# Elliptic Curves with 2-torsion contained in the 3-torsion field

**Laura Paulina Jakobsson**

**Advised by Dr. M. J. Bright**

Universiteit
Leiden

Universita degli studi
di Padova

ALGANT Master's Thesis - 21 June 2016

*Acknowledgement*

First and foremost I would like to thank my advisor Dr. Martin Bright for his guidance and help during the thesis project. I want to also extend my gratitude to all the professors who have taught me in the last two years during and the ALGANT programme for giving me a possibility to do this thesis.

Not forgetting all the friends I made during the two years in Padova and Leiden, I want to thank my friends for sharing the long days and late nights of studying. Finally I would like to thank my family for their support and encouragement that has lead me to where I am now.

# Introduction

The arithmetics of elliptic curves is a well-studied topic in mathematics thanks to the multitude of interesting properties and connections to other topics. Elliptic curves are smooth projective curves, historically arising from elliptic integrals. In more modern research the study of elliptic curves arises naturally in many number theory problems, and elliptic curves even have applications in cryptography. Elliptic curves are interesting also in their own right and in this thesis we shall study one special case of this.

Let $K$ be a number field, i.e. a finite extension of $\mathbb{Q}$, and let $E$ be an elliptic curve over $K$. It is well know that $E$ has an addition of points defined on it and this then gives the curve a group structure. Let $N$ be a positive integer and denote the set of points of order $N$, called $N$-torsion points, by $E[N]$. Then one may define the $N$-*torsion field* (also called $N$-division field) as the finite extension of $K$ given by adjoining the coordinates of the $N$-torsion points, this field is denoted by $K(E[N])$.

If $N$ divides $M$, we have that $E[N] \subseteq E[M]$ which then gives $K(E[N]) \subseteq K(E[M])$ for all elliptic curves $E$ and number fields $K$. Then taking $N, M$ to be coprime raises the question do we have $K(E[N]) \subseteq K(E[M])$ for some $N, M$, and if so what kind of elliptic curves satisfy this condition.

Take $K = \mathbb{Q}$. One can note that if $E/\mathbb{Q}$ has fully rational 2-torsion then we have trivially that $\mathbb{Q}(E[2]) \subseteq \mathbb{Q}(E[N])$ where $N$ is any integer. Then one can find an elliptic curve $E/Q$ satisfying

$$\mathbb{Q}(E[2]) \subseteq \mathbb{Q}(E[3]) \tag{1}$$

Moreover, this containment can also happen when the 2-torsion is not fully rational. In particular the case $\mathbb{Q}(E[2])$ is a degree 6 extension of $\mathbb{Q}$, that is non-abelian, is of interest and there are elliptic curves satisfying (1) with non-abelian 2-torsion field. Our main goal in this thesis is to study this phenomenon for the non-abelian 2-torsion field and to understand when this can happen.

In [1] elliptic curves satisfying (1) with non-abelian 2-torsion field were studied as rational points on the modular curve $X'(6)$, and achieved that each of the elliptic curves is isomorphic to an elliptic curve of the form

$$E : y^2 = x^3 + 3t(1 - 4t^3)x + (1 - 4t^3)(\frac{1}{2} - 4t^3) \text{ for some } t \in \mathbb{Q} \tag{2}$$

This result was expressed as the following theorem.

**Theorem 0.1** (Brau, Jones (2014))**.** *Let $E$ be an elliptic curve over $\mathbb{Q}$. Then $E$ is isomorphic over $\overline{\mathbb{Q}}$ to an elliptic curve $E'$ satisfying $\mathbb{Q}(E'[2]) \subseteq \mathbb{Q}(E'[3])$ if and only if $j(E) = 2^{10}3^3t^3(1 - 4t^3)$ for some $t \in \mathbb{Q}$.*

It is good to note that the above theorem will give elliptic curves with non-abelian 2-torsion field, and that there are other cases not included in the theorem, e.g. when the 2-torsion is fully rational.

However, the proof of the Theorem 0.1 does not provide us with complete understanding of the $j$-invariant, in particular, the question where this $j$-invariant comes from is left open.

One of the ways to approach studying (1) is to note that if a Galois group fixes $\mathbb{Q}(E[3])$, then it must also fix $\mathbb{Q}(E[2])$. This then suggests that studying Galois action on the torsion points of $E$ could give us more information on (1), and indeed this is the case. The action of absolute Galois group of $\mathbb{Q}$, $G_{\mathbb{Q}}$, on sets of torsion points of $E$ defines Galois representations attached to $E$. Then studying the image for these representations allows one to show that an elliptic curve $E/\mathbb{Q}$ satisfying (1) is a non-Serre curve. In [8] it was shown that almost all elliptic curves over $\mathbb{Q}$ are Serre curves. Non-Serre curves have been studied as coming from rational points on modular curves (e.g. in [2]), and this connection to modular curves then motivates us to look at the moduli space of elliptic curves as the second approach.

A moduli space for elliptic curves is a scheme such that each point on the scheme corresponds to a isomorphism class of elliptic curves with some extra structure. It can be shown that a moduli space parametrising elliptic curves with chosen generators for the $N$-torsion exist for $N \geq 3$. It is known that the modular curve $X(N)$ of level $N$ parametrises elliptic curves with a chosen basis for the $N$-torsion. In other words, $X(N)$ is a moduli space for elliptic curves. Then taking a quotient of $X(N)$ by a group $H \subseteq GL_2(\mathbb{Z}/N\mathbb{Z})$ allows us to construct a curve that parametrises elliptic curves with extra conditions. In particular, for a level 6 modular curve we can have the condition (1), and this gives curve $X'(6)$ in [1]. Then the group $H$ giving $X'(6)$ as quotient of $X(6)$ can be given explicitly. This then allows study of the curve $X'(6)$ and one can compute the $j$-invariant for the desired elliptic curves as given in Theorem 0.1.

The organisation of the thesis is as follows. In Chapter 1 we define Galois representations attached to elliptic curves and study the image of these representations. Furthermore, we define Serre curves and establish that an elliptic curve satisfying (1) is not a Serre curve. In Chapter 2 we begin by studying elliptic curves over a scheme and the moduli spaces for them. Then we focus on the specific moduli problem $[\Gamma(N)]$, and study the example $[\Gamma(3)]$ in detail. The final Chapter 3 consist of two parts.The first part focuses on studying modular curves $X(N)$ and $X_H$ obtained from a quotient of $X(N)$ by a group $H$. This is then followed by definition, and studying, of the level 6 modular curve $X'(6)$ parametrising elliptic curves satisfying (1), and a description of the computations needed to reach Theorem 0.1.

# Contents

# Chapter 1

# Galois representations

Let $G$ be a profinite group,i.e. a topologial group tha is isomorphic to a projective limit of finite groups. Let $V$ be a module over a ring $R$ of rank $n$. Then a representation of $G$ is continuous group homomorphism

$$\rho : G \to \mathrm{Aut}(V)$$

A common case is that $V$ is an $n$-dimensional vector space over a field $k$, then after choosing a basis for $V$ the representation becomes $\rho : G \to GL_n(k)$.

Let $K$ be a field and let $G_K = \mathrm{Gal}(\overline{K}/K)$ be the absolute Galois group of $K$. We have that

$$G_K = \varprojlim \mathrm{Gal}(L/K)$$

where $L$ runs over all finite Galois extensions of $K$. The maps $\mathrm{Gal}(L/K) \to \mathrm{Gal}(L'/K)$ for the inverse limit are given as the restriction of $\sigma$ to $L'$ for $\sigma \in \mathrm{Gal}(L/K)$ where $L' \subset L$.

So $G_K$ is a profinite group, and we can define a *Galois representation* simply as a representation of the group $G_K$.

## 1.1 Galois representations attached to elliptic curves

Let $E$ be an elliptic curve defined over the number field $K$. Then one may define Galois representations attached to the elliptic curve by letting the Galois groups $G_K$ act on sets of torsion points of $E$.

### 1.1.1 Mod $m$ representations

Let $\sigma \in G_K$. Let $E/K$ be an elliptic curve and $P = (x, y)$ a point on $E(\overline{K})$. The curve $E$ has a Weierstrass equation

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

We have that $\sigma$ acts on $P$ coordinate wise, then $P$ satisfying the equation implies that so does $\sigma(P)$. Then for all $P, Q$ on $E$ we will get $\sigma(P+Q) = \sigma(P)+\sigma(Q)$. Here $+$ is given by a rational function with all coefficients in $K$. So $\sigma$ induces a group homomorphism $E(\overline{K}) \to E(\overline{K})$, and furthermore through this homomorphism $\sigma$ induces a map $E[m] \to E[m]$.

Choose two points $P, Q$ in $E[m]$ that generate $E[m] \cong (\mathbb{Z}/m\mathbb{Z})^2$. Thus every point in $E[m]$ can be written as $a_1P + a_2Q$ with integers $a_1, a_2$. Take $\alpha \in \mathrm{Aut}(E(\overline{K}))$. Then $\alpha$ restricts to a map $\alpha_m : E[m] \to E[m]$. Computing $\alpha_m$ for the basis $P, Q$ gives that there are integers $a, b, c, d$ such that

$$\alpha_m(P) = aP + bQ \text{ and } \alpha_m(Q) = cP + dQ$$

It follows that each automorphism of $E[m]$ can be represented by $2 \times 2$ matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$. This then defines a homomorphism

$$\begin{aligned} \rho_{E,m} : G_K &\to \mathrm{Aut}(E[m]) \cong GL_2(\mathbb{Z}/m\mathbb{Z}) \\ \sigma &\mapsto \begin{pmatrix} a & b \\ c & d \end{pmatrix} \end{aligned}$$

Indeed this is a Galois representation, particularly the mod $m$ Galois representation attached to elliptic curve $E$.

Note that by the First Isomorphism Theorem we have

$$\rho_{E,m}(G_K) \cong G_K/\ker(\rho_{E,m}) = G_K/\mathrm{Gal}(\overline{K}/K(E[m])) = \mathrm{Gal}(K(E[m])/K) \tag{1.1}$$

Due the above fact the representation $\rho_{E,m}$ is sometimes written as

$$\rho_{E,m} : \mathrm{Gal}(K(E[m]/K)) \to GL_2(\mathbb{Z}/m\mathbb{Z}).$$

**Example 1.1.** *Let $m = 2$ and let $\rho_{E,2}$ be the mod 2 representation attached to an elliptic curve $E$ over $\mathbb{Q}$.*

$$\rho_{E,2} : G_{\mathbb{Q}} \to \mathrm{Aut}(E[2]) \cong GL_2(\mathbb{Z}/2\mathbb{Z})$$

*As* $\rho_{E,2}(G_{\mathbb{Q}}) \cong \mathrm{Gal}(\mathbb{Q}(E[2]/\mathbb{Q}))$*, the possible images of* $\rho_{E,2}$ *and the index of* $\mathrm{Gal}(\mathbb{Q}(E[n]/\mathbb{Q}))$ *in* $GL_2(\mathbb{Z}/2\mathbb{Z})$ *for different* $E$ *can be easily determined based on the 2-torsion points.*

*The torsion for* $E$ *is given by the set of four points* $\{\mathcal{O}, (\alpha, 0), (\beta, 0), (\gamma, 0)\}$*. This gives the* $n$*-torsion field* $\mathbb{Q}(E[2]) = \mathbb{Q}(\alpha, \beta, \gamma)$*.*

*If all* $\alpha, \beta, \gamma$ *are rational numbers, then* $\mathrm{Gal}(\mathbb{Q}(E[2]/\mathbb{Q})) = \{1\}$*, and the image of* $\rho_{E,2}$ *has index 6.*

*If two or more of* $\alpha, \beta, \gamma$ *are not in* $\mathbb{Q}$*, then* $\mathrm{Gal}(\mathbb{Q}(E[2]/\mathbb{Q}))$ *can be written as as the groups*

$$\mathrm{Gal}(\mathbb{Q}(E[2]/\mathbb{Q})) = \begin{cases} \mathbb{Z}/3\mathbb{Z} & \text{if } \alpha, \beta \notin \mathbb{Q}, \gamma \in \mathbb{Q} \\ S_3 & \text{if } \alpha, \beta, \gamma \notin \mathbb{Q} \end{cases}$$

*where* $S_3$ *denotes the permutation group of three elements.*

*Using the formula* $[GL_2(\mathbb{Z}/2\mathbb{Z}) : \mathrm{Gal}(\mathbb{Q}(E[2]/\mathbb{Q}))] = |GL_2(\mathbb{Z}/2\mathbb{Z})|/|\mathrm{Gal}(\mathbb{Q}(E[2]/\mathbb{Q}))|$ *we can compute the index of the image of* $\rho_{E,2}$*. This gives the indices 3 for* $\mathbb{Z}/2\mathbb{Z}$*, 2 for* $\mathbb{Z}/3\mathbb{Z}$ *and 1 for* $S_3$*. Therefore the elliptic curve* $E$ *has surjective* $\rho_{E,2}$ *if and only if* $\mathrm{Gal}(\mathbb{Q}(E[2]/\mathbb{Q})) = S_3$*.*

For the surjectivity of the representation $\rho_{E,n}$ we then have the following theorem by Serre in [13].

**Theorem 1.2** (Serre)**.** *Let* $K$ *be an algebraic number field, and* $E/K$ *an elliptic curve without complex multiplication. Then for all but finitely many primes* $p$*,* $\rho_{E,p} : G_K \to GL_2(\mathbb{F}_p)$ *is surjective.*

### 1.1.2 $\ell$-adic representation

Let $\ell$ be a prime number. Then an $\ell$-adic Galois representation is defined as a continuous homomorphism

$$\phi : G_K \to \mathrm{Aut}(V)$$

where $V$ is a finite-dimensional vector space over $\mathbb{Q}_\ell$ such that $\mathrm{Aut}(V)$ is an $\ell$-adic Lie group.

If $T$ is a free $\mathbb{Z}_\ell$-module of finite rank such that it generates $V$, then $V = T \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$. To define the $\ell$-adic representation attached to elliptic curves, let us first recall the definition of the Tate module of an elliptic curve $E$

$$T_\ell(E) = \varprojlim E[\ell^m]$$

where the maps in the inverse limit are given by the multiplication by $\ell$, i.e. $[\ell] : E[\ell^{n+1}] \to E[\ell^n]$. The Tate module is a free $\mathbb{Z}_\ell$-module of rank 2, i.e. it has a generating set of 2 linearly independent elements. Setting $V_\ell(E) = T_\ell \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ gives a $\mathbb{Q}_\ell$-module with a finite generating set, thus $V_\ell(E)$ is a finite dimensional vector space over $\mathbb{Q}_\ell$. So we may define

$$\rho_{E,\ell^\infty} : G_K \to \operatorname{Aut}(V_\ell(E)) \tag{1.2}$$

We can write $V_\ell = T_\ell[1/\ell]$, this s a localization of $T_\ell$ at $\frac{1}{\ell}$. Then

$$V_\ell/T_\ell = T_\ell[1/\ell]/T_\ell = \bigcup_n \ell^{-n} T_\ell/T_\ell$$

Note that we have $\ell^{-n}T_\ell/T_\ell \cong T_\ell/\ell^n T_\ell \cong E[\ell^n]$. Thus $V_\ell/T_\ell \cong \bigcup_n E[\ell^n]$.

The above isomorphism induces the map $\operatorname{Aut}(T_\ell) \to \operatorname{Aut}(\bigcup_n E[\ell^n])$, which is also an isomorphism. We have the commutative diagram

$$\begin{tikzcd}
\ell^{-n}T_\ell/T_\ell \arrow[r, "{[l^n]}"] & T_\ell/l^nT_\ell \arrow[r, "="] & E[\ell^n] \\
\ell^{-(n+1)}T_\ell/T_\ell \arrow[u, two heads, "{[l]}"] \arrow[r, "{[l^{n+1}]}"] & T_\ell/l^{n+1}T_\ell \arrow[u, "proj"] \arrow[r, "="] & E[\ell^{n+1}] \arrow[u, "{[l]}"]
\end{tikzcd}$$

where $[\ell]$ denotes the multiplication by $\ell$ map. We also have the natural inclusion map $\ell^{-n}T_\ell/T_\ell \to \ell^{-(n+1)}T_\ell/T_\ell$, which gives the maps for the direct limit that is $V_\ell/T_\ell$. Taking the inverse limit of $E[\ell^n]$ is by definition the Tate module $T_\ell$, and we also get that $\varprojlim T_\ell/l^nT_\ell = T_\ell$. Then each of these maps induce a map between the automorphisms. We have that both multiplication by $\ell$ and the inclusion induce the same map $\operatorname{Aut}(\ell^{-(n+1)}T_\ell/T_\ell) \to \operatorname{Aut}(\ell^{-n}T_\ell/T_\ell)$, and so we get the diagram of automorphism groups with the inverse limits

$$\begin{tikzcd}
\vdots & \vdots & \vdots \\
\operatorname{Aut}(\ell^{-(n)}T_\ell/T_\ell) \arrow[u] \arrow[r, "{[l^n]}"] & \operatorname{Aut}(T_\ell/l^nT_\ell) \arrow[u] \arrow[r, "\sim"] & GL_2(\mathbb{Z}/\ell^n\mathbb{Z}) \arrow[u] \\
\operatorname{Aut}(\ell^{-(n+1)}T_\ell/T_\ell) \arrow[u, "{[l]}"] \arrow[r, "{[l^{n+1}]}"] & \operatorname{Aut}(T_\ell/l^{n+1}T_\ell) \arrow[u, "proj"] \arrow[r, "\sim"] & GL_2(\mathbb{Z}/\ell^{n+1}\mathbb{Z}) \arrow[u, "proj"] \\
\vdots \arrow[u] & \vdots \arrow[u] & \vdots \arrow[u] \\
\operatorname{Aut}(V_\ell/T_\ell) \arrow[u] \arrow[r, "\sim"] & \operatorname{Aut}(T_\ell) \arrow[u] \arrow[r, "\sim"] & GL_2(\mathbb{Z}_\ell) \arrow[u]
\end{tikzcd}$$

Then it follows that

$$\mathrm{Aut}(T_\ell) \cong \mathrm{Aut}(V_\ell/T_\ell) \cong \mathrm{Aut}(\bigcup_n E[\ell^n]) \tag{1.3}$$

Let $E[\ell^\infty] = \bigcup_{n\geq 1} E[\ell^n]$. We then have an $\ell$-adic representation

$$\phi_{E,\ell^\infty} : G_K \to \mathrm{Aut}(E[\ell^\infty]) \cong GL_2(\mathbb{Z}_\ell) \tag{1.4}$$

If one considers $GL_2(\mathbb{Z}_\ell)$ inside $GL_2(\mathbb{Q}_\ell)$, then the representations $\phi_{E,\ell^\infty}$ and $\rho_{E,\ell^\infty}$ give the same representation attached to an elliptic curve $E$. This follows from the fact that the action of the Galois group $G_K$ on $V_\ell$ is determined by the action on $T_\ell$. Then the isomorphism (1.3) implies that we can equivalently consider the action of $G_K$ on $E[\ell^\infty]$. We have again a theorem by Serre for the surjectivity of $\rho_{E,\ell^\infty}$ given in [13].

**Theorem 1.3.** *Let $K$ be a number field and $E/K$ be an elliptic curve without complex multiplication. Then for all but finitely many primes $\ell$, we have $\rho_{E,\ell^\infty}(G_K) = \mathrm{Aut}(E[\ell^\infty])$.*

### 1.1.3 Full representation

Let $E_{\text{tors}} := \bigcup_{n\geq 1} E[n]$ be the group of all torsion points of $E$. Then one can define

$$\mathrm{Aut}(E_{\text{tors}}) := \varprojlim \mathrm{Aut}(E[n]).$$

Note that we have $\varprojlim \mathrm{Aut}(E[n]) \cong \varprojlim GL_2(\mathbb{Z}/n\mathbb{Z}) = GL_2(\hat{\mathbb{Z}})$ where $\hat{\mathbb{Z}} = \varprojlim \mathbb{Z}/n\mathbb{Z}$. The Galois group $G_K$ acts on $\mathrm{Aut}(E[n])$ and thus $G_K$ acts continuously on $\mathrm{Aut}(E_{\text{tors}})$, giving the representation

$$\rho_E : G_K \to \mathrm{Aut}(E_{\text{tors}}) \cong GL_2(\hat{\mathbb{Z}}).$$

It is useful to notice that $GL_2(\hat{\mathbb{Z}}) = \prod_\ell GL_2(\mathbb{Z}_\ell)$ where $\ell$ is taken over all primes.

## 1.2 Image of the Galois representations

One of the interesting questions arising from these representations is to understand their image. Let $E$ be an elliptic curve over $K$. For $\rho_{E,n}$ the Theorem 1.2 tells that $\rho_{E,n}$ is surjective in most cases, and Theorem 1.3 states a similar result for $\rho_{E,\ell^\infty}$. For $\rho_E$, there is famous theorem of Serre, which is the following.

**Theorem 1.4.** *Let $E$ be an elliptic curve without complex multiplication over a number field $K$. Then the image of the representation $\rho_E : G_K \to \mathrm{Aut}(E_{tors})$ is an open subgroup of $\mathrm{Aut}(E_{tors}) \cong GL_2(\hat{\mathbb{Z}})$.*

Noting that $\mathrm{Aut}(E_{\mathrm{tors}}) = \prod_\ell \mathrm{Aut}(E[\ell^\infty])$ and that $\rho_{E,\ell^\infty} : G_K \to \mathrm{Aut}(E[\ell^\infty])$ is the $\ell$-th component of $\rho_E$ implies that the above theorem is equivalent to

1. For all primes $\ell$, $\rho_{E,\ell^\infty}(G_K)$ is an open subgroup of $\mathrm{Aut}(E[\ell^\infty])$.

2. For all but finitely many primes $\ell$ the group $\rho_E(G_K)$ contains the $\ell$-th factor $\mathrm{Aut}(E[\ell^\infty])$ of $\mathrm{Aut}(E_{tors})$.

holding simultaneously. For the proof of the theorem see [14] and [13].

From now on we assume that all elliptic curves we encounter are without complex multiplication. It is easy to see that the above theorem does not provide much information on the explicit image of $\rho_E$. So to compute $\rho_E(G_K)$ explicitly one needs to use other approaches. We shall follow the one given in [1], which is to consider the map

$$\pi : \rho_E(G_K) \longrightarrow \prod_\ell \rho_{E,\ell^\infty}(G_K)$$

The image of $\pi$ does project onto each $\ell$-adic factor in $\prod_\ell \rho_{E,\ell^\infty}(G_K)$, however $\pi$ may not be surjective but map to a proper subgroup of $\prod_\ell \rho_{E,\ell^\infty}(G_K)$. For the map $\pi$ to be surjective we need that $K(E[m_1]) \cap K(E[m_2])$ for $m_1$ and $m_2$ coprime, has trivial intersection. The intersection is a Galois extension of $K$, in fact from Galois theory we know that its Galois group is given by $\mathrm{Gal}(\overline{K}/K(E[m_1]))\mathrm{Gal}(\overline{K}/K(E[m_2]))$. If the intersection is non-trivial we have that the Galois group $\mathrm{Gal}(\overline{K}/K(E[m_1]))\mathrm{Gal}(\overline{K}/K(E[m_2]))$ is not $\mathrm{Gal}(\overline{K}/K)$, and so $\pi$ cannot be surjective. The intersection $K(E[m_1]) \cap K(E[m_2])$ for $m_1$ and $m_2$ coprime is called an *entanglement field*, and studying these then allows one to understand the image of $\pi$.

## 1.3 Serre curves

Let us consider the case $K = \mathbb{Q}$ from now on. Then the image of $\rho_E$ for $E/\mathbb{Q}$ depends on the entanglement fields $\mathbb{Q}(E[m_1]) \cap \mathbb{Q}(E[m_2])$ over $\mathbb{Q}$.

It is known that for $E/\mathbb{Q}$ we have the containment

$$\mathbb{Q}(\zeta_n) \subseteq \mathbb{Q}(E[n]) \tag{1.5}$$

If the entanglement field is abelian, then we know from the Kronecker-Weber theorem that it is contained in some cyclotomic fied. This combined with the earlier containment (1.5) gives that over $\mathbb{Q}$ we may have non-trivial entanglement fields, and in fact this is the case. Furthermore we have the containment

$$\mathbb{Q}(\sqrt{\Delta_E}) \subseteq \mathbb{Q}(E[2]) \cap \mathbb{Q}(\zeta_n) \tag{1.6}$$

where $n = 4|\Delta_E|$. Not only can one consider the abelian entanglement fields, but also the non-abelian case. There is one known example of non-abelian entanglement field, namely $\mathbb{Q}(E[2]) \subseteq \mathbb{Q}(E[3])$. For this to be non-abelian $\mathbb{Q}(E[2])$ must be a degree 6 extension and $\mathbb{Q}(E[3])$ a degree 48 extension of $\mathbb{Q}$.

The above observation suggests that the map $\rho_E$ for $E/\mathbb{Q}$ is not surjective. Indeed we have the following proposition given by Serre in [13].

**Proposition 1.5.** *For all elliptic curves $E$ over $\mathbb{Q}$, the image of $\rho_E : G_K \to \mathrm{Aut}(E_{tors})$ is contained in a subgroup of index 2 of $\mathrm{Aut}(E_{tors})$.*

This proposition is then equivalent to saying that we have

$$\left[GL_2(\hat{\mathbb{Z}}) : \rho_E(G_{\mathbb{Q}})\right] \geq 2 \tag{1.7}$$

for all elliptic curves $E$ over $\mathbb{Q}$. It can happen that the containment (1.6) is the only thing preventing $\rho_E$ from being surjective, in this case one has $[GL_2(\hat{\mathbb{Z}}) : \rho_E(G_{\mathbb{Q}})] = 2$. This motivates the following definition.

**Definition 1.6.** *Let $E$ be an elliptic curve over $\mathbb{Q}$. Then $E$ is a* Serre curve *if $[GL_2(\hat{\mathbb{Z}}) : \rho_E(G_{\mathbb{Q}})] = 2$.*

The above definition can be also stated as $E/\mathbb{Q}$ is a Serre curve if $[GL_2(\mathbb{Z}/n\mathbb{Z}) : \rho_{E,n}(G_{\mathbb{Q}})] \leq 2$ for all $n \geq 1$.

It was shown in [8] that almost all elliptic curves over $\mathbb{Q}$ are Serre curves, and moreover that we have the condition $E$ is not a Serre curve if and only if there exists a prime $\ell \geq 5$ with

$\rho_{E,\ell}(G_{\mathbb{Q}}) \subsetneq GL_2(\mathbb{Z}/\ell\mathbb{Z})$, or $[\rho_{E,36}(G_{\mathbb{Q}}), \rho_{E,36}(G_{\mathbb{Q}})] \subsetneq [GL_2(\mathbb{Z}/36\mathbb{Z}), GL_2(\mathbb{Z}/36\mathbb{Z})]$, where $[G, G]$ denotes the commutator subgroup of a group $G$.

Moreover the non-Serre curves have been studied as coming from rational points on modular curves (see Chapter 3 for the definition) and the complete family of such curves is given in [1].

Suppose $E/\mathbb{Q}$ is an elliptic curve that satisfies $\mathbb{Q}(E[2]) \subseteq \mathbb{Q}(E[3])$. In the trivial case that the 2-torsion of $E$ is rational, we have that $[GL_2(\mathbb{Z}/n\mathbb{Z}) : \rho_{E,n}(G_{\mathbb{Q}})] = 6$ as it was computed in the example 1.1 that $\rho_{E,n}(G_{\mathbb{Q}}) = \{1\}$. Then clearly such curve is not a Serre curve. However we are interested in the situation when we have non-abelian extensions, and it can be shown that any curve satisfying $\mathbb{Q}(E[2]) \subseteq \mathbb{Q}(E[3])$ is a non-Serre curve. We show in Chapter 3 that these curves arise from rational points on a modular curve that parametrises non-Serre curves.

# Chapter 2

# Moduli Spaces

One of the big and interesting questions in algebraic geometry is to classify objects. One way of approaching this problem is to look for a scheme that could parametrise the original objects we are interested in. This then allows one to classify objects or families of objects up to a selected equivalence, for example isomorphism, by having a one to one correspondence between the points in the scheme and the equivalence classes. One example of this would be the $j$-invariant for elliptic curves. It is well know that the $j$-invariant divides elliptic curves into isomorphism classes over algebraically closed fields, moreover it provides a one to one correspondence between the classes and points in $\mathbb{P}^1$, which then is the space parametrising elliptic curves by isomorphism. By studying the parametrising scheme one can often learn more about the objects of interest.

At times the problem can be approached in a very concrete way. We now compute an example for parametrising elliptic curves with a point of order 6 ([16], exercise 8.13)

**Example 2.1.** *Let $E$ be an elliptic curve over a number field $K$ and let $P$ be a point of order 6 with coordinates $(u, v)$. We know that it has a Weierstrass equation*

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

*Then there is a change of coordinates giving the equation*

$$y^2 + sxy + ty = x^3 + tx^2$$

*satisfying $s, t \in K$, $(0, 0)$ is a point of order $6$ and the tangent line to $E$ at $(0, 0)$ is given by $y = 0$.*

*A point $Q$ of order 6 must satisfy $[3]Q = -[3]Q$, in particular $P = (0,0)$ satisfies this. There exists a formula for computing the addition on elliptic curves and applying this we get the following equation*

$$s - 1 - t = 1 + s^2 - 2t - 2s$$

*This simplifies to*

$$t = s^2 - 3s + 2$$

*Now any point on the curve $t = s^2 - 3s + 2$ defines an elliptic curve that has a point of order 6 and Weierstrass equation of the form*

$$y^2 + sxy + (s^2 - 3s + 2)y = x^3 + (s^2 - 3s + 2)x^2 \tag{2.1}$$

*Moreover every elliptic curve with a point of order 6 is isomorphic to a curve of the form (2.1).*

## 2.1 Moduli spaces for curves

The curve in the previous example is called a moduli space, or modular curve. Moduli spaces arise as solutions to the moduli problem; a problem of parametrising geometric objects. Our goal is to study elliptic curves so it's natural to narrow the problem down to parametrising curves. In this section we provide a short introduction to general moduli spaces of curves before moving on to considering the case of elliptic curves, for more detailed treatment of moduli spaces of curves see [11] and [5].

A *moduli problem* in general consists of objects and equivalences between them, and a definition for families of these objects over a scheme with equivalences between the families. Then the scheme would be a space parametrising the objects, with a universal family over the scheme.

In our case the objects are algebraic curves over fields and the equivalence between curves is taken to be isomorphism between curves. A family of algebraic curves over a scheme $S$ is defined as a map

$$f : C \to S$$

which is a flat proper morphism with every geometric fibre being a smooth curve. Note that sometimes this is just called an algebraic curve over $S$, e.g. in [9], and not a family of curves.

We say that two families $f : C \to S$ and $g : C' \to T$ are isomorphic if there are isomorphisms $h : C \to C'$ and $h' : S \to T$ such that the diagram below commutes.

$$\begin{tikzcd}
C \arrow[r, "h"] \arrow[d, "f"'] & C' \arrow[d, "g"] \\
S \arrow[r, "h'"] & T
\end{tikzcd}$$

For a scheme $M$ to classify the curves given in the moduli problem it would need to satisfy the following. $M$ has a family of curves $f : \mathcal{C} \to M$ such that for any family of curves $g : C \to S$ there is a unique morphism $h : S \to M$ satisfying $C \cong h^*\mathcal{C} = S \times_M \mathcal{C}$. The curve $\mathcal{C}$ is the universal curve. This is in fact the definition for a *fine moduli space*. If such moduli space exists then it is unique up to isomorphism. Let $M'$ be another scheme satisfying the conditions and let $f' : \mathcal{C}' \to M'$ be a family of curves. Then by the universal property of the moduli space we have the morphisms $h : M' \to M$ and $h' : M \to M'$. By definition the morphisms are unique, so $h'$ is the inverse of $h$ and we get that $M \cong M'$.

An equivalent way of defining the moduli problem is to use the moduli functor

$$\begin{array}{rcl}
F : Sch & \to & Sets \\
S & \mapsto & \{\text{families of curves over S}\}/\cong \\
(S \to S') & \mapsto & (C/S' \to S \times_{S'} C)
\end{array}$$

Then the fine moduli space is a scheme that represents the moduli functor. This means that there exists a scheme $M$ such that the functor $F$ is isomorphic to the contravariant functor $\mathrm{Hom}_{Sch}(-, M) : Sch \to Sets$ given by $S \mapsto \mathrm{Hom}_{Sch}(S, M)$. Then $M$ represents the functor $F$.

The problem arising from this definition is that fine moduli spaces for algebraic curves do not exist due to the automorphisms of the curves. To illustrate this we consider a simple example of curve over $\mathbb{C}$.

**Example 2.2.** *Let $C$ be a curve over $\mathbb{C}$, such that there exists a non-trivial automorphism of $C$, say $\sigma$. We can consider the product $\mathbb{C} \times C$. Note that $\mathbb{Z}$ has an action on $\mathbb{C}$ given by $kz = z + 2\pi ik$ for all $z \in \mathbb{C}$ and $k \in \mathbb{Z}$. Also this can then be used to define an action of $\mathbb{Z}$ on $\mathbb{C} \times C$ by $k(z, P) = (z + 2\pi ik, \sigma^k(P))$. Then clearly the action commutes with the natural projection $\mathbb{C} \times C \to \mathbb{C}$. Now we have that $\mathbb{C}/2\pi i \cong \mathbb{C}^*$ via the exponential map, then the quotient $(\mathbb{C} \times C)/\mathbb{Z}$ gives a family of curves over $\mathbb{C}^*$. Moreover each of the fibres in this family is isomorphic to $C$. Suppose that $M$ is a fine moduli space and $f : \mathcal{C} \to M$ is the* *universal curve for it. Then we must have unique morphism $h : \mathbb{C}^* \to M$ and an isomorphism $(\mathbb{C} \times C)/\mathbb{Z} \cong \mathbb{C}^* \times \mathcal{C}$. The last isomorphism cannot hold and so we get that there is no fine moduli space.*

There are different ways to resolve the issue of not having a fine moduli space. These are defining a coarse moduli space, rigidifying the problem, and using algebraic stacks. We look at rigidifying the moduli problem, that is adding points to give extra structure, and study this for the specific case of elliptic curves in the following sections.

## 2.2 Moduli space for elliptic curves

To define a moduli space for elliptic curves, one needs to first define elliptic curves over an arbitrary base scheme. In this section and in the following ones this chapter we follow closely [9] and all the theorems and definitions can be found in it unless otherwise mentioned.

**Definition 2.3.** *Let $S$ be a scheme and define an elliptic curve $E$ over $S$, denoted by $E/S$, as a smooth morphism of schemes*

$$f : E \to S$$

*such that each fibre of $f$ is a geometrically connected curve of genus one, and with a chosen section $0$ in $E(S)$.*

The sections $p$ in $E(S)$ are points on the curve $E$, and these two terms are used interchangeably.

### 2.2.1 Group structure on $E/S$

For elliptic curves over a field, we know that an elliptic curve $E$ over some field $K$ has addition of two points defined on it and that $E$ forms a group under this operation. One may also define this type of a structure on elliptic curve over a scheme.

To use the definition given in [9] we first say what is an ideal sheaf for a point. On a smooth curve $C/S$ any section $s \in C(S)$ defines a relative Cartier divisor by $[s]$. Recall that $D$ is a relative Cartier divisor in $C/S$ if it is a closed subscheme $D \subset C$ such that $D$ is flat over $S$ and the ideal sheaf $I(D) \subseteq \mathcal{O}_E$ is an invertible $\mathcal{O}_E$-module. So we can consider the ideal sheaf for

$s \in C(S)$, and in particular in our case, by taking a point $P \in E(S)$ we have an ideal sheaf for the point $P$, $I(P)$, given by the ideal sheaf of the relative Cartier divisor $[P]$.

**Theorem 2.4** ([9], Theorem 2.1.2)**.** *Let $E/S$ be an elliptic curve over a scheme $S$. There exists a structure of commutative group scheme on $E/S$ such that for all $S$-schemes $T$, and for any three sections $P, Q, R$ in $E(T) = E_T(T)$, we have $P + Q = R$ if and only if there exists an invertible sheaf $\mathcal{L}_0$ on $T$ and an isomorphism of invertible sheaves on $E_T$*

$$I(P)^{-1} \otimes I(Q)^{-1} \otimes I(0) \cong I(R)^{-1} \otimes f_T^*(\mathcal{L}_0).$$

Note that the section 0 behaves as the identity element on the structure defined by the above theorem.

### Points of order N

Now with the above theorem it makes sense to talk about the point $NP$ defined by adding $P$ to itself $N$ times. Over a field we have that a point $P$ on an elliptic curve has order $N$ if $[N]P = O$, and we want to define an analogy of this for elliptic curves over schemes. In [9] the points with exact order $N$ are defined via Cartier divisors, but we shall use alternative definition that is equivalent by Lemma 1.4.4. in [9].

**Definition 2.5.** *Suppose that $N$ is invertible on $S$. Let $P$ be a point in $E(S)$ satisfying $NP = 0$, then $P$ has* exact order *$N$ if for every geometric point* $\mathrm{Spec}(k) \to S$ *of $S$, the induced point $P_k \in E(k)$ has exact order $N$ in the usual sense, i.e. $N$ is the least positive integer that kills $P_k$.*

Note that for this definition it follows that if $P$ has exact order $N$ then $NP = 0$, which resembles the definition for elliptic curves over fields. The converse is false. For example take $P$ to be a point of exact order of 2, then $6P = 0$ but $P$ is not a point of exact order of 6. For the multiplication by $N$ map we can get the following theorem.

**Theorem 2.6.** *Let $E/S$ be an elliptic curve over scheme $S$, and let $N \geq 1$ be an integer. Then the $S$-homomorphism*

$$[N] : E \to E$$

*is finite locally free of rank $N^2$. Furthermore if $N$ is invertible on $S$, then the kernel of the map, $E[N]$ is finite etale over $S$, and locally on $S$ we have $E[N] \cong (\mathbb{Z}/N\mathbb{Z})^2_S$.*

Here the local condition in the theorem is taken to be locally in the étale topology, as otherwise the isomorphism may not hold.

### 2.2.2 Weierstrass equation for $E/S$

For $E/S$ to have a Weierstrass equation we mean that there exists functions $x$ and $y$ embedding it to $\mathbb{P}^2_S$. This then gives a subscheme of $\mathbb{P}^2_S$ defined by a homogeneous polynomial.

Recall that over a field we know the polynomial is a cubic with one point at $\infty$. This is also the case for each fibre of $E/S$. The fibres are by definition genus 1 curves over a field, i.e. elliptic curves, so we know that each fibre is given by the usual Weierstrass equation for elliptic curves. To show that an elliptic curve $E/S$ also has such a polynomial, one can show that functions $x$ and $y$ exist Zariski locally on $S$ using a similar method to showing an elliptic curve has Weierstrass equation via the Riemann-Roch theorem. For the details see ([9],§2.2). For an elliptic curve $E/S$ we cannot use the Riemann-Roch theorem directly as it is not defined for arbitrary base scheme, however, there exists a generalisation that can be used to establish that locally there exists functions $x$ and $y$ satisfying the generalised Weierstrass equation

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

with $a_i \in \mathcal{O}_S(U)$, where $U$ is the Zariski open covering of $S$ where the the functions $x$ and $y$ are defined.

The general Weierstrass equation for elliptic curves can also be approached from the other direction, i.e. first defining a curve as a subscheme of $\mathbb{P}^2_S$ and then showing that this curve is indeed an elliptic curve over $S$. This is followed for example in [7]. We can define a curve $C$ over $S$ as a closed subscheme of $\mathbb{P}^2_S$ by the homogeneous polynomial

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3 \tag{2.3}$$

where $a_i \in \mathcal{O}_S(S)$. The polynomial has a discriminant $\Delta$ defined by the same way as for an elliptic curve over a field with equation given by the form (2.3), see for example [16]. Then we can define the discriminant of the curve to be this $\Delta$, and we have $\Delta \in \mathcal{O}_S(S)$ as it is defined with the coefficients of the equation (2.3).

Choose the point $(0:1:0)$ in $\mathbb{P}^2_S$. This point can be viewed as a section on the curve $C$ given as a subscheme of $\mathbb{P}^2_S$. Then there is the following proposition.

**Proposition 2.7.** *Let $S$ be a scheme and let $C$ be a curve over $S$ given by (2.3). Suppose that $\Delta \in \mathcal{O}_S(S)^\times$. Then the curve $C$ with the section $(0:1:0)$, is a smooth curve over $S$ with each fibre being a genus 1 curve.*

We give an outline of the proof, for the details see ([7],§1.1). One can show that the morphism $C \to S$ is a flat and proper. For each geometric point $x$ of $S$ we can consider the fibre at that point, given by $C \times_S \operatorname{Spec}(k(x))$ where $k(x)$ is the residue field of $x$. So each fibre is a curve over the field $k(x)$ given by an equation of the form (2.3), and so we know each one has genus 1. Lastly to show that $\Delta \in \mathcal{O}_S(S)^\times$ implies that the curve is smooth we again consider the fibres at each geometric point of $S$. We have that the curve $C$ is smooth if and only if it is smooth on all the fibres. If $\Delta = 0$ in the fibre, then it is not a smooth curve over a field, and so we must have that $\Delta \neq 0$ at the fibres. This then implies that the curve is smooth if and only if $\Delta \neq 0$ at every geometric point of $S$, that is $\Delta \in \mathcal{O}_S(S)^\times$.

Hence we have that the subscheme defined by (2.3) is a smooth curve over $S$ such that every fibre is a curve of genus one and there is a chosen section, and this is precisely our definition of an elliptic curve. So we get that $E/S$ has a Weierstrass equation given by (2.3).

### 2.2.3 Category of elliptic curves

Recalling that the definition for a moduli problem requires one to know how to define equivalence between the elliptic curves, we will then need to define what is an isomorphism between the elliptic curves $E/S$ and $E'/S'$. First we shall define the category of elliptic curves.

**Definition 2.8.** *The category of elliptic curves, $\mathcal{E}ll$, is the category with objects elliptic curves $f: E \to S$ with section $0$ over a base scheme $S$. The morphisms in the category are given by pairs $(h: S' \to S, g: E' \to E)$ such that the following diagram commutes and that $E' \to E \times_S S'$ is an isomorphism of elliptic curves over $S'$.*

$$\begin{tikzcd}
E' \arrow[r, "g"] \arrow[d, "f'"'] & E \arrow[d, "f"] \\
S' \arrow[r, "h"] & S
\end{tikzcd}$$

*Furthermore, one requires that the section* $0_{S'} : S' \to E'$ *induced by* $0$ *equals* $0$.

The category $\mathcal{E}ll$ is sometimes called a modular stack, for example in [3].

In the category of elliptic curves we have a contravariant functor given by

$$\begin{aligned} \mathrm{Hom}_{\mathcal{E}ll}(-, E/S) : \mathcal{E}ll &\longrightarrow Sets \\ E'/S' &\mapsto \mathrm{Hom}_{\mathcal{E}ll}(E'/S', E/S) \end{aligned}$$

For each pair $(h, g)$ in $\mathrm{Hom}_{\mathcal{E}ll}(E'/S', E/S)$ we can consider the pullback of $E$ by $h$. This is given by $h^*(E) = E \times_S S'$. Then as we have the maps $g$ and $f'$ the properties of pull back imply that there exists a function $g' : E' \to h^*E$ that is unique up to isomorphism, satisfying.

$$\begin{tikzcd}
E' \arrow[dr, dotted, "g'"] \arrow[drr, bend left, "g"] \arrow[ddr, bend right, "f'"'] & & \\
& h^*E \arrow[r] \arrow[d] & E \arrow[d, "f"] \\
& S' \arrow[r, "h"] & S
\end{tikzcd}$$

A fibre for $h^*E/S'$ is given by

$$h^*E \times_{S'} \mathrm{Spec}(k(y)) = E \times_S S' \times_{S'} \mathrm{Spec}(k(y)) = E \times_S \mathrm{Spec}(k(y))$$

where $k(y)$ is the residual field of $y \in S'$. Then clearly the each fibre is a curve of genus one. So $h^*E$ is an elliptic curve over $S'$.

Note that as both squares in the diagram commute we have that each pair $(h, g)$ defines unique map $g'$. On the other hand if we have the maps $h$ and $g'$, one can construct $g$. Thus we may write

$$\mathrm{Hom}_{\mathcal{E}ll}(E'/S', E/S) = \{(h, g') : h : S' \to S, g' : E' \to h^*E\}.$$

### 2.2.4 Moduli problem

Having defined the category for elliptic curves one may now define the moduli problem.

**Definition 2.9.** *A moduli problem for elliptic curves is a contravariant functor*

$$\mathcal{P} : \mathcal{E}ll \to Sets.$$

For a moduli functor $\mathcal{P}$ the set $\mathcal{P}(E/S)$ is called a level $\mathcal{P}$ structure on $E/S$.

As with the moduli problem for algebraic curves, we say that the moduli problem $\mathcal{P}$ is representable if it is representable as a functor. That is, there exists an elliptic curve $\mathcal{E}$, and a scheme $M$ such that $\mathcal{P}$ is isomorphic with $\mathrm{Hom}_{\mathcal{E}ll}(-, \mathcal{E}/M)$ as functors.

Clearly this definition allows to have many different moduli functors for elliptic curves, and depending on the chosen functor elliptic curves with different properties can be parametrised with the moduli space. We are interested in studying elliptic curves with chosen $N$-torsion, hence we want to study the moduli problem parametrising elliptic curves with a specific $N$-torsion points.

For this purpose we introduce the level $N$ structure on an elliptic curve.

**Definition 2.10.** *Let $E/S$ be an elliptic curve and let $N \geq 1$ be an integer. Then a* level N-structure*, or* $\Gamma(N)$-structure *on $E/S$ is the homomorphism of group schemes*

$$\alpha : (\mathbb{Z}/N\mathbb{Z})^2_S \to E[N]$$

*such that $\alpha(1, 0)$ and $\alpha(0, 1)$ are generators for $E[N]$.*

If $N$ is invertible on $S$ then it follows from Theorem 2.6 that $\alpha$ is an isomorphism.

Using the level $N$-structure we can define a functor that parametrises elliptic curves with a chosen basis for $N$-torsion. Let $\mathcal{E}ll/S$ denote the category of elliptic curves over $S$-schemes, i.e. $E/T$ with $T$ an $S$-scheme. Then the functor is given as

$$\begin{array}{rcl} [\Gamma(N)] : \mathcal{E}ll/S & \to & Sets \\ E/T & \mapsto & \text{level N-structures } \alpha : (\mathbb{Z}/N\mathbb{Z})^2 \to E[N] \text{ on } E/T \end{array} \tag{2.4}$$

If one considers $S = \mathrm{Spec}\mathbb{Z}[1/N]$, that is the universal base scheme where $N$ is invertible. Let $T$ be an $\mathbb{Z}[1/N]$-scheme, then the functor can be expressed as

$$E/T \mapsto \{\text{isomorphisms } \alpha : (\mathbb{Z}/N\mathbb{Z})^2 \xrightarrow{\sim} E[N]\}$$

Recalling that the first definition for the moduli functor was given as functor from schemes to sets, this then motivates the definition for the naive functor

$$\begin{aligned} F_N : Sch/S &\rightarrow Sets \\ T &\mapsto \text{isomorphism classes of } E/T \text{ with a level } N \text{ structure } \alpha \end{aligned} \tag{2.5}$$

It can be shown that if the functors $F_N$ and $[\Gamma(N)]$ are represented by the same scheme, if they are taken over the same base scheme, thus they can be considered to give the same moduli problem. We have that if $[\Gamma(N)]$ is representable by $\mathcal{E}/M$ then $F_N$ is representable by $M$. Conversely, if $F_N$ is represented by a scheme $M$ then $[\Gamma(N)]$ is represented by $\mathcal{E}/M$ with $\mathcal{E}$ being the universal curve.

We then have the diagram of functors

$$\begin{tikzcd} \mathcal{E}ll \arrow[r, "{[\Gamma(N)]}"] \arrow[d, "f"'] & Sets \arrow[d, "\text{id}"] \\ Sch \arrow[r, "F_N"] & Sets \end{tikzcd}$$

where $f$ is taken to be the functor given by $E/T \mapsto T$.

## 2.3 Representability of the moduli functor

Naturally one would like to ask the question when is the moduli problem $[\Gamma(N)]$ representable. To answer this question we introduce the concept of being relatively representable.

**Definition 2.11.** *Let $\mathcal{P}$ be a moduli problem for elliptic curves. $\mathcal{P}$ is said to be* relatively representable *over $\mathcal{E}ll$ if for every $E/S$ the functor $(Sch/S) \rightarrow Sets$ given by $T \mapsto \mathcal{P}(E/T)$ is representable by an $S$-scheme.*

We say that $\mathcal{P}$ is affine if the $S$-scheme representing the functor $(Sch/S) \rightarrow Sets$ is affine. It can be shown that $[\Gamma(N)]$ satisfies this property, and the functor in the definition is $F$,

$$\begin{aligned} F : Sch/S &\rightarrow Sets \\ T &\mapsto \text{level N-structures } \alpha : (\mathbb{Z}/N\mathbb{Z})^2 \rightarrow E[N] \text{ on } E/T \end{aligned} \tag{2.6}$$

for the moduli problem $[\Gamma(N)]$, and that the scheme representing $F$ is affine.

**Theorem 2.12.** *Let $N \geq 1$. The functor $[\Gamma(N)]$ is represented by a finite $S$-scheme, i.e. $[\Gamma(N)]$ is relatively representable. Moreover $[\Gamma(N)]$ is finite etale over $S$.*

Furthermore we have that for $N \geq 3$, $[\Gamma(N)]$ is rigid, which means it satisfies the following definition.

**Definition 2.13.** *Moduli problem $\mathcal{P}$ is* rigid *if for any $E/S$ and any level $\mathcal{P}$ structure $\alpha$ the pair $(E/S, \alpha)$ has no non-trivial automorphisms.*

With the two above definitions in mind we can now formulate the necessary and sufficient condition for a moduli problem to be representable.

**Theorem 2.14.** *Let $\mathcal{P}$ be a relatively representable and affine moduli problem over $\mathcal{E}ll/S$. Then $\mathcal{P}$ is representable if and only if it is rigid.*

If the moduli problem $\mathcal{P}$ is also etale, then the moduli space $M$ is a smooth affine curve over $S$.

Finally we state the theorem describing the representability of the $[\Gamma(N)]$- functor when $N$ is invertible in the base scheme $S$.

**Theorem 2.15.** *Let $[\Gamma(N)]$ the functor given by (2.4). $[\Gamma(N)]$ is representable for $N \geq 3$ and its moduli scheme is smooth affine curve over* $\mathrm{Spec}\mathbb{Z}[1/n]$

This results follows from Theorem 2.14 and from that $[\Gamma(N)]$ is relatively representable and rigid for $N \geq 3$.

### 2.3.1 Example $[\Gamma(3)]$

Let $[\Gamma(3)]$ be functor for the level 3 moduli problem given for $\mathbb{Z}[1/3]$-schemes. We have seen that to compute the moduli space we may consider the functor given by

$$E/S \to \{\text{isomorphisms } \alpha : (\mathbb{Z}/3\mathbb{Z})^2 \to E[3]\}$$

Let $S$ be a $\mathbb{Z}[1/3]$-scheme, and take $(E/S, \alpha)$ be an elliptic curve with a level 3 structure.

Define the sections $P = \alpha(1,0)$ and $Q = \alpha(0,1)$ in $E(S)$. As seen earlier these sections can be considered to be points on the curve $E$.

In the section 2.2.2 we saw that on a Zariski open cover $U$ of $S$ there are functions $x$ and $y$ on $E$, and these functions give a generalised Weierstrass equation

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

with the coefficients $a_i \in \mathcal{O}_S(U)$. Similar to Example 2.1 we can simplify the Weierstrass equation with a coordinate change. The coordinates of the point $P$ are given by functions $x(P), y(P)$ on $S$. Then changing $x$ and $y$ by subtracting the functions $x(P)$ and $y(P)$ will give $P = (0, 0)$ and the equation takes the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x \tag{2.7}$$

We can considering that the tangent line at $P$ for the affine equation. Then this line is given by an equation $a_3y = a_4x$. $P$ corresponds to a point of order 3 in each fibre, which are elliptic curves over a field given by the equation (2.7). If the tangent line at $P$ is given by $a_4x = 0$, then it is so in each fibre. For elliptic curves over field we know that tangent line parallel to the $y$-axis corresponds to a point of order 2, but $P$ is a point of order 3 so it is not possible to have tangent line parallel to the $y$-axis at $P$. This then tells $a_3 \neq 0$ in any of the fibres, and so is invertible in $S$. Changing the function $y$ by subtracting $(a_4/a_3)x$ from $y$ will remove the coefficient $a_4$ from the Weierstrass equation. Then the tangent line at $P$ will have the equation $y = 0$.

Note that as $P$ is a point of order 3 we have that the tangent line must intersect at $P$ with multiplicity 3. This can be seen by considering the fibres again. Intersection of multiplicity 3 at a point of order 3 is known for elliptic curves over a field, in particular this means that in each fibre the tangent line has intersection of multiplicity 3. This implies that $a_2$ must also be 0 in each fibre. So now we can deduce that the tangent line at $P$ must intersect with multiplicity 3 as $P$ is a point of order 3, and moreover we get an equation of the form

$$y^2 + a_1xy + a_3y = x^3 \tag{2.8}$$

Furthermore computing the discriminant $\Delta = a_3^3(a_1^3 - 27a_3)$ of $E$, we find that $a_3$ and $a_1^3 - 27a_3$ are invertible as the discriminant must be invertible. This again follows from that if $\Delta = 0$ in some fibre, then this fibre is not an elliptic curve, and so $\Delta \neq 0$ in all fibres implying that it must be invertible in $S$.

Let $Q = (u, v)$. The coordinates $u$ and $v$ are invertible functions on $S$. This is because if $u = 0$ then (2.8) would give $v = 0$ or $-a_3$, so $Q = \pm P$ which is not possible as $P$ and $Q$ form a basis for $E[3]$. Now if $v = 0$ then we would get that $u$ is also 0 and that $P = Q$.

Considering the tangent line at $Q$ we can compute $a_1$ and $a_3$ in terms of $u$ and $v$. Let $y = c - bx$ be the tangent line to $E$ at $Q$. The line intersects $E$ with multiplicity 3 at $Q$ due to $Q$ being a point of order 3. Combining this with that $x - u$ is a local parameter then we get the equation

$$x^3 - (c - bx)^2 - a_1 x(c - bx) - a_3(c - bx) = (x - u)^3$$

The coefficients of powers of $x$ give the following system of equations

$$\begin{cases} 3u = b^2 - a_1 b \\ 3u^2 = 2bc - a_1 c + a_3 b \\ u^3 = c^2 + a_3 c \end{cases} \tag{2.9}$$

For $(u, v)$ to be a point of order 3 it must satisfy the above equations. The first equation gives that $b$ must be invertible as $u$ is invertible. This then implies we can adjust $x$ and $y$ such that we get a tangent line $x + y = c$ where $c = u + v$. So now one can write the equations (2.9) as

$$\begin{cases} 3u = 1 - a_1 \\ 3u^2 = 2(u + v) - a_1(u + v) + a_3 \\ u^3 = (u + v)^2 + a_3(u + v) \end{cases}$$

The first two equations can be used to express $a_1$ and $a_3$ in terms of $u$ and $v$, which gives $a_1 = 1 - 3u$, $a_3 = -3uv - u - v$. Then from the remaining equation we get $u^2 + 3uv + 3v^2 = 0$.

Now define the ring $R = \mathbb{Z}[u, v][1/3, 1/\Delta, 1/u]/(u^2 + 3uv + 3v^2)$, where $\Delta$. Then $M := \mathrm{Spec}R$ is the moduli space with universal curve

$$\mathcal{E} : y^2 + a_1 xy + a_3 y = x^3$$

with $a_1, a_3$ given by the above equations in $u$ and $v$, and the points $P_3 = (0, 0)$, $Q_3 = (u, v)$ giving the level 3 structure $\alpha_3 : (\mathbb{Z}/3\mathbb{Z})^2_S \to \mathcal{E}[3]$.

To show that the curve $u^2 + 3uv + 3v^2$ indeed parametrises elliptic curves we show that $\mathcal{E}/M$ represents the functor $[\Gamma(3)]$. Recall that for $\mathcal{E}/M$ to represent the functor we must have the natural isomorphism between the functors $[\Gamma(3)]$ and $\mathrm{Hom}_{\mathcal{E}ll}(-, \mathcal{E}/M)$. That is the diagram

$$\begin{tikzcd}
\mathrm{Hom}_{\mathcal{E}ll}(E/S, \mathcal{E}/M) \arrow[r, "\phi_{E/S}"] \arrow[d, "f'"'] & {[\Gamma(3)](E/S)} \arrow[d, "f"] \\
\mathrm{Hom}_{\mathcal{E}ll}(E'/S', \mathcal{E}/M) \arrow[r, "\phi_{E'/S'}"'] & {[\Gamma(3)](E'/S')}
\end{tikzcd}$$

Let $E/S$ be an elliptic curve over some scheme $S$, then from section 2.2.3 we know that $\mathrm{Hom}_{\mathcal{E}ll}(E/S, \mathcal{E}/M)$ can be written as $\{(h,g) : h : S \to M, g : E \to h^*\mathcal{E}\}$. Next we want to define a map $\phi_{E/S} : \mathrm{Hom}_{\mathcal{E}ll}(E/S, \mathcal{E}/M) \to [\Gamma(3)](E/S)$. To do this we need the pullback of $\alpha_3$ by $h$. We know that $h^*\mathcal{E}$ is an elliptic curve, so we can define the pullback of $\alpha_3$

$$h^*\alpha_3 : (\mathbb{Z}/3\mathbb{Z})^2_S \to h^*(\mathcal{E}[3])$$

Note that this map is an isomorphism. Now we can define the map

$$\begin{aligned} \phi_{E/S} : \mathrm{Hom}_{\mathcal{E}ll}(E/S, \mathcal{E}/M) &\longrightarrow [\Gamma(3)](E/S) \\ (h,g) &\mapsto g^{-1} \circ h^*\alpha_3 \end{aligned}$$

We want to show that the map $\phi_{E/S}$ is an isomorphism. The map $h$ in the pair $(h,g)$ is locally a morphism of affine schemes, so it can be defined in terms of the map between the rings. Let $S = \mathrm{Spec}A$ locally, then we have a map $\phi : R \to A$. We define this map by sending $u, v \in R$ to the functions $u$ and $v$ on $S$ associated to a level 3-structure $\alpha : (\mathbb{Z}/3\mathbb{Z})^2_S \to E[3]$.

Now we have a Zariski open cover $\bigcup_i U_i$ od $S$ and a morphism $U_i \to \mathrm{Spec}R$ for each $i$ defined by the functions $u$ and $v$. On an intersection $U_i \cap U_j$ for some $i$ and $j$ we have two maps to $\mathrm{Spec}R$. A point $x \in U_i \cap U_j$ is being mapped to two elliptic curves over $S$. Considering the fibre at the point $x$ we have that both elliptic curves must have the same fibre. Thus we get that the elliptic curves over $S$ coming from $x$ are in the same isomorphism class and thus the morphism $U_i \to \mathrm{Spec}R$ and $U_j \to \mathrm{Spec}R$ give the same morphism on the intersection. This then gives a glueing for the local morphism and we will have a map $S \to M$.

Then $E$ is given by the Weierstrass equation (2.8), and furthermore so is $h^*\mathcal{E}$. Thus the map $g : E \to h^*\mathcal{E}$ is a canonical isomorphism that satisfies $g \circ \alpha = h^*\alpha_3$. The equality of level 3-structures follows from that $g$ induces a map between $E[3]$ and $h^*\mathcal{E}[3]$, which is an isomorphism as $g$ is an isomorphism. It follows that the map $\phi_{E/S}$ is bijective.

Set $\phi^{-1}_{E/S}(\alpha) = (h,g)$. This then gives the inverse for $\phi_{E/S}$, and so it follows that it defines an isomorphism for all $E/S \in \mathcal{E}ll$.

The isomorphism shows that $\mathcal{E}/M$ represents the functor $[\Gamma(3)]$, and hence the curve $u^2 + 3uv + 3v^2$ parametrises elliptic curves with a chosen basis for the 3-torsion.

# Chapter 3

# The modular curve $X'(6)$

From the results of the previous chapter we know that we can parametrise elliptic curves with a chosen basis for the $n$-torsion points with smooth affine curves. However this does not provide enough information on our problem of parametrising elliptic curves $E$ with $\mathbb{Q}(E[2]) \subseteq \mathbb{Q}(E[3])$. Studying modular curves as moduli spaces for elliptic curves provides information on elliptic curves with a level structure together with some extra conditions. One can show that the modular curve $X(N)$ is the moduli space corresponding to the moduli problem $[\Gamma(N)]$ given in the previous chapter.

## 3.1 Modular curve $X(N)$

Let $\mathbb{H} = \{z \in \mathbb{C} : \Im(z) > 0\}$ be the upper half plane, and let $\Gamma(N)$ be the subgroup of $SL_2(\mathbb{Z})$ given by $\{\gamma \in SL_2(\mathbb{Z}) : \gamma \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{N}\}$. There is an action of $\Gamma(N)$ on $\mathbb{H}$ given by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} z = \frac{az+b}{cz+d}$$

for all $z \in \mathbb{H}$. So one can look at the set $Y(N) = \mathbb{H} \setminus \Gamma(N)$. Then $Y(N)$ is a non-compact Riemann surface, and one can compactify it by adding finitely many points. Namely these points are $\mathbb{P}^1(\mathbb{Q}) \setminus \Gamma(N)$, the cusps of $\Gamma(N)$.

Let us define $X(N) := \mathbb{H} \setminus \Gamma(N) \cup \mathbb{P}^1(\mathbb{Q}) \setminus \Gamma(N)$ as the modular curve. Note that it is also common to define $X(N)$ as $\mathbb{H}^* \setminus \Gamma(N)$, where $\mathbb{H}^*$ is the extended upper half plane, i.e. $\mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})$. One can easily see that these two definitions for $X(N)$ are the same.

Studying $X(N)$ as an analytic space, it can be shown that $X(N)$ is a compact Riemann surface of dimension 1 (see for example [4]). A compact Riemann surface of dimension one can be viewed as an algebraic curve. Thus we may study $X(N)$ as an algebraic curve instead of a Riemann surface.

The curve $X(N)$ has a natural structure as a curve over $\mathbb{C}$ from the definition. By considering the function field $\mathbb{C}(X(N))$ for $X(N)$ one can show that the field of definition for $X(N)$ as an algebraic curve is in fact $\mathbb{Q}(\mu_N)$ where $\mu_N$ is the group of $N$-th roots of unity.

First consider the function field for $X(1)$. The function field $\mathbb{C}(X(N))$ is generated by the modular invariant $j : \mathbb{H} \to \mathbb{C}$, which is holomorphic on $\mathbb{H}$ and surjective. So we have that $\mathbb{C}(X(N)) = \mathbb{C}(j)$. As we have one to one correspondence between points in $\mathbb{H}$ and lattices in $\mathbb{C}$, it is easy to see that this modular invariant $j$ is in fact the usual $j$-invariant for elliptic curves over $\mathbb{C}$.

As we have a canonical projection $X(N) \to X(1)$ we get that the function field of $X(N)$ is an extension of $\mathbb{C}(j)$. The functions in $\mathbb{C}(X(N))$ are modular functions of level $N$ on $\mathbb{H}$. One can express the different types of functions in terms of points of finite order of an elliptic curve. Let $E_L$ be an elliptic curve over $\mathbb{C}$ given by

$$y^2 = 4x^3 - g_2(L) - g_3(L)$$

where $L$ is the lattice $\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ in $\mathbb{C}$. The points of finite order on $E_L$ are given by the formula

$$\left( \wp(a \begin{bmatrix} \omega_1 \\ \omega_2 \end{bmatrix}; L), \wp'(a \begin{bmatrix} \omega_1 \\ \omega_2 \end{bmatrix}; L) \right)$$

Here $\wp$ denotes the Weierstrass $\wp$ function relative to lattice $L$ and $a$ is a row vector in $\mathbb{Q}^2$. Recall that $\wp(z; L) = \frac{1}{z^2} + \sum_{\substack{\omega \in L \\ \omega \neq 0}} \left( \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right)$. Then one can define the function $f_a$ on $\mathbb{H}$

$$f_a(z) = \frac{g_2(L) g_3(L)}{\Delta(L)} \wp(a \begin{bmatrix} \omega_1 \\ \omega_2 \end{bmatrix}; L)$$

Then we have the following

**Proposition 3.1.** *For every positive integer $N$,*

$$\mathbb{C}(j, f_a | a \in ((\mathbb{Z}/N\mathbb{Z})^2 - (0,0))/\pm 1)$$

*is the function field for $X(N)$.*

For proof see [15] Proposition 6.1.

It can be shown that adjoining the functions $f_a$ given in Proposition 3.1 also adjoins the $x$-coordinates of the $N$-torsion points of the elliptic curve $E_j$ (see [4] for details). Here $E_j$ is an elliptic curve over $\mathbb{C}$ such that it has $j(E_j) = j$. This elliptic curve is given by the equation

$$E_j : \ y^2 + xy = x^3 - \frac{36}{j - 1728}x - \frac{1}{j - 1728} \tag{3.1}$$

Then we get the following Proposition describing the function field of $X(N)$.

**Proposition 3.2.** *Let $E_j$ be an elliptic curve over $\mathbb{C}$, given by the equation (3.1), so the $j$-invariant of $E$ is $j$. Then the field of meromorphic functions on $X(N)$ is given by*

$$\mathbb{C}(X(N)) = \mathbb{C}(j, x(E_j[N]))$$

The field $\mathbb{C}(j, E_j[N])$ can be decomposed to $\mathbb{C} \otimes \mathbb{Q}(j, E_j[N])$, and so we can consider the function field over $\mathbb{Q}$. The field $\mathbb{Q}(j, x(E_j[N]))$ gives all the rational functions on $X(N)$, and moreover the field $\mathbb{Q}(j, x(E_j[N]))$ defines $X(N)$ as a curve over $\mathbb{Q}(\mu_N)$.

Now that we know $X(N)$ to be an algebraic curve defined over the field $\mathbb{Q}(\exp(2\pi i/N))$, we may also consider it as a curve over the scheme $\mathrm{Spec}(\mathbb{Z}[1/N])$. Then it has been shown in [3] that $X(N)$ represents the functor $F_N : Sch/S \to Sets$ given by $F_N(T) =$ isomorphism classes of elliptic curves over $T$ with a level $N$ structure $\alpha$ such that $\zeta(\alpha) = \exp(2\pi i/N)$. The map $\zeta(\alpha)$ is given by $\zeta(\alpha) = e_N(\alpha^{-1}(1,0), \alpha^{-1}(0,1))$ and $e_N$ is the usual Weil pairing for elliptic curves. In the section 2.3 we saw that the moduli problem $[\Gamma(N)]$ was representable if and only if the naive moduli problem $F_N$ is representable, and more over that they correspond to the same moduli space. From this we have that as a scheme $X(N)$ is the moduli space for $[\Gamma(N)]$. As the moduli spaces are unique up to isomorphism it follows that $X(N)$ is the moduli space parametrising elliptic curves with the chosen basis for $N$-torsion.

The above also implies that the curve in the Example 2.3.1, $\mathrm{Spec}\mathbb{Z}[u,v][1/3, 1/\Delta, 1/u]/(u^2 + 3uv + 3v^2)$ is the modular curve $Y(3)$, and thus we know that $Y(3)$ has a defining equation $u^2 + 3uv + 3v^2$.

It is worth noting that the modular curves $X_1(N)$ and $X_0(N)$ are often studied as they also parametrise elliptic curves. These curves are defined by taking the quotient of $\mathbb{H}^*$ by the groups $\Gamma_1(N) = \{\gamma \in SL_2(\mathbb{Z}) : \gamma \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} (\text{mod } n)\}$ and $\Gamma_0(N) = \{\gamma \in SL_2(\mathbb{Z}) : \gamma \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} (\text{mod } n)\}$ respectively. Then $X_1(N)$ parametrises elliptic curves with a chosen point of order $N$ and $X_0(N)$ parametrises elliptic curves with an subgroup of order $N^2$.

## 3.2 Quotient curve $X_H$

We know that there is a natural surjective projection

$$X(n) \to X(1) \tag{3.2}$$

that gives the field extension $\mathbb{C}(X(N))$ of $\mathbb{C}(j)$. As we have that $\mathbb{C}(X(N)) = \mathbb{C}(j, E_j[N])$, it is not hard to see that the field extension $\mathbb{C}(X(N))/\mathbb{C}(j)$ is a finite extension, moreover it is a Galois extension. The Galois group for this covering is given by $\Gamma(1)/\Gamma(n) \cong SL_2(\mathbb{Z}/n\mathbb{Z})/\{\pm 1\}$. In the previous section we have seen that the function field can be taken over $\mathbb{Q}$. The extension $\mathbb{Q}(j, E_j[N])/\mathbb{Q}(j)$ is also a Galois extension, however the Galois group is isomorphic to $GL_2(\mathbb{Z}/N\mathbb{Z})$.

Taking a normal subgroup of $G \subset SL_2(\mathbb{Z}/n\mathbb{Z})$ will correspond to intermediate Galois covering $X_G$ of $X(n) \to X(1)$ with $X_G \cong X(n)/G$. This follows from the theory for Galois coverings, as normal subgroups of the Galois group correspond to intermediate field extensions of the function fields. Let $H \subset GL_2(\mathbb{Z}/n\mathbb{Z})$ and set $H_0 = H \cap SL_2(\mathbb{Z}/n\mathbb{Z})$. Let us denote by $X_H$ the quotient curve $X(n)/H_0$.

As a curve over $\mathbb{C}$, $X_H$ is defined by the group $H_0$. The non-cuspidal points of $X_H$ correspond to pairs of $\mathbb{C}$-isomorphism classes of of elliptic curves $E$ and $H_0$-orbit of level $N$-structures. Furthermore, from the fact that $X(N)$ is a curve defined over the field $\mathbb{Q}(\mu_N)$, $X_H$ is defined as an algebraic curve over the field $\mathbb{Q}(\mu_N)^{\det H}$. Here $\mathbb{Q}(\mu_N)^{\det H}$ denotes the subfield of $\mathbb{Q}(\mu_N)$ fixed by the action of $\det H \subseteq (\mathbb{Z}/N\mathbb{Z})^\times$. Note that $\text{Gal}(\mathbb{Q}(\mu_N)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$. Thus if $\det : H \to (\mathbb{Z}/n\mathbb{Z})^\times$ is surjective then $X_H$ is a curve defined over $\mathbb{Q}$ with a function field corresponding to the group $H$. Conversely, if $K$ is a function field of an algebraic curve, then the Galois group $H$ corresponding to the field $K$ satisfies $\det H = (\mathbb{Z}/N\mathbb{Z})^\times$. This gives the following proposition, for the proof see [4].

**Proposition 3.3.** *Let $H \subseteq GL_2(\mathbb{Z}/N\mathbb{Z})$ and let $K$ be the subfield of $\mathbb{Q}(j, E_j[N])$ corresponding to $H$. Then $det: H \to (\mathbb{Z}/N\mathbb{Z})^\times$ is surjective if and only if $K$ is a function field of an algebraic curve over $\mathbb{Q}$.*

For $X(N)$ we have the intermediate coverings from the modular curves $X_1(N)$ and $X_0(N)$, and it can be shown that the groups corresponding to these curves are

$$\left\{\pm\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} : b \in \mathbb{Z}/N\mathbb{Z}\right\} \text{ and } \left\{\pm\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : a, b, c \in \mathbb{Z}/N\mathbb{Z}\right\}$$

as subgroups of $GL_2(\mathbb{Z}/N\mathbb{Z})/\pm I$ and that they have the function fields

$$\mathbb{Q}(j, f_1) \text{ and } \mathbb{Q}(j, j_N)$$

where $f_1 = f_{(0,1)}$ and $j_N(\tau) = j(N\tau)$.

The function field for the $X_H$ is then the fixed field of $\mathbb{C}(j, E_j[N])$ under the action of $H$.

### 3.2.1 Galois action on the curve

Let $H \subset GL_2(\mathbb{Z}/N\mathbb{Z})$, and suppose that $\det H = (\mathbb{Z}/N\mathbb{Z})^\times$ and $-I \in H$ from now on. Let $X_H$ be the quotient curve as defined earlier, then $X_H$ indeed corresponds to an algebraic curve over $\mathbb{Q}$ by Proposition 3.3.

The group $GL_2(\mathbb{Z}/N\mathbb{Z})$ is the automorphism group for $(\mathbb{Z}/N\mathbb{Z})^2$, so then $H \subseteq GL_2(\mathbb{Z}/N\mathbb{Z})$ has an action on the group of level $N$-structures through the action on $(\mathbb{Z}/N\mathbb{Z})^2$. We can define a *level $H$ structure* on an elliptic curve $E$ as the $H$-orbit of level $N$ structures. In the notation of [3] this is given as $\mathrm{Hom}((\mathbb{Z}/N\mathbb{Z})^2, E[N])/H$. Then we have the following proposition

**Proposition 3.4.** *Let $k$ be a field of characteristic $p$ and $H \subset GL_2(\mathbb{Z}/N\mathbb{Z})$. Suppose that $p$ does not divide $N$. Then every non-cuspidal point $x \in X_H(k)$ is defined by an elliptic curve $E$ over $k$ with a level $H$ structure.*

The absolute Galois group $G_k$ for a field $k$ also acts on the points of $X_H(\overline{k})$. Then the points in $X_H(k)$ are fixed under the action of $G_k$. In particular this means that we get an action of $G_k$ on the pairs $E/k$ and level $H$ structure, and that $G_k$ preserves the isomorphism classes. $G_k$ acts on the level $N$ structure $\alpha$ via $E[N]$. Recall that in Chapter 1 we obtained that the action on $E[N]$ is described with the representation $\rho_{E,N} : G_k \to \mathrm{Aut}(E[N]) \cong GL_2(\mathbb{Z}/N\mathbb{Z})$. Then we have that the action of $G_k$ on the set of level $N$ structures can be described with the $\rho_{E,N}(G_k)$ orbits of level $N$ structures. So if $G_k$ fixes the isomorphism classes then the $\rho_{E,N}(G_k)$ orbit of level $N$ structure $\alpha$ must be contained in the $H$ orbit of $\alpha$. And thus we get that $\rho_{E,N}(G_k) \subseteq g^{-1}Hg$ for some $g \in GL_2(\mathbb{Z}/N\mathbb{Z})$.

### 3.2.2 $j$-map

Recall that the $j$-map from $X(1)$ to $\mathbb{P}^1(\mathbb{C})$ is the analytic isomorphism given by $\tau \mapsto j(\mathbb{C}/\Lambda_\tau)$, with $\mathbb{C}/\Lambda_\tau$ being the elliptic curve defined by the lattice $\Lambda_\tau$. For the modular curve $X(n)$ we have the $j$-map given by

$$j : X(n) \to X(1) \to \mathbb{P}^1 \tag{3.3}$$

where the first map is the natural projection, which is then followed by the usual $j$-map. Let $\varphi : \mathbb{Q}(j) \to \mathbb{Q}(X(N))$ induce map of function fields. This map is just the inclusion so we have $\varphi(\mathbb{Q}(j)) = \mathbb{Q}(j)$. Then the degree of $j$ is given by $\deg j = [\mathbb{Q}(X(N)) : \varphi(\mathbb{Q}(j))]$. As $\mathbb{Q}(X(N))/\mathbb{Q}(j)$ is a Galois extension we have that the degree of it is equal to $|GL_2(\mathbb{Z}/N\mathbb{Z})|$. As $-I$ is in $H$, we get that the map $X(N) \to X(1) \cong \mathbb{P}^1$ factors through $X_H$, so we get the map

$$j : X(N) \to X_H \to \mathbb{P}^1$$

The map $X(N) \to X_H$ is given by mapping the point $x \in X(N)(k)$, corresponding to a isomorphism class of the pair $E/k$ and a level $N$ structure $\alpha$, to the point $y \in X_H(k)$ corresponding to the isomorphism class of the pair $E/k$ with level $H$ structure given by the $H$ orbit of $\alpha$. Then from this it is easy to see that $(E, \alpha)$ and $(E, \beta)$ map to the same point in $X_H$ if and only if $\alpha$ and $\beta$ are in the same $H$-orbit. This is then $|H|$ to one map, and thus gives that the degree of $X(N) \to X_H$ is $|H|$.

So then we get that the degree of the $j$-map for $X_H$, that is $j : X_H \to X(1) \cong \mathbb{P}^1$ is given by $|GL_2(\mathbb{Z}/N\mathbb{Z})|/|H| = [GL_2(\mathbb{Z}/N\mathbb{Z}) : H]$.

We may summarise the discussed properties of the quotient curve $X_H$ in to the following statement as given in [2].

**Proposition 3.5.** *Let $H \subset GL_2(\mathbb{Z}/n\mathbb{Z})$, $H_0 = H \cap SL_2(\mathbb{Z}/n\mathbb{Z})$ with det : $H \to (\mathbb{Z}/n\mathbb{Z})^\times$ surjective and $-I \in H$. Then*

1. *The curve $X_H = X(n)/H_0$ is defined over $\mathbb{Q}$.*
2. *A non-cuspidal point of $X_H(\mathbb{Q})$ corresponds to elliptic curve $E$ over $\mathbb{Q}$ with*

$$\mathit{Gal}(\mathbb{Q}(E[n])/\mathbb{Q}) \subseteq g^{-1}Hg$$

   *for some $g \in GL_2(\mathbb{Z}/n\mathbb{Z})$.*

3. *The $j$-map $j : X_H \to \mathbb{P}^1$ defines a morphism of degree $[GL_2(\mathbb{Z}/n\mathbb{Z}) : H]$ over $\mathbb{Q}$.*

From this it follows that to describe the modular curve parametrising elliptic curves with the 2-torsion in the 3-torsion field it suffices to find the subgroup $H$.

## 3.3 Modular curve $X'(6)$

We want to find the curve $X(n)/H$ to parametrise elliptic curves $E/\mathbb{Q}$ with $\mathbb{Q}(E[2]) \subseteq \mathbb{Q}(E[3])$. We have a natural choice $n = 6$, as both 2- and 3-torsion points are contained in the 6-torsion points.

By definition the curve $X(6)$ is given by $\mathbb{H}^* \setminus \Gamma(6)$. From Theorem 2.15 and that $X(N)$ is a moduli space we have that $X(6)$ is a smooth curve over Spec$\mathbb{Z}[1/6]$. We also know that the function field of $X(6)$ is given by $K_6 = \mathbb{C}(j, E_j[6])$. The function field $K_6$ can be used to get the explicit equation for $X(6)$, this was done by Ishida in [6]. The approach uses the generators $t$ and $s$ of $K_6$ to get a polynomial $F_6(X, Y) \in \mathbb{Z}[\zeta_6][X, Y]$ with $F_6(s, t) = 0$, and this polynomial is $Y^3 - X^2 + 1$ and it gives the curve $X(6)$. The method given in [6] works for $X(N)$ with $N \geq 6$. There exist other approaches to computing the equation for a modular curve $X(N)$, for example in [18] Yang uses more analytic approach with the $\eta$-function to get the defining equations for the modular curves. One can also consider the genus of $X(6)$, it is known to be 1 and this is easy to see from its defining equation.

Let $H \subset GL_2(\mathbb{Z}/6\mathbb{Z})$ with det : $H \to (\mathbb{Z}/6\mathbb{Z})^\times$ surjective and $-I \in H$. Then the quotient curve $X(6)/H$ defines a modular curve of level 6. We denote this modular curve by $X'(6)$.

### 3.3.1 Group $H$ for $X'(6)$

Recall that we have the following diagram of field extensions

$$\begin{tikzcd}
& \mathbb{Q}(E[6]) \arrow[dl, dash] \arrow[dr, dash] & \\
\mathbb{Q}(E[2]) \arrow[dr, dash] & & \mathbb{Q}(E[3]) \arrow[dl, dash] \\
& \mathbb{Q} &
\end{tikzcd}$$

It follows from the Galois theory for finite extensions that as $\mathbb{Q}(E[6])/\mathbb{Q}$ is a Galois extension, then so are $\mathbb{Q}(E[6])/\mathbb{Q}(E[2])$ and $\mathbb{Q}(E[6])/\mathbb{Q}(E[3])$. The Galois groups of $\mathbb{Q}(E[6])/\mathbb{Q}(E[2])$ and $\mathbb{Q}(E[6])/\mathbb{Q}(E[3])$ correspond to normal subgroups of $\text{Gal}(\mathbb{Q}(E[6])/\mathbb{Q})$. Then by Galois theory $\mathbb{Q}(E[2]) \subseteq \mathbb{Q}(E[3])$ if and only if $\text{Gal}(\mathbb{Q}(E[6])/\mathbb{Q}(E[3])) \subseteq \text{Gal}(\mathbb{Q}(E[6])/\mathbb{Q}(E[2]))$.

For non-cuspidal points of a level 6 modular curve $X'(6)$, we have that the elliptic curves $E$ associated to the points satisfy $\text{Gal}(\mathbb{Q}(E[6])/\mathbb{Q}) \subseteq g^{-1}Hg$ by Proposition 3.5. Then for $\text{Gal}(\mathbb{Q}(E[6])/\mathbb{Q}(E[3])) \subseteq \text{Gal}(\mathbb{Q}(E[6])/\mathbb{Q}(E[2]))$ to hold, the subset of $g^{-1}Hg$ fixing points of order 3 must be contained in the subset of $g^{-1}Hg$ fixing points of order 2.

So we want to find $H \subseteq GL_2(\mathbb{Z}/6\mathbb{Z})$ with $\det H = (\mathbb{Z}/6\mathbb{Z})^\times$ and $-I \in H$, and satisfying the above condition. We also know that $H$ should give a curve parametrising non-Serre curves defined in Chapter 1. Recall that we have the condition $E$ is not a Serre curve if and only if there exists a prime $\ell \geq 5$ with $\rho_{E,\ell}(G_\mathbb{Q}) \subsetneq GL_2(\mathbb{Z}/\ell\mathbb{Z})$, or $[\rho_{E,36}(G_\mathbb{Q}), \rho_{E,36}(G_\mathbb{Q})] \subsetneq [GL_2(\mathbb{Z}/36\mathbb{Z}), GL_2(\mathbb{Z}/36\mathbb{Z})]$. In [1] it was shown that this is implies that $H$ must be the image of a maximal subgroup $G$ in $GL_2(\mathbb{Z}/36\mathbb{Z})$ for the map $\pi_{36,6} : GL_2(\mathbb{Z}/36\mathbb{Z}) \to GL_2(\mathbb{Z}/6\mathbb{Z})$ with $G$ satisfying $\det G = (\mathbb{Z}/36\mathbb{Z})^\times$, $[G, G] \subsetneq [GL_2(\mathbb{Z}/36\mathbb{Z}), GL_2(\mathbb{Z}/36\mathbb{Z})]$ and for all $d \in \{2, 3\}$ $\pi_{36,d}(G) = GL_2(\mathbb{Z}/d\mathbb{Z})$. From this it then follows that $H$ is a index 6 subgroup of $GL_2(\mathbb{Z}/6\mathbb{Z})$.

Define $\mathcal{N} \subset GL_2(\mathbb{Z}/3\mathbb{Z})$ as the subgroup given by

$$\mathcal{N} = \{\begin{pmatrix} x & -y \\ y & x \end{pmatrix} : x^2 + y^2 \equiv 1 \bmod 3\} \sqcup \{\begin{pmatrix} x & y \\ y & -x \end{pmatrix} : x^2 + y^2 \equiv -1 \bmod 3\} \tag{3.4}$$

$\mathcal{N}$ is the only index 6 normal subgroup in $GL_2(\mathbb{Z}/3\mathbb{Z})$. There is an exact sequence

$$1 \to \mathcal{N} \to GL_2(\mathbb{Z}/3\mathbb{Z}) \xrightarrow{\theta} GL_2(\mathbb{Z}/2\mathbb{Z}) \to 1 \tag{3.5}$$

The map $\theta : GL_2(\mathbb{Z}/3\mathbb{Z}) \to GL_2(\mathbb{Z}/2\mathbb{Z})$ is a surjective group homomorphism. The existence of $\theta$, and hence the existence of (3.5), is purely group theoretic. Also this then explain why there are no other coprime integers $n$ and $m$ satisfying $\mathbb{Q}(E[n]) \subseteq \mathbb{Q}(E[m])$ as we do not have a surjective map between the groups $GL_2(\mathbb{Z}/m\mathbb{Z}) \to GL_2(\mathbb{Z}/n\mathbb{Z})$.

Using the Chinese remainder theorem the graph of $\theta$ can be viewed as a subgroup of $GL_2(\mathbb{Z}/6\mathbb{Z})$.

Set $H$ to be the graph of $\theta$, i.e.

$$H = \{(g_2, g_3) \in GL_2(\mathbb{Z}/2\mathbb{Z}) \times GL_2(\mathbb{Z}/3\mathbb{Z}) : \theta(g_3) = g_2\} \tag{3.6}$$

Clearly $-I$ is in $H$. Note that $H$ is not a normal subgroup of $GL_2(\mathbb{Z}/6\mathbb{Z})$.

Let $E$ be an elliptic curve associated to a non-cuspidal point of $X'(6)$. Then the groups $\mathrm{Gal}(\mathbb{Q}(E[6])/\mathbb{Q}(E[3]))$ and $\mathrm{Gal}(\mathbb{Q}(E[6])/\mathbb{Q}(E[2]))$ are contained in some subgroups of $g^{-1}Hg$.

$\mathrm{Gal}(\mathbb{Q}(E[6])/\mathbb{Q}(E[2]))$ fixes the 2-torsion elements. Let $G_2 \subseteq g^{-1}Hg$ be the elements fixing 2-torsion, then $G_2$ must have $g_2 = \mathrm{id}$. Moreover $\theta(g_3) = \mathrm{id}$ implies that $G_2$ is a conjugate of $\{\mathrm{id}\} \times \mathcal{N}$. This is a normal subgroup, and thus $G_2 = \{\mathrm{id}\} \times \mathcal{N}$.

Similarly let $G_3 \subseteq g^{-1}Hg$ be the elements fixing 3-torsion, then $G_3$ must have $g_3 = \mathrm{id}$. Then it follows that $g_2 = \theta(\mathrm{id}) = \mathrm{id}$, too. Thus $G_3 = \{\mathrm{id}\} \times \{\mathrm{id}\}$.

Clearly $G_3 \subseteq G_2$, which implies that

$$\mathrm{Gal}(\mathbb{Q}(E[6])/\mathbb{Q}(E[3])) \subseteq \mathrm{Gal}(\mathbb{Q}(E[6])/\mathbb{Q}(E[2]))$$

Hence $\mathbb{Q}(E[2]) \subseteq \mathbb{Q}(E[3])$.

This shows that for the elliptic curves given by the non-cuspidal points of $X'(6)(\mathbb{Q})$ the condition $\mathrm{Gal}(\mathbb{Q}(E[6])/\mathbb{Q}) \subseteq g^{-1}Hg$ for some $g \in GL_2(\mathbb{Z}/n\mathbb{Z})$ is equivalent to $\mathbb{Q}(E[2]) \subseteq \mathbb{Q}(E[3])$.

There are other subgroups $G$ of $GL_2(\mathbb{Z}/6\mathbb{Z})$ that give a modular curve $X(6)/G$ that can parametrise elliptic curves with $\mathbb{Q}(E[2]) \subseteq \mathbb{Q}(E[3])$, but then they do not have non-abelian 2-torsion for every curve and hence not the curves we are interested in.

### 3.3.2 More on $X'(6)$

Studying the map $X'(6) \to X(1)$ gives further information on the curve $X'(6)$, in particular we can find the genus and cusps of $X'(6)$. The map is given as the natural projection in the

$j$-map. Thus from Proposition 3.5 (3) we know that it has degree 6.

We may use the Riemann-Hurwitz formula to compute the genus of the curve. The formula is given for a morphism between curves $\phi : C_1 \to C_2$ with degree $d$, and let $g(C_1)$ and $g(C_2)$ denote the genus of each curve, then

$$2g(C_1) - 2 = d(2g(C_2) - 2) + \sum_{P \in C_1} (e_P - 1) \tag{3.7}$$

where $e_P$ is the ramification index at $P$. So in our case we know that $g(X(1)) = 0$ and $d = 6$, then the formula becomes

$$2g(X'(6)) = -10 + \sum_{P \in X'(6)} (e_P - 1)$$

The ramification index is 1 for all but finitely many points, so now we would like to compute the index for those points in $X'(6)$ where the map is ramified. $X'(6) \to X(1)$ is part of the $j$-map, so then the points have same ramification index as $j$. The only point where $e_P$ is not 1 are the points correspnding to elliptic curves with $j$-invariant 0 or 1728, and at $\infty$. The ramification indices for these points can be computed and they are 3,2 and 6 respectively. See [12] for the computation details. Hence we get that $\sum_{P \in X'(6)} (e_P - 1) = (3-1)(2-1)(6-1) = 10$ and $g(X'(6)) = 0$.

The cusps of $X'(6)$ are given by the preimage of the cusps in $X(1)$. It is known that $X(1)$ has only one cusp, $\infty$. As $\infty$ has ramification index 6 for the map $X'(6) \to X(1)$, and the degree of the map is also 6 we have that the preimage of $\infty$ contains only one point. Therefore $X'(6)$ has only one cusp.

Cusps in a modular curve are by definition orbits in $\mathbb{P}^1(\mathbb{Q})$, so we have that the absolute Galois group $G_{\mathbb{Q}}$ acts on them. The curve $X'(6)$ only has one cusp, so it must be fixed under the action of $G_{\mathbb{Q}}$ and hence it is a rational point on the curve.

We are interested in the elliptic curves parametrised by this curve $X'(6)$ and one way to describe both the curve and the elliptic curves it parametrises is to find an explicit expression for the $j$-map. First step in this would be to find the function field $\mathbb{Q}(X'(6))$ for $X'(6)$. From earlier sections we know that it is the fixed field of $\mathbb{Q}(j, E_j[6])$ under the action of $H$. Moreover as $X'(6)$ has genus 0, the function field has one generator and can be written as $\mathbb{Q}(t)$ for some uniformizer $t$.

The uniformizer $t$ has degree 1, and as all the other maps can be written as polynomials in $t$ with rational coefficients we have that $j$ is a polynomial of degree 6 in $t$. Viewing $j$ as the modular invariant we know that it can be expressed as $1728f$, where $f$ is a modular function of degree 6 on $X'(6)$, which then implies that the coefficients of the polynomial in $t$ must be multiples of 1728.

Supposing that one can compute the function field $\mathbb{Q}(X'(6))$ explicitly, then a uniformizer $t$ can be found with the aid of computational software. And then it follows that if one knows $t$ one can compute the polynomial for $j$. The values of the coefficients may vary depending on the choice of $t$. So then with the right choice of $t$, one should get the following result

**Theorem 3.6** ([1], Theorem 1.4)**.** *There exists a uniformizer $t : X'(6) \to \mathbb{P}^1$ such that $j = 2^{10}3^3t^3(1-4t^3)$ where $j : X'(6) \to \mathbb{P}^1$ is the $j$-map.*

We know from section 3.3.1 that a non-cuspidal point $x \in X'(6)(\mathbb{Q})$ corresponds to an isomorphism class of an elliptic curve $E$ over $\mathbb{Q}$ satisfying $\mathbb{Q}(E[2]) \subseteq \mathbb{Q}(E[3])$. For the curve $E$ we also have $j(E) = j(x)$, so the above theorem is equivalent to the following given in the introduction.

**Theorem 3.7** (Brau and Jones, 2014)**.** *Let $E$ be an elliptic curve over $\mathbb{Q}$. Then $E$ is isomorphic over $\overline{\mathbb{Q}}$ to an elliptic curve $E'$ satisfying $\mathbb{Q}(E'[2]) \subseteq \mathbb{Q}(E'[3])$ if and only if $j(E) = 2^{10}3^3t^3(1-4t^3)$ for some $t \in \mathbb{Q}$.*

Unfortunately we were not able to do the explicit computations given above to verify the theorems. The suggested approach for computations arises naturally from studying the background theory, nevertheless there are likely to be also other possible approaches to the computation that can give the desired explicit result.

# References

[1] J. Brau and N. Jones. *Elliptic Curves with the 2-torsion contained in the 3-torsion field.* Proc. Amer. Math. Soc. **144** (2016), no. 3, 925-936.

[2] A.C. Cojocaru, D. Grant and N. Jones. *One-parameter families of elliptic curves over $\mathbb{Q}$ with maximal Galois representations*, Proc. Lond. Math. Soc. **103**, no. 3 (2011), 645-675.

[3] P. Deligne and M. Rapoport. *Les schemas de modules de courbes elliptiques.* in Modular Functions of One Varaible II, Lecture notes in Mathematics **349** (1973) 143-316.

[4] F. Diamond and J. Shurman. *A First Course in Modular Forms.* Graduate Texts in Mathematics 228, Springer, New York, 2005.

[5] J. Harris and I. Morrison. *Moduli of curves.* Graduate Texts in Mathematics 187, Springer, New York, 1998.

[6] N. Ishida. *Generators and equations for modular function fields of principal congruence subgroups*, Acta Arithmetica **LXXXV.3** (1998), 197-207.

[7] J. Jin. *Homogeneous division polynomials for Weierstrass elliptic curves*, arXiv:1303.4327 [math.AG].

[8] N. Jones, *Almost all elliptic curves are Serre curves*, Trans. Amer. Math. Soc. **362** (2010), 1547-1570.

[9] N. Katz and B. Mazur. *Arithmetic Moduli of Elliptic Curves.* Ann. Math. Studies **108**. Princeton University Press, Princeton, NJ, 1985.

[10] B. Mazur. *Rational points on modular curves.* in Lecture Notes in Math. 601, Springer, New York, 1977, 107-148.

[11] Mumford. *Curves and their Jacobians.* University of Michigan Press, 1975.

[12] K. Ribbet and W. Stein. *Modular Forms, Hecke Operators, and Modular Abelian Varieties.* University of Washington, 2003.

[13] J-P. Serre. *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques.* Invent. Math. **15**(1972), 259-331.

[14] J-P. Serre. *Abelian l-adic representations and elliptic curves.* Benjamin, 1968.

[15] G. Shimura. *Introduction to the arithmetic theory of automorphic forms.* Publications of the Mathematical Society of Japan 11, Princeton University Press, Princeton, 1971.

[16] J. Silverman. *Arithmetic of Elliptic Curves.* Graduate Texts in Mathematics 106, Springer, New York, 1986.

[17] G. Wiese. *Galois representations* (notes). <http://math.uni.lu/∼wiese/notes/GalRep.pdf> (June 2016).

[18] Y. Yang. *Defining equations of modular curves.* Advances in Mathematics **204**(2006), 481-508.