m(r)a_r^2 \equiv \sum m(r)b_r^2 \equiv \sum m(r)a_rb_r \equiv 0$ mod 9, which is a modular unit on $X(9)$. To see that F is indeed a modular unit, consider the fact that the divisor of each of $g_{(a_r,b_r)}$ is supported at the cusps. Hence so is for their products. Moreover,the above theorem

tells us that $\prod_r \mathfrak{k}_{(a_r,b_r)}^{m(r)}$ is of level $\Gamma(9)$ and since Δ is of level $\Gamma(9)$, it follows that so is F.

The next task is to find the set (a_r, b_r) and corresponding $m(r) \in \mathbb{Z}$ that satisfy the quadratic relations. Elkies chooses one of the three orbits of the action of G on the cusps of $X(9)$ and takes $\{(a_r, b_r)\}$ corresponding to the 12 cusps in the orbit. Moreover, this choice with $m(r) = 1$ for any r, indeed satisfies the quadratic relations. In addition, we have that $g_{(-a_r,-b_r)}$ and $g_{(a'_r,b'_r)}$ are scalar multiples of $g_{(a_r,b_r)}$, where $(a'_r, b'_r) \equiv (a_r, b_r) \bmod 9$. Since the action of G on (a_r, b_r) corresponding to the 12 cusps just permutes the elements, we have that the divisor of F is invariant under G.

To check that F actually defines a function on $X(9)/G$, we need to check that F is in fact G invariant, i.e. $F(g\tau) = F(\tau)$, for all $g \in G, \tau \in X(9)$. Since $X(9)/G$ is of genus 0 and its function field is generated by a single transcendental function, we may as well pick F as this element. Hence there exists a homomorphism $\chi : G \to \mathbb{C}^*$ such that $F(g\tau) = \chi(g)F(\tau)$, for any $g \in G, \tau \in X(9)$. Then Elkies claims that χ is trivial. To see this, take $g = \tilde{T}$, a 3-cycle in G and suppose $\chi(\tilde{T}) = 1$. Then we have that $(\tilde{S}\tilde{T})^3 = 1$ implies $(\tilde{S}\tilde{T})^2 = \tilde{T}^{-1}\tilde{S}^{-1}$. So $\chi((\tilde{S}\tilde{T})^2) = \chi(\tilde{S}\tilde{T}\tilde{S}\tilde{T}) = \chi(\tilde{S})^2\chi(\tilde{T})^2 = \chi(\tilde{S})^2$. But since $(\tilde{S}\tilde{T})^2 = \tilde{T}^{-1}\tilde{S}^{-1}$, this equals $\chi(\tilde{T}^{-1}\tilde{S}^{-1}) = \chi(\tilde{T})^{-1}\chi(\tilde{S})^{-1} = \chi(\tilde{S})^{-1}$ and therefore $\chi(\tilde{S})^3 = 1 = \chi(\tilde{S}^3)$. However we know that $\tilde{S}^4 = I$ and thus $\chi(\tilde{S}^4) = 1 = \chi(\tilde{S}^3)\chi(\tilde{S}) = \chi(\tilde{S})$. We conclude that $\chi(\tilde{S}) = 1$. If χ is not trivial, choose an element τ in the preimage of a fixed point on $X(9)$ of $\tilde{T}$. Then since $\chi(\tilde{T}) \neq 1$ and $F(\tilde{T} \cdot \tau) = \chi(\tilde{T})F(\tau) = F(\tau)$, we have that $F(\tau) = 0$, which contradicts the fact that the divisor of F is supported at the cusps. As a result, χ is trivial and $F(g \cdot \tau) = F(\tau)$, i.e. F is a function on $X(9)/G$.

To take into account the fact that the description of the cusps of $X(9)$ that we have, live in $(\mathbb{Z}/9\mathbb{Z})^2$, we let $q_9 := e^{\frac{2\pi i\tau}{9}}$ to be the local parameter and normalize F by setting $q_z := \zeta^b q_9^a$ (where $\zeta = e^{\frac{2\pi i}{9}}$). Hence $q_\tau^n = q_9^{9n}$ and the term having the Bernoulli polynomial as an index now equals $q_\tau^{\frac{1}{2}} B_2(\frac{a}{9}) = q_9^{\frac{9}{2}(\frac{a^2}{9^2} - \frac{a}{9} + \frac{1}{6})} = q_9^{\frac{1}{2}(\frac{a^2}{9} - a + \frac{9}{6})}$. Putting $\alpha = \frac{1}{2}(\frac{a^2}{9} - a + \frac{9}{6})$ (notice the misprint in [Elkies], p.4, paragraph 1, line 3), we have that

$$g_{(a,b)}(\tau) = q_9^\alpha (1 - \zeta^b q_9^a) \prod_{n=1}^{\infty} (1 - \zeta^b q_9^{9n+a})(1 - \zeta^{-b} q_9^{9n-a})$$

(in [Elkies], p.4, paragraph 1, line 2, this is the function denoted by $s(a, b)$).

We now move on to compute the q_9-expansions of F about the 3 cusps $\infty, 0, 1$ of $X(9)/G$ (denoted by F_∞, F_0, F_1 respectively). This computation can be found

in Appendix - section 6.1, code 6 (lines 1-13). The results are the following:

$$F_\infty = q^{-1} - 1 + c_2 q + c_4 q^2 + (c_1 + 2)q^3 + c_2 q^4 + O(q^5)$$

$$F_0 = q + c_1 q^2 + 2q^3 + (c_1 - c_4 + 1)q^4 + (c_1 - c_4 + 2)q^5 + (-2c_4 + 1)q^6 + O(q^7)$$

$$F_1 = 1 + (-c_1 + 1)q + (-c_1 + 1)q^2 - c_2 q^3 + (c_1 + 2(c_2 - 1))q^4 + (c_1 + 2c_2 - 1)q^5 + O(q^6)$$

We notice that our result differs from the q_9 expansion of F at ∞ in [Elkies] up to an automorphism $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ whose orbit on the triples c_1, c_2, c_4 (where $c_i := \zeta^i + \zeta^{-i}$) is given by $c_1 \mapsto c_4$, $c_2 \mapsto c_1$, $c_4 \mapsto c_2$. We would then like to find the fractional linear transformations sending F_∞ to F_0 and F_1 and consequently read the values of F_∞ at the two other cusps. So we write $\frac{wF_\infty + x}{yF_\infty + z}$ for this transformation and compute the values of w, x, y, z when the fractional linear transformation equals F_0 and F_1. The computation (in Appendix - section 6.1, code 6 (lines 14-34)) returns $F_0 = \frac{c_4}{c_4 F_\infty + 1}$ and $F_1 = \frac{F_\infty + 1 - c_1}{F_\infty}$. In particular, we see that the value of F at the cusp 0 is $\frac{-1}{c_4} = c_1 - 1$ and at the cusp 1 is 0 (and of course at the cusp ∞, the value of F is ∞). These values also indicate that F is not a $\mathbb{Q}$-rational function on $X(9)/G$.

4.8 A rational structure of $X(9)/G$

As pointed out in sections 4.5 and 4.7, the rational function $F : X(9)/G \xrightarrow{\sim} \mathbb{P}^1_{\mathbb{C}}$ has coefficients in $K = \mathbb{Q}(\zeta + \zeta^{-1})$. However, we are interested in an isomorphism $X(9)/G \xrightarrow{\sim} \mathbb{P}^1_{\mathbb{C}}$ over $\mathbb{Q}$. To solve this, we need to find a fractional linear transformation A of $\mathbb{P}^1_{\mathbb{C}}$ with coefficients in K, for which $x = A \circ F$ will be an automorphism of $\mathbb{P}^1_{\mathbb{C}}$ changing the $\mathbb{Q}$-structure such that $j : X(1) \xrightarrow{\sim} \mathbb{P}^1_{\mathbb{C}}$ is now rational in the variable x. To summarize, we need the following commutative diagram:

$$\begin{array}{ccccc}
\mathbb{H}^* & & & & \\
\downarrow & & & & \\
\bar{\Gamma}_G \setminus \mathbb{H}^* & \xrightarrow[F]{\cong} & \mathbb{P}^1_{\mathbb{C}} & \xrightarrow[A]{\cong} & \mathbb{P}^1_{\mathbb{C}} \\
\downarrow & & & & \downarrow f \\
\mathrm{PSL}_2(\mathbb{Z}) \setminus \mathbb{H}^* & & \xrightarrow[j]{\cong} & & \mathbb{P}^1_{\mathbb{C}}
\end{array}$$

If we regard j as a rational function of F, then it follows that j must have its poles at the values of F at the cusps, each with multiplicity 9 since the q_9 expansion of j looks like $j = q_9^{-9} + 744 + 196884q_9^9 + ...$ (see Appendix - section 6.1, code 6 (lines 35-41)). Thus j as a rational function of F looks like

$$j(F) = \frac{g(F)}{F^9(F-(c_1-1))^9}.$$

As a result, we now need to find $g(F)$. We do that by computing the q_9 expansion at ∞ of $g = F^9(F-(c_1-1))^9 j$ and then find how does $g(F)$ looks like by comparing the q_9 expansions of $g = \sum_{n=-27}^{\infty} c_n q_9^n$ and $b_0 + b_1 F_\infty + ... + b_{27}F_\infty^{27}$. Observe here that we stop at the coefficient of F_∞^{27}, since the local index of $g(F)$ equals $g(F)^{-1}(\infty) = 3 \cdot 9 = 27$. The above expression gives a system of equations

$$\begin{aligned}
b_{0,0} + b_{1,0}a_{-27}(F_\infty) + ... + b_{27,0}a_{-27}(F_\infty^{27}) &= c_{-27} \\
b_{0,1} + b_{1,1}a_{-26}(F_\infty) + ... + b_{27,1}a_{-26}(F_\infty^{27}) &= c_{-26} \\
\vdots & \vdots \\
b_{0,27} + b_{1,27}a_0(F_\infty) + ... + b_{27,27}a_0(F_\infty^{27}) &= c_0
\end{aligned}$$

(where $a_k(F_\infty^i)$ denotes the k-th coefficient of F_∞^i for some integer i). Solving this system for the unknowns $b_0, ..., b_{27}$ (see Appendix - section 6.1, code 6 (lines 42-45)) we find that $g(F) = b_0 + b_1F_\infty + ... + b_{27}F_\infty^{27}$ is a polynomial in F of degree 27 over the field K. So writing $j(F) = \frac{g(F)}{F^9(F-(c_1-1))^9}$ we have a rational function of degree 27 in F that is defined over K.

The last step is to find the linear fractional transformation $A : \mathbb{P}^1_{\mathbb{C}} \to \mathbb{P}^1_{\mathbb{C}}$. As pointed out, F takes the values ∞, $c_1 - 1$ and 0 at the cusps ∞, 0 and 1. Thus we would like A to send these values to the triple c_1, c_2, c_4 which is a $\mathrm{Gal}(K/\mathbb{Q})$-orbit in K. To summarize, we want the following:

$$\begin{array}{ccccc}
\text{Cusps of } X(9)/G & & \mathbb{P}^1_{\mathbb{C}} & & \mathbb{P}^1_{\mathbb{C}} \\
& \overset{F}{\mapsto} & & \overset{A}{\mapsto} & \\
\{\infty, 0, 1\} & & \{\infty, 0, c_1 - 1\} & & \{c_1, c_2, c_4\}
\end{array}$$

mapped in such a way such that the composite $A \circ F$ is $\mathrm{Gal}(K/\mathbb{Q})$-equivariant.

We choose the map

$$A: \begin{array}{rcl} \infty & \mapsto & c_1 \\ 0 & \mapsto & c_4 \\ c_1 - 1 & \mapsto & c_2 \end{array}$$

To compute A, we write $A(s) = \frac{ws+x}{ys+z} = \frac{w+\frac{x}{s}}{y+\frac{z}{s}}$. We want $A(0) = c_4$, $A(\infty) = c_1$ and $A(c_1 - 1) = c_2$, which give the following equations:

$$\frac{x}{z} = c_4 \Rightarrow x - c_4 z = 0 \tag{4.1}$$

$$\frac{w}{y} = c_1 \Rightarrow w - c_1 y = 0 \tag{4.2}$$

$$\frac{w(c_1-1)+x}{y(c_1-1)+z} = c_2 \Rightarrow w(c_1-1) + x - c_2(c_1-1)y - c_2 z = 0 \tag{4.3}$$

In a - section 6.1, code 6 (lines 46-55), we compute that

$$A = \frac{(-\zeta^5 - \zeta^2 + \zeta)t + \zeta^5 + \zeta^2 - \zeta + 1}{t + 2\zeta^5 - \zeta^4 + 3\zeta^2 - 3\zeta + 3} = \frac{c_1 t + 1 - c_1}{t - 2c_1 + c_2 + 3}.$$

We are now in a very strong position, since we may compose $\frac{g(t)}{t^9(t-(c_1-1))^9} : \mathbb{P}^1_{\mathbb{C}} \to \mathbb{P}^1_{\mathbb{C}}$ with the inverse automorphism $A^{-1} : \mathbb{P}^1_{\mathbb{C}} \to \mathbb{P}^1_{\mathbb{C}}$ and get the function

$$f := \frac{g(t)}{t^9(t-(c_1-1))^9} \circ A^{-1} : \mathbb{P}^1_{\mathbb{C}} \to \mathbb{P}^1_{\mathbb{C}}.$$

Then f as a function of $x := A \circ F$ equals to $\frac{g(t)}{t^9(t-(c_1-1))^9} \circ A^{-1}(A(F)) = \frac{g(F)}{F^9(F-(c_1-1))^9} = j(F)$ and indeed f is defined over $\mathbb{Q}$. We compute this explicitly in Appendix - section 6.1, code 6 (lines 56-57);

$$f(x) = \frac{-3^7 \cdot 5 \cdot 2^{12}(x-2)^3 x^3 (x^3 - \frac{12}{5}x^2 + \frac{6}{5}x - \frac{1}{5})(x^6 - \frac{21}{4}x^5 + \frac{177}{16}x^4 - \frac{187}{16}x^3 + \frac{105}{16}x^2 - \frac{15}{8}x + \frac{1}{4})^3}{(x^3 - 3x + 1)^9}.$$

4.9 The universal elliptic curve and an alternative approach

As we saw in section 4.8 the function $f(x) : X(9)/G \cong \mathbb{P}^1_{\mathbb{C}} \to \mathbb{P}^1_{\mathbb{C}}$ is $\mathbb{Q}$-rational and is equal to the j-function applied to the projection map $X(9)/G \to X(1)$. Hence we can write down explicitly the equations of the elliptic curves over $\mathbb{Q}$ parametrized by $X(9)/G$ using the **universal elliptic curve**:

$$E_{f(x)} : y^2 = 4z^3 - \frac{27f(x)}{f(x)-1728}z - \frac{27f(x)}{f(x)-1728}.$$

This elliptic curve has j-invariant equal to $f(x)$. So if we restrict $f(x) : \mathbb{P}^1_{\mathbb{Q}} \to \mathbb{P}^1_{\mathbb{Q}}$, then we get that the elliptic curve $E_{f(x)}$ is defined over $\mathbb{Q}$. Moreover, any elliptic curve $E/\mathbb{Q}$ that has $\rho_{3,E}$ surjective mod 3 and not mod 9 is isomorphic to an elliptic curve of the form $E_{f(x)}$ for some $x \in \mathbb{P}^1_{\mathbb{Q}}$.

So we now have an explicit description of the elliptic curves over $\mathbb{Q}$ satisfying the above condition. However, given an elliptic curve $E/\mathbb{Q}$, how can one decide whether $\rho_{3,E}$ is surjective mod 3 and not mod 9? The first thing we could do is to compute its j-invariant and check whether this value lies in the image of the function $f(x)$, for some $x \in \mathbb{P}^1_{\mathbb{Q}}$. However, this is a hard task since $f(x)$ is a rational function in x of degree 27. Elkies in his paper determines all non-zero integral values of $f(x)$ (that we also obtain in Appendix - section 6.1, code 6 (line 58) for different values of x since Elkies uses a different set of representatives for the cusps of $X(9)/G$ when he writes down the function $f(x)$). In fact, he proves that the following table contains all of the integral values of $f(x)$: (In this table we denote by a vector $[a_1, a_2, a_3, a_4, a_6]$ the elliptic curve $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ and N_E its conductor)

x	$j = f(x)$	E	N_E
∞	4374	$[0,0,0,-27-42]$	$2^3 3^5$
-2	419904	$[0,0,0,-162,792]$	$2^8 3^5$
0	-44789760	$[0,0,1,-135,-604]$	$3^5 5^2$
$\frac{-1}{2}$	15786448344	$[0,0,0,-5427,153882]$	$2^5 3^5$
2	24992518538304	$[0,0,0,-201042,34695912]$	$2^8 3^5 17^2$
$\frac{-3}{2}$	-92515041526500	$[0,0,0,-1126035,459913278]$	$2^3 3^5 19^2$
$\frac{-1}{3}$	-70043919611288518656	$[0,0,1,-1127379978,-14569799990728]$	$3^5 97^2 101^2$

An alternative approach to this question comes from the fact that at primes $p \nmid 3N_E$, $\text{tr}\ \rho_{3,E}(\text{Frob}_p) = a_p(E)$ and $\det \rho_{3,E}(\text{Frob}_p) = p$ (see Theorem 3.9) and the following result:

Theorem 4.9 ***Jordan's theorem:*** *Suppose A is a finite group and B a subgroup of A such that every element of A is conjugate to an element of B. Then $B = A$.*

Proof: Since every element of A is conjugate to an element of B, we can write $A = \cup_{g \in A} g^{-1}Bg$. In fact, since the action of conjugation is a group automorphism, we can do even better and write $A = \cup_{g \in B\backslash A} g^{-1}Bg$, for g now being a coset of $B\backslash A$. But then we have that $|g^{-1}Bg| = |B|$ and hence $|A| = |B\backslash A||g^{-1}Bg|$. However, the sets $\{g^{-1}Bg\}_{g \in B\backslash A}$ have non-empty intersection because they all contain the identity element. Thus the only way the above equation can hold is when $|B\backslash A| = 1$ and $B = A$. □

So to test whether a subgroup A is contained in the image of $\bar{\rho}_{3,E}$, it suffices to compute the traces of all the elements of A (denote this set by tr_A) and check whether $\text{tr}\ \rho_{3,E}(\text{Frob}_p)$ mod 9 surjects on tr_A for different primes $p \nmid 3N_E$ such that $\bar{\rho}_{3,E}(\text{Frob}_p)$ mod 9 is an element of A (where in the case of $A = \text{SL}_2(\mathbb{Z}/9\mathbb{Z})$, $\det \rho_{3,E}(\text{Frob}_p) \equiv 1 \bmod 9$). If it does, then since every element of A is conjugate to an element with trace in the set tr_A, we can conclude using the above theorem that $\bar{\rho}_{3,E}$ mod 9 surjects on A. Of course this does not account for an effective algorithm since we cannot prove that it terminates at a certain prime.

Chapter 5

Conclusion

In this essay we have been successful with the objective been set at the beginning; that is to give a clear exposition of the densely written paper of Elkies [Elkies], expanding on the major tools being used. One of the main reasons this paper has driven the need to do as such, is a possible error in the function

$$f(x) = -\frac{3^7(x^2-1)^3(x^6+3x^5+6x^4+x^3-3x^2+12x+16)^3(2x^3+3x^2-3x-5)}{(x^3-3x-1)^9}.$$

Due to the nature of this paper, spotting where a possible error has occurred was quite not possible. Hence we decided to recalculate everything step by step from the beginning and give a new equation of $f(x)$, that is

$$f(x) = \frac{-3^7 \cdot 5 \cdot 2^{12}(x-2)^3x^3(x^3-\frac{12}{5}x^2+\frac{6}{5}x-\frac{1}{5})(x^6-\frac{21}{4}x^5+\frac{177}{16}x^4-\frac{187}{16}x^3+\frac{105}{16}x^2-\frac{15}{8}x+\frac{1}{4})^3}{(x^3-3x+1)^9}.$$

As a result, even in the case where we have performed an error in our calculations, spotting the error is now a much easier task.

It has been mentioned in chapter 1 that the case of the surjectivity of 2-adic Galois representations attached to elliptic curves over $\mathbb{Q}$, has been studied in the paper [Dokchitser]. However, the methods being used there are quite different from Elkies' methods; in particular the theory of modular curves is not being used at all and no explicit parametrization via the j-invariant exists. As a result, a natural development of this essay would be to use Elkies' methods and modular curves to find an explicit parametrization of elliptic curves over $\mathbb{Q}$ that satisfy $\bar{\rho}_{2,E}$ surjective mod 2 and not mod 4, or even the case where $\bar{\rho}_{2,E}$ is surjective mod 4 and not mod 8. This would involve finding maximal proper subgroups (call such a subgroup G) of $\mathrm{SL}_2(\mathbb{Z}/4\mathbb{Z})$ that surject on $\mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z})$ (or maximal subgroups of $\mathrm{SL}_2(\mathbb{Z}/8\mathbb{Z})$ that

surject on $\mathrm{SL}_2(\mathbb{Z}/4\mathbb{Z})$) and investigating the modular curve $X(2)/G$. Essentially this would require easier calculations than the $X(9)/G$ case, however one could run into several problems such as the group G not being unique up to conjugacy (in which case one would need to consider the modular curves $X(2)/G$ for any such G up to conjugacy) or even that $X(2)/G$ may not have a model over $\mathbb{Q}$. It is however a fun problem that due to lack of time we did not include in this dissertation.

Another possible development of this essay would have been to investigate the surjectivity of Galois representations attached to elliptic curves over number fields. This is however, a much harder problem (see for example [Greicius])

Chapter 6

Appendix

6.1 Code

In this section we give the code we have used for computations on a computer. The computer programs used are namely SAGE, MAGMA and GAP.

1.
```
// This code written in SAGE computes the first 50 terms of
// the q-expansion of the basis vector of the 1-dimensional
// space of cusp forms S_2(Γ_0(11))

S = CuspForms(Gamma0(11),2); S;
Cuspidal subspace of dimension 1 of Modular Forms space of dimension
2 for Congruence Subgroup Gamma0(11) of weight 2 over Rational Field

f=S.basis()[0];

f.q_expansion(50);
q - 2*q^2 - q^3 + 2*q^4 + q^5 + 2*q^6 - 2*q^7 - 2*q^9 - 2*q^10 + q^11
- 2*q^12 + 4*q^13 + 4*q^14 - q^15 - 4*q^16 - 2*q^17 + 4*q^18 + 2*q^20
+ 2*q^21 - 2*q^22 - q^23 - 4*q^25 - 8*q^26 + 5*q^27 - 4*q^28 + 2*q^30
+ 7*q^31 + 8*q^32 - q^33 + 4*q^34 - 2*q^35 - 4*q^36 + 3*q^37 - 4*q^39
- 8*q^41 - 4*q^42 - 6*q^43 + 2*q^44 - 2*q^45 + 2*q^46 + 8*q^47 + 4*q^48
- 3*q^49 + O(q^50)
```

2.
```
// This code written in SAGE computes the trace of the
// Frobenius of the elliptic curve E/Q : y^2 + y = x^3 - x^2 - 10x - 20
// of conductor 11 at primes up to 50
```

```
// Access Cremona's database of elliptic curves with conductor
// up to 10000 using the variable c
c = CremonaDatabase(); c;
Cremona's database of elliptic curves

// List all elliptic curves in the database of conductor 11
c.allcurves(11);
{'a1': [[0, -1, 1, -10, -20], 0, 5], 'a3': [[0, -1, 1, 0, 0], 0,
5], 'a2': [[0, -1, 1, -7820, -263580], 0, 1]}

// List all primes up to 50 and assign to the variable a
n=1; a=[];
while n<50 :
if (n in Primes()) :
a.append(n); n=n+1; a;
[2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47]

// Compute the trace of the Frobenius of the elliptic curve
// 'a1': [0, -1, 1, -10, -20] of conductor 11 at each prime
// in the list a
b=[]; i=0; n=a[0];
for n in a :
n=a[i] ;
if (n <> 3) & (n <> 11):
E = EllipticCurve(GF(n), [0, -1, 1, -10, -20]) ;
t = E.trace_of_frobenius(); b.append(t % 9) ;
i=i+1 ;
b ;
[7, 1, 7, 4, 7, 0, 8, 0, 7, 3, 1, 3, 8]
```

3.
```
// This code written in GAP computes the maximal subgroups
// of SL_2(Z/9Z), their orders,
// as well as the order of their image in SL_2(Z/3Z)

// Assign to the variable A the group SL_2(Z/9Z)
A:= SL(2,ZmodnZ(9));
SL(2,Z/9Z)
```

```
// Compute the conjugacy classes of
// the maximal subgroups of A
ConjugacyClassesMaximalSubgroups( A );
[ Group([ [ [ ZmodnZObj( 7, 9 ), ZmodnZObj( 4, 9 ) ],
[ ZmodnZObj( 1, 9), ZmodnZObj( 2, 9 ) ] ],
[ [ ZmodnZObj( 3, 9 ), ZmodnZObj( 8, 9 ) ],
[ ZmodnZObj( 1, 9), ZmodnZObj( 6, 9 ) ] ],
[ [ ZmodnZObj( 8, 9 ), ZmodnZObj( 0, 9 ) ],
[ ZmodnZObj( 0, 9 ), ZmodnZObj( 8, 9 ) ] ],
[ [ ZmodnZObj( 7, 9 ), ZmodnZObj( 3, 9 ) ],
[ ZmodnZObj( 3, 9 ), ZmodnZObj( 4, 9 ) ] ],
[ [ ZmodnZObj( 1, 9 ), ZmodnZObj( 6, 9 ) ],
[ ZmodnZObj( 3, 9 ), ZmodnZObj( 1, 9 ) ] ],
[ [ ZmodnZObj( 4, 9 ), ZmodnZObj( 3, 9 ) ],
[ ZmodnZObj( 3, 9 ), ZmodnZObj( 7, 9 ) ] ] ])^G,
Group([ [ [ ZmodnZObj( 7, 9 ), ZmodnZObj( 7, 9 ) ],
[ ZmodnZObj( 6, 9 ), ZmodnZObj( 1, 9 ) ] ],
[ [ ZmodnZObj( 8, 9 ), ZmodnZObj( 0, 9 ) ],
[ ZmodnZObj( 0, 9 ), ZmodnZObj( 8, 9 ) ] ],
[ [ ZmodnZObj( 7, 9 ), ZmodnZObj( 3, 9 ) ],
[ ZmodnZObj( 3, 9 ), ZmodnZObj( 4, 9 ) ] ],
[ [ ZmodnZObj( 1, 9 ), ZmodnZObj( 6, 9 ) ],
[ ZmodnZObj( 3, 9 ), ZmodnZObj( 1, 9 ) ] ],
[ [ ZmodnZObj( 4, 9 ), ZmodnZObj( 3, 9 ) ],
[ ZmodnZObj( 3, 9 ), ZmodnZObj( 7, 9 ) ] ] ])^G,
Group([ [ [ ZmodnZObj( 7, 9 ), ZmodnZObj( 7, 9 ) ],
[ ZmodnZObj( 6, 9 ), ZmodnZObj( 1, 9 ) ] ],
[ [ ZmodnZObj( 7, 9 ), ZmodnZObj( 4, 9 ) ],
[ ZmodnZObj( 1, 9 ), ZmodnZObj( 2, 9 ) ] ],
[ [ ZmodnZObj( 3, 9 ), ZmodnZObj( 8, 9 ) ],
[ ZmodnZObj( 1, 9 ), ZmodnZObj( 6, 9 ) ] ],
[ [ ZmodnZObj( 8, 9 ), ZmodnZObj( 0, 9 ) ],
[ ZmodnZObj( 0, 9 ), ZmodnZObj( 8, 9 ) ] ] ])^G ]

// Assign to variables G1, G2, G3 the first, second and third
// conjugacy class of maximal subgroup of A
```

```
G1:= Group( [ [ [ ZmodnZObj( 7, 9 ), ZmodnZObj( 4, 9 ) ],
[ ZmodnZObj( 1, 9 ), ZmodnZObj( 2, 9 ) ] ],
[ [ ZmodnZObj( 3, 9 ), ZmodnZObj( 8, 9 ) ],
[ ZmodnZObj( 1, 9 ), ZmodnZObj( 6, 9 ) ] ],
[ [ ZmodnZObj( 8, 9 ), ZmodnZObj( 0, 9 ) ],
[ ZmodnZObj( 0, 9 ), ZmodnZObj( 8, 9 ) ] ],
[ [ ZmodnZObj( 7, 9 ), ZmodnZObj( 3, 9 ) ],
[ ZmodnZObj( 3, 9 ), ZmodnZObj( 4, 9 ) ] ],
[ [ ZmodnZObj( 1, 9 ), ZmodnZObj( 6, 9 ) ],
[ ZmodnZObj( 3, 9 ), ZmodnZObj( 1, 9 ) ] ],
[ [ ZmodnZObj( 4, 9 ), ZmodnZObj( 3, 9 ) ],
[ ZmodnZObj( 3, 9 ), ZmodnZObj( 7, 9 ) ] ] ]);

G2:= Group([ [ [ ZmodnZObj( 7, 9 ), ZmodnZObj( 7, 9 ) ],
[ ZmodnZObj( 6, 9 ), ZmodnZObj( 1, 9 ) ] ],
[ [ ZmodnZObj( 8, 9 ), ZmodnZObj( 0, 9 ) ],
[ ZmodnZObj( 0, 9 ), ZmodnZObj( 8, 9 ) ] ],
[ [ ZmodnZObj( 7, 9 ), ZmodnZObj( 3, 9 ) ],
[ ZmodnZObj( 3, 9 ), ZmodnZObj( 4, 9 ) ] ],
[ [ ZmodnZObj( 1, 9 ), ZmodnZObj( 6, 9 ) ],
[ ZmodnZObj( 3, 9 ), ZmodnZObj( 1, 9 ) ] ],
[ [ ZmodnZObj( 4, 9 ), ZmodnZObj( 3, 9 ) ],
[ ZmodnZObj( 3, 9 ), ZmodnZObj( 7, 9 ) ] ] ]);

G3:= Group([ [ [ ZmodnZObj( 7, 9 ), ZmodnZObj( 7, 9 ) ],
[ ZmodnZObj( 6, 9 ), ZmodnZObj( 1, 9 ) ] ],
[ [ ZmodnZObj( 7, 9 ), ZmodnZObj( 4, 9 ) ],
[ ZmodnZObj( 1, 9 ), ZmodnZObj( 2, 9 ) ] ],
[ [ ZmodnZObj( 3, 9 ), ZmodnZObj( 8, 9 ) ],
[ ZmodnZObj( 1, 9 ), ZmodnZObj( 6, 9 ) ] ],
[ [ ZmodnZObj( 8, 9 ), ZmodnZObj( 0, 9 ) ],
[ ZmodnZObj( 0, 9 ), ZmodnZObj( 8, 9 ) ] ] ]);

// Compute the order of G1, G2, G3
Order(G1);
216
```

```
Order(G2);
162

Order(G3);
24

// Assign to the variable B the group SL_2(Z/3Z)
B:= SL(2,ZmodnZ(3));
SL(2,3)

// Assign to the variables H1, H2, H3 the images of the groups
// G1, G2, G3 in SL_2(Z/3Z)
H1:= Subgroup(B,[[[ ZmodnZObj( 1, 3 ), ZmodnZObj( 1, 3 ) ],
[ ZmodnZObj( 1, 3 ), ZmodnZObj( -1, 3 ) ] ],
[ [ ZmodnZObj( 0, 3 ), ZmodnZObj( -1, 3 ) ],
[ ZmodnZObj( 1, 3 ), ZmodnZObj( 0, 3 ) ] ],
[ [ ZmodnZObj( -1, 3 ), ZmodnZObj( 0, 3 ) ],
[ ZmodnZObj( 0, 3 ), ZmodnZObj( -1, 3 ) ] ],
[ [ ZmodnZObj( 1, 3 ), ZmodnZObj( 0, 3 ) ],
[ ZmodnZObj( 0, 3 ), ZmodnZObj( 1, 3 ) ]]] );

H2:= Subgroup(B,[[[ ZmodnZObj( 1, 3 ), ZmodnZObj( 1, 3 ) ],
[ ZmodnZObj( 0, 3 ), ZmodnZObj( 1, 3 ) ] ],
[ [ ZmodnZObj( -1, 3 ), ZmodnZObj( 0, 3 ) ],
[ ZmodnZObj( 0, 3 ), ZmodnZObj( -1, 3 ) ] ],
[ [ ZmodnZObj( 1, 3 ), ZmodnZObj( 0, 3 ) ],
[ ZmodnZObj( 0, 3 ), ZmodnZObj( 1, 3 ) ]]] );

H3:= Subgroup(B,[[[ ZmodnZObj( 1, 3 ), ZmodnZObj( 1, 3 ) ],
[ ZmodnZObj( 0, 3 ), ZmodnZObj( 1, 3 ) ] ],
[ [ ZmodnZObj( 1, 3 ), ZmodnZObj( 1, 3 ) ],
[ ZmodnZObj( 1, 3 ), ZmodnZObj( -1, 3 ) ] ],
[ [ ZmodnZObj( 0, 3 ), ZmodnZObj( -1, 3 ) ],
[ ZmodnZObj( 1, 3 ), ZmodnZObj( 0, 3 ) ] ],
[ [ ZmodnZObj( -1, 3 ), ZmodnZObj( 0, 3 ) ],
[ ZmodnZObj( 0, 3 ), ZmodnZObj( -1, 3 ) ]]] );
```

```
// Compute the order of the groups H1, H2, H3
Order(H1);
8

Order(H2);
6

Order(H3);
24
```

4. // This code written in GAP constructs the group G'
   // and lists its elements of the form $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$

```
// Assign to the variable A the group GL_2(Z/9Z)
A:=GL(2, ZmodnZ(9));
GL(2,Z/9Z)

// Construct the group G'
G':= Subgroup(A, [ [ [ ZmodnZObj( 0, 9 ), ZmodnZObj( 4, 9 ) ], [ ZmodnZObj(
2, 9 ), ZmodnZObj( 0, 9 ) ] ],
[ [ ZmodnZObj( 4, 9 ), ZmodnZObj( 1, 9 ) ],
[ ZmodnZObj( -3, 9 ), ZmodnZObj( 4, 9 ) ] ],
[ [ ZmodnZObj( 1, 9 ), ZmodnZObj( 0, 9 ) ],
[ ZmodnZObj( 0, 9 ), ZmodnZObj( 1, 9 ) ] ],
[ [ ZmodnZObj( 2, 9 ), ZmodnZObj( 0, 9 ) ],
[ ZmodnZObj( 0, 9 ), ZmodnZObj( 2, 9 ) ] ],
[ [ ZmodnZObj( 4, 9 ), ZmodnZObj( 0, 9 ) ],
[ ZmodnZObj( 0, 9 ), ZmodnZObj( 4, 9 ) ] ],
[ [ ZmodnZObj( -1, 9 ), ZmodnZObj( 0, 9 ) ],
[ ZmodnZObj( 0, 9 ), ZmodnZObj( 1, 9 ) ] ],
[ [ ZmodnZObj( -4, 9 ), ZmodnZObj( 0, 9 ) ],
[ ZmodnZObj( 0, 9 ), ZmodnZObj( 4, 9 ) ] ],
[ [ ZmodnZObj( -2, 9 ), ZmodnZObj( 0, 9 ) ],
[ ZmodnZObj( 0, 9 ), ZmodnZObj( 2, 9 ) ] ]]);
G';
<matrix group of size 144 with 8 generators>
```

```
// Return a list of elements of the form (a b; 0 1)
// in the group G'
alpha:=[]; i:=0;
while i in [0..8] do
j:=0;
while j in [0..8] do
if [ [ ZmodnZObj( i, 9 ), ZmodnZObj( j, 9 ) ], [ ZmodnZObj( 0, 9 ),
ZmodnZObj( 1, 9 ) ] ] in G' then
Add(alpha,[ [ ZmodnZObj( i, 9 ), ZmodnZObj( j, 9 ) ], [ ZmodnZObj(
0, 9 ), ZmodnZObj( 1, 9 ) ] ] ); fi;
j:= j+1 ;
od;
i:= i+1 ;
od;
alpha;
[ [ [ ZmodnZObj( 1, 9 ), ZmodnZObj( 0, 9 ) ],
[ ZmodnZObj( 0, 9 ), ZmodnZObj( 1, 9 ) ] ],
[ [ ZmodnZObj( 8, 9 ), ZmodnZObj( 0, 9 ) ],
[ ZmodnZObj( 0, 9 ), ZmodnZObj( 1, 9 ) ] ] ]
```

5.
```
// This code written in SAGE constructs the
// congruence subgroup Γ_G
// via a description of the permutations
// L=[1, 1, 0, 1] and R=[1, 0, 1, 1]
// acting by right multiplication on the set
// of cosets G \ SL_2(Z)
// and computes its projective index as well as
// the number of elliptic points of periods 2 and 3
// (Note that SAGE at the current time has no other way of
// constructing an arbitrary congruence subgroup other
// than Γ_0(N), Γ_1(N), Γ(N))

// Assign to the variable G the symmetric group on 27 letters
G = SymmetricGroup(27);

// Write L and R as permutations in G
```

```
L= G("(1,10,25,12,22,15,26,14,5) (2,4,16,18,21,27,20,9,8)
(3,7,19,17,6,13,24,23,11)"); L;
(1,10,25,12,22,15,26,14,5)(2,4,16,18,21,27,20,9,8)
(3,7,19,17,6,13,24,23,11)

R= G("(1,7,8,19,27,20,17,18,6) (2,10,22,23,15,5,16,21,9)
(3,4,13,26,14,24,11,25,12)"); R;
(1,7,8,19,27,20,17,18,6)(2,10,22,23,15,5,16,21,9)
(3,4,13,26,14,24,11,25,12)

// Construct Γ_G
GammaG= ArithmeticSubgroup_Permutation(L, R); GammaG ;
Arithmetic subgroup corresponding to permutations
L=(1,10,25,12,22,15,26,14,5)(2,4,16,18,21,27,20,9,8)
(3,7,19,17,6,13,24,23,11),
R=(1,7,8,19,27,20,17,18,6)(2,10,22,23,15,5,16,21,9)
(3,4,13,26,14,24,11,25,12)

// Test whether Γ(9) is a subgroup of Γ_G
Gamma(9).is_subgroup(GammaG) ;
True

// Compute the projective index of Γ_G
GammaG.projective_index() ;
27

// Compute the number of elliptic points of Γ_G of period 2
GammaG.nu2() ;
3

// Compute the number of elliptic points of Γ_G of period 3
GammaG.nu3() ;
3
```

6.
```
// This code written in MAGMA carries out the computations
// needed in sections 4.7 and 4.8.
// We use line numbering and reference where needed in the
// context with the appropriate line numbering
```

```
// Define the cyclotomic field K in the variable z
// by adjoining a 9-th root of unity to the rationals
1) K<z>:= CyclotomicField(9);

// Define the Laurent series ring R with coefficients in the
// field K with precision up to the term q_9^50
2) R<q>:=LaurentSeriesRing(K,50);

// Assign to the variable alpha the function in the
// variable a that computes the Bernoulli polynomial (1/2)B_2(a/9)
3) alpha := func< a,b | 1/2*((a^2)/9 - a + 9/6) >;

// Assign to the variable r the function in variables a,b that
// computes the product of the first 11 terms in the infinite
// product of the function g_{a,b}(τ) ommiting the first term q_9^α
4) r := func<a,b | (1-z^b*q^a)* & *[ (1-z^b*q^(9*n+a))*(1-z^(-b)*q^(9*n-a))
:  n in [1..10]] >;

// The q_9-expansion of F at the cusp infinity, F_∞
5) F1:=q^(alpha(1,0)+alpha(2,1)+alpha(3,1)+alpha(6,1)+alpha(7,1)+alpha(0,2)
+ alpha(4,3)+alpha(5,3)+alpha(2,4)+alpha(4,4)+alpha(5,4)+alpha(7,4))
*r(1,0)*r(2,1)*r(3,1)*r(6,1)*r(7,1)*r(0,2)*r(4,3)*r(5,3)*r(2,4)*r(4,4)
*r(5,4)*r(7,4);
6) F1/:= LeadingCoefficient(F1);

// The q_9-expansion of F at the cusp 0, F_0
7) F2:=q^(alpha(0,1)+alpha(4,0)+alpha(1,2)+alpha(2,2)+alpha(7,2)+alpha(8,2)
+alpha(2,3) + alpha(7,3)+alpha(1,4)+alpha(3,4)+alpha(6,4)+alpha(8,4))
*r(0,1)*r(4,0)*r(1,2)*r(2,2)*r(7,2)*r(8,2)*r(2,3)*r(7,3)*r(1,4)*r(3,4)
*r(6,4)*r(8,4);
8) F2/:= LeadingCoefficient(F2);

// The q-expansion of F at the cusp 1, F_1
9) F3:=q^(alpha(2,0)+alpha(1,1)+alpha(4,1)+alpha(5,1)+alpha(8,1)+alpha(3,2)
+alpha(4,2)+alpha(5,2)+alpha(6,2)+alpha(1,3)+alpha(8,3)+alpha(0,4))
*r(2,0)*r(1,1)*r(4,1)*r(5,1)*r(8,1)*r(3,2)*r(4,2)*r(5,2)*r(6,2)*r(1,3)
```

```
*r(8,3)*r(0,4);
10) F3/:= LeadingCoefficient(F3);

// Check that F_∞, F_0 and F_1 have coefficients in Q(ζ + ζ^{-1})
11) L<c>:=sub<K | z +1/z>;
12) RR<qq>:=LaurentSeriesRing(L,50);
13) F1 in RR; F2 in RR; F3 in RR;

// The following code is to compute the fractional linear transformations
// sending F_∞ to F_0 and F_1

// Define the function field Kwxyz of K in the variables w,x,y,z
14) Kwxyz<w,x,y,z> := FunctionField(K,4);

// Assign to RR in variable qq the
// Laurent Series over Kwxyz with precision of 4 terms
15) RR<qq> := LaurentSeriesRing(Kwxyz,4);

// Assign to the variable FF the fractional linear transformation
// in variables w,x,y,z and F_∞
// that returns the q_9 expansion of FF up to the term q_9^4
16) FF := (w * RR!F1 + x) / (y * RR!F1 + z);

// Define the function findratlin in the variable F that computes
// the values of the variables w,x,y,z when F is assigned
// to F_0 or F_1
17) findratlin := function(F)
// Define the projective space P^3_{Q(ζ_9)}
18)    P3 := ProjectiveSpace(K,3);
// List the difference of the coefficients of the function
// FF and F up to the term q_9^3
19)    coeffs := [ Coefficient(FF,i) - Coefficient(F,i) :  i in [0..3]
];
// Define the scheme in P^3_{Q(ζ_9)} that is defined as the
// zero locus of the numerators of
// the entries of the list coeffs
20)    X := Scheme(P3, [ Numerator(c) :  c in coeffs] );
```

```
// Define the scheme in P^3_{Q(ζ9)} that is defined as the
// zero locus of the denominators of
// the entries of the list coeffs
21)   Y := Scheme(P3, [ Denominator(c) :  c in coeffs] );
// Find the set-theoretic difference of the two sets X and
// Y and reassign to the variable X
22)   X := Difference(X,Y);
// Check that the scheme X is 0 dimensional
23)   assert Dimension(X) eq 0;
// Find the set of rational points of X that do not belong
// to Y and assign to the variable pts
24)   pts := { P : P in RationalPoints(X) | P notin Y };
// Check that the set pts has cardinality 1
25)   assert # pts eq 1;
// Assign to the variable P the unique element of the set pts
26)   P := Rep(pts);
// The function findratlin outputs a matrix with entries
// the coordinates of the variable P in the field Q(ζ9)
// The entries (a_{i,j}) of this matrix correspond to
// a_{1,1} = w, a_{1,2} = x, a_{2,1} = y, a_{2,2} = z
27)   return Matrix(K, [[P[1],P[2]],[P[3],P[4]]]);
28) end function;

// Evaluate the function findratlin in F_0
29) M2:=findratlin(F2); M2;

// Evaluate the function findratlin in F_1
30) M3:=findratlin(F3); M3;

// Compute the value of F at the cusp 0 and check that
// it lies in the field Q(ζ + ζ^{-1})
31) x2 := -M2[2,2]/M2[2,1];
32) x2 in L;

// Compute the value of F at the cusp 1 and check that
// it lies in the field Q(ζ + ζ^{-1})
33) x3 := -M3[2,2]/M3[2,1];
```

```
34) x2 in L;

// The following code is to compute the q_9 expansion of
// the j-function

// Compute the space of modular forms of level 1 and
// weight 4 and 6, with precision of 50 terms
35) M4:=ModularForms(1,4); SetPrecision(M4,50);
36) M6:=ModularForms(1,6); SetPrecision(M6,50);

// Compute the basis of M4 and M6 which are
// the Eisenstein series E_4 and E_6
37) E4:=Basis(M4)[1]; E6:=Basis(M6)[1];

// Define the Laurent series ring S with coefficients in the
// rationals with precision up to the term q^50
38) S<q>:=LaurentSeriesRing(Rationals(),50);

// Define the Eisenstein series E_4 and E_6 as elements of S
39) E4:= S!PowerSeries(E4); E6:= S!PowerSeries(E6);

// Compute the q-expansion of the j-function
40) j := 1728*(E4^3) / (E4^3 - E6^2);

// Compute the q_9-expansion of the j-function
41) j := Evaluate(j, q^9);

// The following code computes the function g(F)
// as a polynomial in F of degree 27 with
// coefficients in the field Q(ζ + ζ^-1)

// Define the function g which is defined over Q(ζ + ζ^-1)
42) g := (F1 - x2)^9 * (F1 - x3)^9 * j;

// Define the 28×28 matrix with entries (a_{-28+i}(F_∞)^{j-1})_{i,j} (See section
4.8)
```

```
43) M := Matrix([[ Coefficient(F1^j, i) :  i in [-27..0] ] :  j in
[0..27] ]);

// Define the 28×1 vector with entries (c_{-28+i})_{i,1} (See section 4.8)
44) v := Vector([ Coefficient(g, i) :  i in [-27..0]]);

// Solve the system Mx=v, where x is the 28 × 1 vector
// with entries (b_{i-1})_{i,1}, which are
// the coefficients of the polynomial g(F)
45) x := Solution(M,v);

// Define the function field of Q(ζ_9)
46) _ <t> := FunctionField(K);

// Assign to variable g the polynomial g(F)
47) g := & +[ x[j+1] * t^j :  j in [0..27] ];

// Define the function ff := g(t) / t^9(t-(c_1-1))^9
48) ff := g / ((t-x2)^9 * (t-x3)^9);

// This part of the code computes the
// fractional linear transformation A

// Define the cyclotomic field K in the variable z
// by adjoining a 9-th root of unity to the rationals
49) K<z> := CyclotomicField(9);

// Define the Galois orbit in Q(ζ), c_1, c_2, c_4 in the field K
50) c1 := K!(z + 1/z); c2 := K!(z^2 + 1/z^2); c4 := K!(z^4 + 1/z^4);

// Define the projective space P^3_{Q(ζ_9)} in the variables w,x,y,z
51) P3<w,x,y,z> := ProjectiveSpace(K,3);

// Define the scheme in P3<w,x,y,z> that is defined as the
// zero locus of the equations 4.1,4.2,4.3 in section 4.8
52) X := Scheme(P3, [x - c4*z, w - c1*y, w*(c1-1)+x-c2*(c1-1)*y-c2*z
]);
```

```
// Check that X has dimension 0
53) assert Dimension(X) eq 0;

// Assign to P=(w,x,y,z) the unique rational point of X
54) P := Rep(RationalPoints(X));

// Compute the function A
55) A:= (P[1]*t+P[2])/(P[3]*t+P[4]);

// Compute A^-1
56) A_inverse := (P[4]*t - P[2]) / (-P[3]*t + P[1]);

// Compute the function f := ff o A^-1 and
// assign it to the variable f
57) f := Evaluate(ff,A_inverse); f;

// Compute the integral values of f(x)
// for values of x = a/b such that
// a in {-20,...,20}, b in {1,...,20}
58) { j :  a in [-20..20], b in [1..20] | Denominator(j) eq 1 where
j is Evaluate(ff,a/b) };
```

6.2 The reduction map $\mathbf{SL}_2(\mathbb{Z}) \to \mathbf{SL}_2(\mathbb{Z}/N\mathbb{Z})$ is surjective

Lemma 6.1 *The reduction mod N map $SL_2(\mathbb{Z}) \to SL_2(\mathbb{Z}/N\mathbb{Z})$ is surjective.*

Proof: Let $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. Then $ad - bc \equiv 1 \bmod N$ and if $fc = fd \equiv 0 \bmod N$ for some $f \in \mathbb{Z}/N\mathbb{Z}$, then $f(ad-bc) = f \equiv 0 \bmod N$. Hence c, d are coprime mod N. Next we show that the pair (c, d) has a lift $(c_0, d_0) \in \mathbb{Z}^2$ such that c_0, d_0 are coprime. Take an arbitrary lift c_1 of c_0 and d_0 in $\mathbb{Z}$. Without loss of generality we may assume that $d_0 \neq 0$ (by adding a multiple of N). If p is a prime dividing d_0 then p does not divide both c_1 and N since otherwise c, d would not be coprime mod N (just take $f = \frac{N}{p}$ in previous argument which gives $f \not\equiv 0 \bmod N$).

Define $c_p := c_1 + t_p N$, where $t_p := \begin{cases} 0, & \text{if } p \nmid c_1 \\ 1, & \text{otherwise} \end{cases}$

Then p does not divide c_p and by the Chinese remainder theorem we can find a $t \in \mathbb{Z}$ such that $t \equiv t_p \bmod p$, for every prime p dividing d_0. Put $c_0 := c + tN$. Then (c_0, d_0) is a coprime pair in $\mathbb{Z}^2$ that reduces to (c, d) mod N.

We can now consider the matrix $\begin{pmatrix} a + xN & b + yN \\ c_0 & d_0 \end{pmatrix}$, where $x, y \in \mathbb{Z}$ are chosen as follows; the determinant of this matrix equals $(ad_0 - bc_0) + N(xd_0 - yc_0)$. Since c_0, d_0 are coprime, we can find integers x_0, y_0 such that $x_0 d_0 - y_0 c_0 = 1$ and $N(x_0 d_0 - y_0 c_0) = N$. But $ad_0 - bc_0 \equiv 1 \bmod N$ and thus $ad_0 - bc_0 = 1 + wN$ for some $w \in \mathbb{Z}$. However, $wN = N(wx_0 d_0 - wy_0 c_0)$ and letting $x := wx_0$, $y := wy_0$, we have that $(ad_0 - bc_0) + N(xd_0 - yc_0) = 1 + wN - wN = 1$. So the matrix $\begin{pmatrix} a + xN & b + yN \\ c_0 & d_0 \end{pmatrix}$ lives in $\mathrm{SL}_2(\mathbb{Z})$ and reduces to $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. $\square$

Bibliography

[B C D T] Christophe Breuil, Brian Conrad, Fred Diamond and Richard Taylor. On the modularity of elliptic curves over **Q**: wild 3-adic exercises. J. Amer. Math. Soc. **14** (2001), no. 4, 843–939 (electronic).

[Dia & Shur] F. Diamond & J. Shurman. *A first course in modular forms.* Vol. 228. Graduate Texts in Mathematics. Springer, New York, 2005.

[Dokchitser] Tim and Vladimir Dokchitser. *Surjectivity of mod* 2^n *representations of elliptic curves.* arXiv:1104.5031v1 [math.NT] 26 Apr 2011.

[Elkies] Noam D. Elkies. *Elliptic curves with 3-adic Galois representation surjective mod 3 but not mod 9.* arXiv:math/0612734v1 [math.NT] 23 Dec 2006.

[Greicius] Aaron Greicius, Elliptic curves with surjective global Galois representation, Ph.D. thesis, University of California, Berkeley, 2007.

[Hartshorne] Robin Hartshorne. *Algebraic Geometry.* Vol.52. Graduate Texts in Mathematics. Springer-Verlag, 1977.

[Knapp] Anthony W. Knapp. *Elliptic curves.* Mathematical Notes 40. Princeton University Press. Princeton, New Jersey, 1992.

[Kub & Lang] Daniel S. Kubert, Serge Lang. *Modular units.* Vol.244. A Series of Comprehensive Studies in Mathematics. Springer-Verlag, New York, 1981.

[Neukirch] Jürgen Neukirch. *Algebraic Number Theory.* English translation. Vol.322. Springer-Verlag, Berlin, Heidelberg, 1999.

[Serre 1] Jean-Pierre Serre. *A course in arithmetic.* Vol.7. Graduate Texts in Mathematics. Springer-Verlag, 1973.

[Serre 2] Jean-Pierre Serre. *Abelian l-Adic Representations and Elliptic curves*. Wellesley, Mass.: A.K. Peters, 1997.

[Silverman 1] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*. Vol.106. Graduate Texts in Mathematics. Springer-Verlag, 1986.

[Silverman 2] Joseph H. Silverman. *Advanced topics in the Arithmetic of Elliptic Curves*. Vol.151. Graduate Texts in Mathematics. Springer-Verlag, 1994.