# Congruences of Elliptic Curves

**Zexiang Chen**

**Clare College**

**University of Cambridge**

**This dissertation is submitted for the degree of**

*Doctor of Philosophy*

**January 27, 2016**

## Abstract

Let $E$ be an elliptic curve over $\mathbb{Q}$ and $n$ be a positive integer. We study the families of elliptic curves which have the same mod $n$ Galois representations as $E$. In particular, we compute the equations for the modular curves $X_E(n)$ for $n = 6, 8, 10, 12$ which parametrise the families of elliptic curves that are $n$-congruent to $E$. These curves are twists of the modular curves $X(n)$ which parametrise families of elliptic curves with full level $n$ structure. Searching for rational points on the curves $X_E(n)$ enables us to find non-isogenous pairs of elliptic curves which are $n$-congruent.

Using the equations for $X_E(n)$, we compute the equations for the modular diagonal quotient surface $Z_{n,\epsilon}$ for some $n$. Searching for rational curves on the these surfaces enables us to find infinitely many pairs of non-isogenous $n$-congruent elliptic curves. Kani and Schanz determined the classification type of these surfaces. In particular, when $n \leq 12$ and $\epsilon = 1$, the surfaces $Z_{n,1}$ are either rational, elliptic K3 or elliptic surfaces. Based on this observation, they made the conjecture that there are infinitely many pairs of non-isogenous elliptic curves which are $n$-congruent to each other when $n \leq 12$. Our work, together with the work previously done by other people, shows that there are infinitely many pairs of non-isogenous $n$-congruent elliptic curves for each $n \leq 12$.

We also compute $X_E^r(n)$ for some values of $r \in (\mathbb{Z}/n\mathbb{Z})^*$ with $r$ not a square in $(\mathbb{Z}/n\mathbb{Z})^*$. Points on these curves correspond to elliptic curves $F$ which are $n$-congruent to $E$ with some conditions on the Weil Pairings depending on $r$.

## Introduction

Let $E$ be an elliptic curve over $\mathbb{Q}$. The $n$-torsion subgroup $E[n]$ of $E$ is a $G_{\mathbb{Q}}$-module. This thesis studies the mod $n$ Galois representation $G_{\mathbb{Q}} \to \mathrm{Aut}(E[n])$. The research topic is motivated by the following applications of congruences of elliptic curves

1. Mazur [M] asked whether there are any pair of non-isogenous elliptic curves with the same mod 7 representation. Kraus and Oesterle [KO] answered this question by giving an explicit example of such pairs. Halberstadt and Kraus [HK] later showed that there are actually infinitely many non-isogenous pairs of 7-congruent elliptic curves. Motivated by Mazur's question, Kani and Schanz [KS] studied the geometry of the modular diagonal quotient surfaces $Z_{n,\epsilon}$ that parametrise pairs of $n$-congruent elliptic curves. In particular, when $n \leq 12$ and $\epsilon = 1$ these surfaces are either rational, elliptic K3 or elliptic surfaces. This prompted them to conjecture that for any $n \leq 12$ there are infinitely many pairs of $n$-congruent non-isogenous elliptic curves over $\mathbb{Q}$. We prove this conjecture in the thesis.

2. Kani and Schanz [KS] determined the classification type of the modular diagonal quotient surfaces. We give explicit the equations for some of the surfaces.

3. Poonen, Schaefer and Stoll [PSS] used 7-congruence as one ingredient in their study of the Diophantine equation $x^2 + y^3 = z^7$.

4. It was observed by Cremona and Mazur [CM] that if elliptic curves $E$ and $F$ are $n$-congruent then the Mordell-Weil group of $F$ can sometimes be used to explain elements of the Tate-Shafarevich group of $E$.

We give a list of the previous results in this research area done by others

1. For $n \leq 5$, Rubin and Silverberg [RS1], [S1] gave explicit formulae for the families of elliptic curves parametrised by the modular curves $X_E(n)$ . Fisher [F1], [F2] used invariant method to give explicit formulae for families of elliptic curves parametrised by the modular curves $X_E^{\pm}(n)$.

2. For $n = 6$, Rubin and Silverberg [RS2] computed the equation for $X_E(6)$ and Roberts [R1] gave families of elliptic curves parametrsied by $X_E(6)$. They gave infinitely many non-isogenous pairs of elliptic curves which are 6-congruent. We compute the equation for $X_E^-(6)$ in this thesis.

3. For $n = 7$, Halberstadt and Kraus [HK] computed the equation for $X_E(7)$ and Poonen, Schaefer and Stoll [PSS] computed the equation for $X_E^-(7)$. They gave infinitely many non-isogenous pairs of elliptic curves which are 7-congruent.

4. For $n = 9$, Fisher [F4] computed the equations for $X_E^{\pm}(9)$ and the equations for the modular diagonal quotient surfaces $Z_{9,\pm 1}$. He then gave infinitely many non-isogenous pairs of elliptic curves which are 9-congruent.

5. For $n = 11$, Fisher [F3] computed the equations for $X_E^{\pm}(11)$ and the equations for the modular diagonal quotient surfaces $Z_{11,\pm 1}$. He then gave infinitely many non-isogenous pairs of elliptic curves which are 11-congruent.

Therefore, to verify Kani's conjecture, we focus on the cases $n = 8, 10, 12$ in this thesis.

In Section 1, we give some background and preliminary knowledge. Most materials in this section can be found in [S]. We list our main theorems at the end of the section.

In Section 2, we recall the equations of the classical modular curves $X(n)$ for $n \leq 6$. Using these we work out the equations for $X(n)$ when $n = 8, 10, 12$. The equations of $X(n)$ when $n = 8, 10, 12$ can also be found in [Y], using different methods. We require the forgetful map $X(n) \to X(n/2)$ when $n = 8, 10, 12$ and so we work out the function field of $X(n)$, as an extension of the function field of $X(n/2)$ for $n = 8, 10, 12$ in Section 2.

In Section 3, we recall the equations for the twists $X_E^r(n)$ when $n \leq 5$ and $r \in (\mathbb{Z}/n\mathbb{Z})^*$. In particular, we recall a lemma which shows that $X_E^3(4)$ can be identified with $X_E(4)$. This is one of the important observations we use in Section 6 to compute $X_E^3(8)$ and $X_E^7(8)$.

In Section 4, we compute the equations for $X_E(6)$ and $X_E^-(6)$. Rubin and Silverberg already gave an equation for $X_E(6)$ and Roberts gave the forgetful map $X_E(6) \to X_E(3)$ for most elliptic curves $E$ except for some curves with specific $j$-invariant. We use a different method to compute $X_E(6)$ based on the fact that geometrically the function field of $X_E(6)$ is an $S_3$ extension of the function field of $X_E(3)$. We give (simpler) forgetful map $X_E(6) \to$

$X_E(3)$ for every elliptic curve $E$. We then extend our method to work out the equations for $X_E^-(6)$ and show that there are infinitely many non-isogenous pairs of elliptic curves which are reversely 6-congruent.

In Section 5, we extend our method in Section 4 to work out the equations for $X_E(10)$. Despite the fact that the equations are not simple, we manage to find infinitely many pairs of non-isogenous elliptic curves which are 10-congruent.

In Section 6, we compute the equations for $X_E^r(8)$ for $r = 1, 3, 5, 7$. We use the observation that geometrically the function field of $X_E^r(8)$ is an $(\mathbb{Z}/2\mathbb{Z})^3$ extension of the function field $X_E(4)$. Together with a few computations we give the equations for $X_E(8)$ and $X_E^5(8)$. The equations for $X_E^3(8)$ and $X_E^7(8)$ are obtained from some cocycle computations. We also give the forgetful map $X_E^r(8) \to X_E^{\bar{r}}(4)$ for each $r = 1, 3, 5, 7$ where $\bar{r} = r \bmod 4$.

In Section 7, we adapt our method in Section 6 to compute the equations for $X_E(12)$. We use the observation that geometrically the function field of $X_E(12)$ is an $(\mathbb{Z}/2\mathbb{Z})^3$ extension of the function field $X_E(6)$. This method again allows us to write down the forgetful map $X_E(12) \to X_E(6)$ and hence we compute the forgetful map $X_E(12) \to X_E(3)$ which enables us read off the family of elliptic curves parametrised by $X_E(12)$.

In Section 8, we compute the modular diagonal quotient surfaces $Z_{n,\epsilon}$ for $n = 7, 8$. Some of these surfaces are elliptic K3 or elliptic surfaces. We give Weierstrass form of these surfaces and in particular we show that each of these surfaces has a rational section over $\mathbb{Q}$.

In Section 9, we give some numerical examples of pairs of non-isogenous $n$-congruent elliptic curves and list a few further questions which can be considered in this research topic.

**Acknowledgement**

I am grateful for all the support I have received when researching and writing up this dissertation. I would like to thank my supervisor, Dr. Tom Fisher, who has given me remarkable advice, guidance and patience for my research project.

I would like to thank the Math fellows in Clare College, Dr.Maciej Dunajski and Professor Andrew Thomason, for their support during the seven years I have spent in Clare College. I would also like to thank the friends I have made through mathematics: Cangxiong Chen, Si Cheng, Ildar Gaisin, Zhi Jin, Yukako Kezuka, Jack Lamplugh, Guolong Li, Zhenlin Low, Adam Morgan and Monique van Beek. I would also like to thank my friend Rong Zhang for some games of DotA2 when I had a hard time with Math.

Finally, I would like to thank my parents for their financial support.

## Declaration

I hereby declare that this thesis is the result of my work and includes nothing which is the outcome of work done in collaboration. I also declare that this thesis is not substanially the same as any other that I have submitted for a degree of diploma at any other university.

**For the time I spent with Mathematics**

余情悦其淑美兮，纠舒窈之琼衣
彷微光之瑶碧兮，惧芳华之我欺

思娥姣之攸远，揽明月而要之
追隔世之流年，步秋桑而约词

盼康河以长伴兮，收暮霞之朝夕
采延延之玉莲兮，拨磬弦之涟漪

意白首之游梦兮，归苍颜之有期
念已往之不顾兮，掩生岁之尘熙

# Contents

# 1 Background and Preliminary knowledge

## 1.1 Notation

Let $K$ be a perfect field of characteristic not equal to $2, 3$ or $5$. Throughout, $E/K$ will be an elliptic curve defined over $K$ with point at infinity $O$. The field $K$ will usually be $\mathbb{Q}$ and we fix a short Weierstrass equation

$$E : y^2 = x^3 + ax + b$$

with $a, b \in K$. We will write $\Delta_E := -16(4a^3 + 27b^2)$ for its discriminant. We will denote the absolute Galois group $\mathrm{Gal}(\bar{K}/K)$ by $G_K$.

Let $n$ be a positive integer which is not divisible by the characteristic of $K$. We will write $E[n]$ for the kernel of multiplication-by-$n$ map

$$[n] : E \to E.$$

If $E$ is an elliptic curve, write

$$\rho_{E,n} : G_K \to \mathrm{Aut}(E[n]) \subset \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$$

for the (isomorphism class of the) mod $n$ representation of $E$. So $G_K$ can naturally be embedded as a subgroup of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ in terms of its action on the $n$-torsion points. Explicitly, if $s \in G_K$ and we fix $\{P, Q\}$ a basis for $E[n]$, then there exist $s_{ij} \in \mathbb{Z}/n\mathbb{Z}, i, j \leq 2$ with $s_{11}s_{22} - s_{12}s_{21}$ coprime to $n$, such that

$$s(P) = s_{11}P + s_{21}Q, \quad s(Q) = s_{12}P + s_{22}Q.$$

Then we define $\rho_{E,n}(s)$ to be the matrix

$$\begin{pmatrix} s_{11} & s_{12} \\ s_{21} & s_{22}. \end{pmatrix}.$$

We will use the following convention. For any $P, Q \in E[n]$ and

$$\alpha = \begin{pmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{pmatrix},$$

we write

$$\alpha P = \alpha_{11} P + \alpha_{21} Q, \quad \alpha Q = \alpha_{12} P + \alpha_{22} Q.$$

Throughout, we will denote the set of $n$th roots of unity by $\mu_n$. We will write $\mathrm{PSL}_2(\mathbb{Z}/n\mathbb{Z}) = \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})/\{\pm I\}$ and $\mathrm{PGL}_2(\mathbb{Z}/n\mathbb{Z}) = \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})/\Lambda$ where $\Lambda$ is the set of scalar matrices.

For each $n \geq 3$ we will write $\zeta_n$ for a fixed $n$th root of unity. For convention, we write $i$ for $\zeta_4$.

## 1.2 Isogenies

We give the definition and basic properties of isogenies. Details can be found in [S, Chapter 3].

**Definition 1.2.1.** *Let $E_1$ and $E_2$ be elliptic curves. An isogeny from $E_1$ to $E_2$ is a non-zero morphism*

$$\phi : E_1 \to E_2 \text{ satisfying } \phi(O) = O.$$

*Two elliptic curves $E_1$ and $E_2$ are isogenous if there is an isogeny from $E_1$ to $E_2$ with $\phi(E_1) \neq \{O\}$.*

We state the following basic properties

**Theorem 1.2.2.** *(i) Let $\phi : E_1 \to E_2$ be an isogeny. Then*

$$\phi(P+Q) = \phi(P) + \phi(Q) \text{ for all } P, Q \in E_1.$$

*So $\phi$ is a group homomorphism.*

*(ii) Let $E$ be an elliptic curve and let $\Phi$ be a finite subgroup of $E$. There are a unique elliptic curve $E'$ and a separable isogeny*

$$\phi : E \to E' \text{ satisfying } \ker \phi = \Phi.$$

*(iii) Let $\phi : E_1 \to E_2$ be a nonconstant isogeny of degree $m$. Then there exists a unique isogeny*

$$\hat{\phi} : E_2 \to E_1 \text{ satisfying } \hat{\phi} \circ \phi = [m] \text{ on } E_1.$$

*The map $\hat{\phi}$ is called the* **dual isogeny** *of $\phi$. Moreover, $\hat{\hat{\phi}} = \phi$ and so*

$$\phi \circ \hat{\phi} = [m] \text{ on } E_2.$$

**Proof.** See [S, Chapter 3]. □

## 1.3 The Weil Pairing

Let $E$ be an elliptic curve. There is a bilinear pairing

$$e_m : E[m] \times E[m] \to \mu_m$$

called the Weil pairing, on each elliptic curve. Proper definition and construction of the Weil pairing can be found in [S, Chapter 3]. We list the main properties of the Weil pairing.

**Proposition 1.3.1.** *The Weil pairing $e_m$ has the following properties:*

*(i) It is bilinear.*

*(ii) It is alternating.*

*(iii) It is non-degenerate*

*(iv) It is Galois equivariant.*

*(v) It is compatible:*

$$e_{mm'}(S,T) = e_m([m']S,T) \text{ for all } S \in E[mm'] \text{ and } T \in E[m].$$

**Proof.** See [S, Chapter 3]. □

The following is an immediate consequence

**Corollary 1.3.2.** *There exists points $S, T \in E[m]$ such that $e_m(S,T)$ is a primitive $m$th root of unity. In particular, if $E[m] \subset E(K)$, then $\mu_m \subset K^*$.*

**Proof.** See [S, Chapter 3, Corollary 8.1]. □

Let $\phi : E_1 \to E_2$ be a non constant isogeny and $\hat{\phi} : E_2 \to E_1$ be its dual isogeny. The following proposition says that $\phi$ and $\hat{\phi}$ are adjoint with respect to the Weil pairing.

**Proposition 1.3.3.** *For all $m$-torsion points $S \in E_1[m]$ and $T \in E_2[m]$,*

$$e_m(S, \hat{\phi}(T)) = e_m(\phi(S), T).$$

**Proof.** See [S, Chapter 3]. $\square$

In particular, since $\hat{\phi}$ is surjective, if we write $Q = \hat{\phi}T$ then

**Corollary 1.3.4.** *For all $m$-torsion points $S, Q \in E_1[m]$,*

$$e_m(S, Q)^r = e_m(\phi(S), \phi(Q))$$

*where $r = \deg(\phi)$.*

**Proof.** Write $Q = \hat{\phi}$ and so by Theorem 1.2.2(iii) $rT = \phi(Q)$. The result then follows from Proposition 1.3.1(i). $\square$

Here is another straightforward corollary which we will use later.

**Corollary 1.3.5.** *For each $n \geq 2$, $P, Q \in E[n]$ and $\alpha \in \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$, we have*

$$e_n(P, Q)^{\det \alpha} = e_n(\alpha P, \alpha Q).$$

**Proof.** This follows from Proposition 1.3.1(i) and (ii). $\square$

## 1.4 Modular Curves

A modular curve $Y(\Gamma)$ is a Riemann surface, or the corresponding algebraic curve, constructed as a quotient of the complex upper half-plane $\mathfrak{H}$ by the action of a congruence subgroup $\Gamma$ of the modular group $\mathrm{SL}_2(\mathbb{Z})$. Let $X(\Gamma)$ denote the compactification of $Y(\Gamma)$, which is obtained by adding finitely many points (called the cusps of $\Gamma$) to this quotient. The points of a modular curve parametrise isomorphism classes of elliptic curves, together with some additional structure depending on the group $\Gamma$.

Let $n$ be a positive integer. The most common examples of modular curves are $X(n), X_0(n)$ and $X_1(n)$ associated with the subgroups of $\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$

$$\Gamma(n) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, d \equiv 1 \bmod n \text{ and } b, c \equiv 0 \bmod n \right\},$$

$$\Gamma_0(n) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : c \equiv 0 \bmod n \right\},$$

$$\Gamma_1(n) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, d \equiv 1 \bmod n \text{ and } c \equiv 0 \bmod n \right\}.$$

We start with the modular interpretations of these modular curves. Fix an $n^{\text{th}}$ root of unity $\zeta_n$.

**Definition 1.4.1.** *Each point on $Y_0(n)$ corresponds to an isomorphism class $(E, C)$ where $E$ is an elliptic curve and $C$ is a subgroup of $E[n]$ of order $n$. Equivalently, each point corresponds to an isomorphism class $(E, \phi)$ where $\phi : E \to E'$ is a cyclic isogeny of degree $n$ for some elliptic curve $E'$.*

**Definition 1.4.2.** *Each point on $Y_1(n)$ corresponds to an isomorphism class $(E, P)$ where $E$ is an elliptic curve and $P$ is a point on $E$ with exact order $n$.*

**Definition 1.4.3.** *Each point on $Y(n)$ corresponds to an isomorphism class $(E, P, C)$ where $E$ is an elliptic curve, $P$ is a point on $E$ with exact order $n$ and $C$ is a subgroup of $E[n]$ of order $n$ such that $P$ and $C$ generate $E[n]$. By Proposition 1.3.1, there is a unique point $Q \in C$ such that $e_n(P, Q) = \zeta_n$. Therefore we will also identify points on $Y(n)$ with triples $(E, P, Q)$.*

**Lemma 1.4.4.** *Equivalently, $Y(n)$ parametrises isomorphism classes $(E, \phi)$ where $E$ is an elliptic curve and*

$$\phi : \mathbb{Z}/n\mathbb{Z} \times \mu_n \to E[n]$$

*is an isomorphism with the property that $e_n(\phi(a_1, \zeta_1), \phi(a_2, \zeta_2)) = \zeta_2^{a_1}/\zeta_1^{a_2}$, where $\zeta_1, \zeta_2$ are $n^{th}$ roots of unity.*

**Proof.** Given $(E, P, C)$, define $\phi$ by $\phi(a, \zeta) = aP + Q$ for the unique $Q \in C$ such that $e_n(P, Q) = \zeta$. Conversely, given $(E, \phi)$, define $P = \phi(1, 1)$ and $Q = \phi(0, \zeta)$ where $\zeta$ is a primitive $n^{\text{th}}$ root of unity. Then take $C = \langle Q \rangle$. $\square$

This interpretations above allow one to give purely algebraic definitions of modular curves, without reference to complex numbers, and, moreover, prove that modular curves are defined either over $\mathbb{Q}$, or a cyclotomic field. Write $X_0(n), X_1(n), X(n)$ for the compactifications of $Y_0(n), Y_1(n), Y(n)$ respectively.

### 1.4.1 Total Spaces

Let $n \geq 3$. We will describe the elliptic surface associated to the universal elliptic curves above $X(n)$. References can be found in [S1]. There is a quasi-projective surface $W(n)$ defined over $\mathbb{Q}$, with a projection morphism

$$\pi_n : W(n) \to Y(n)$$

and a zero-section $Y(n) \to W(n)$, both defined over $\mathbb{Q}$, with $n^2$ sections defined over $\bar{\mathbb{Q}}$ of order dividing $N$, and such that the fibers of $\pi_n$ correspond to the triples $(E, P, C)$ classified by $Y(n)$. The variety $W(n)$ can be viewed as the universal elliptic curve with level structure as above. Let $W(n)[n]$ denote the $n^2$ sections of $\pi_n$ of order dividing $n$, viewed as a $G_{\mathbb{Q}}$-module. Roughly speaking, $W(n)$ can be viewed as an elliptic curve over the function field of $X(n)$ and the $n$-torsion points of $W(n)$ are defined over the function field of $X(n)$.

### 1.4.2 Action of Projective Special Linear Groups

Recall that $\mathrm{PSL}_2(\mathbb{Z}/n\mathbb{Z}) = \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})/\{\pm I\}$. There is a natural action of $\mathrm{PSL}_2(\mathbb{Z}/n\mathbb{Z})$ on the modular curves $X(n)$. Let $(E, P, C)$ be a point on $Y(n)$ and let $Q$ be a generator of the cyclic subgroup $C$. Then for each $\alpha = \begin{pmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$, define

$$\alpha P = \alpha_{11} P + \alpha_{21} Q, \quad \alpha Q = \alpha_{12} P + \alpha_{22} Q.$$

Then

$$\alpha \circ (E, P, C) \colon= (E, \alpha P, \langle \alpha Q \rangle)$$

is another point on $Y(n)$ because $e_n(P, Q) = e_n(\alpha P, \alpha Q)$ by Corollary 1.3.5. When $\alpha = -I$, the action is trivial because $(E, P, Q) = (E, -P, -Q)$ as $[-1]$ is an automorphism of $E$. Therefore we have an action of $\mathrm{PSL}_2(\mathbb{Z}/n\mathbb{Z})$ on $Y(n)$.

### 1.4.3 The Forgetful Maps

For each $n$, the forgetful map $\chi_n : X(n) \to X(1)$ is the quotient map by the action of $\mathrm{PSL}_2(\mathbb{Z}/n\mathbb{Z})$. More generally, for each $m|n$, there is a natural surjective reduction

$$\mathrm{PSL}_2(\mathbb{Z}/n\mathbb{Z}) \to \mathrm{PSL}_2(\mathbb{Z}/m\mathbb{Z})$$

and let $H_{n,m}$ be the kernel of this map. $H_{n,m}$ is a normal subgroup of $\mathrm{PSL}_2(\mathbb{Z}/n\mathbb{Z})$ and acts on $X(n)$. The forgetful map corresponding to $H_{n,m}$ is denoted by $\chi_{m,n} : X(n) \to X(m)$. Roughly speaking, the forgetful map $\chi_{n,m}$ is to keep the level $m$ structures of the elliptic curves parametrised by $X(n)$.

For each $n$, let $K_n(L)$ be the function field of $X(n)$ over $L$ where $L$ is a field of characteristic not equal to 2 or 3. Then we have the following theorem

**Theorem 1.4.5.** *The extension $K_n(\mathbb{C})/K_1(\mathbb{C})$ is Galois with Galois group $\mathrm{PSL}_2(\mathbb{Z}/n\mathbb{Z})$.*

**Proof.** See [R, Theorem 1]. □

Here is an immediate corollary by taking the quotients

**Corollary 1.4.6.** *For each $m|n$, $K_n(\mathbb{C})/K_m(\mathbb{C})$ is Galois with Galois group $H_{n,m}$. In particular, if $m > 2$ is even and $n = 2m$ then $H_{n,m} \cong (\mathbb{Z}/2\mathbb{Z})^3$ and if $m$ is odd and $n = 2m$ then $H_{n,m} \cong S_3$.*

**Proof.** The first statement is clear. If $m > 2$ is even and $n = 2m$, then

$$H_{2m,m} = \ker(\mathrm{PSL}_2(\mathbb{Z}/2m\mathbb{Z}) \to \mathrm{PSL}_2(\mathbb{Z}/m\mathbb{Z}))$$

is generated by

$$M_1 = \begin{pmatrix} 1+m & 0 \\ 0 & 1+m \end{pmatrix},\ M_2 = \begin{pmatrix} 1 & 0 \\ m & 1 \end{pmatrix},\ M_3 = \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix}.$$

Since $M_1, M_2, M_3$ commute with each other and they all have order 2, we conclude that $H_{8,4} \cong (\mathbb{Z}/2\mathbb{Z})^3$.

If $m$ is odd and $n = 2m$ then $H_{2m,m}$ is generated by

$$M_2 = \begin{pmatrix} 1 & 0 \\ m & 1 \end{pmatrix},\ M_3 = \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix}.$$

In this case, $M_2$ and $M_3$ do not commute and we have a group of order 6. So it must be $S_3$. Note that in the second case $M_1$ is not an element in $\mathrm{PSL}_2(\mathbb{Z}/2m\mathbb{Z})$ because the determinant is $(1+m)^2$ which is not coprime to $2m$. $\square$

We state the following standard fact about the ramified points under the forgetful map $\chi_n$.

**Proposition 1.4.7.** *Let $n \geq 1$. The forgetful map $\chi_n : X(n) \to X(1)$ is ramified at the points above $\infty, 0, 1728$ with ramification index $n, 3, 2$ respectively.*

## 1.5 Twists of Modular Curves

### 1.5.1 Twists of Curves

We introduce the definition of twists of curves and give some basic properties. Details can be found in [S, Chapter 10.2].

**Definition 1.5.1.** *Let $C/K$ be a smooth projective curve. The isomorphism group of $C$, denoted by $Aut(C)$, is the group of $\bar{K}$-isomorphism from $C$ to itself. We denote the subgroup of $Aut(C)$ consisting of isomorphism defined by $K$ by $Aut_K(C)$.*

**Definition 1.5.2.** *A twist of $C/K$ is a smooth curve $C'/K$ that is isomorphic to $C$ over $\bar{K}$. We treat two twists as equivalent if they are isomorphic over $K$. The set of twists of $C/K$, modulo $K$-isomorphism, is denoted by $Twist(C/K)$.*

Let $C'$ be a twist of $C$ and so there is an isomorphism $\phi : C' \to C$ defined over $\bar{K}$. To measure the failure of $\phi$ to be defined over $K$, we consider the map

$$\xi : G_{\bar{K}/K} \to \mathrm{Aut}(C), \quad \xi(s) = ({}^s\phi)\phi^{-1}$$

where ${}^s\phi = s \circ \phi \circ s^{-1}$. It turns out that

**Theorem 1.5.3.** *(i) $\xi$ is a 1-cocycle, i.e.,*

$$\xi_{s_1 s_2} = ({}^{s_1}\xi_{s_2})\xi_{s_1}, \quad \textit{for all } s_1, s_2 \in G_K.$$

*The associated cohomology class in $H^1(G_K, Aut(C))$ is denoted by $\{\xi\}$.*

*(ii) The cohomology class $\{\xi\}$ is determined by the $K$-isomrphism class of $C'$ and is independent of the choice of $\phi$. We thus obtain a natural map*

$$Twist(C/K) \to H^1(G_K, Aut(C)).$$

*(iii) The map in (ii) is a bijection.*

*More generally, if $X$ is a quasiprojective variety over $K$ then the above construction gives a one-to-one correspondence*

$$Twist(X/K) \to H^1(G_K, Aut(X)).$$

**Proof.** For (i), (ii) and (iii)See [S, Chapter 10]. For the general case, see [W]. □

**Remark** Note that Silverman used different notation in [S]. He used Isom instead of Aut for the automorphism group and he used right action whereas we use left action, so that we have

$$^{s_1 s_2}\phi =^{s_1} (^{s_2}\phi).$$

In practise, it is often not easy to compute the inverse of the map

$$\text{Twist}(C/K) \to H^1(G_K, \text{Aut}(C)).$$

### 1.5.2 Families of Elliptic Curves With The Same Mod $n$ Representations

**Definition 1.5.4.** *Let $n \geq 1$ be a positive integer. We say two elliptic curves $E_1/K$ and $E_2/K$ are n-congruent if $E_1[n]$ and $E_2[n]$ are isomorphic as $G_K$-modules. More precisely, there exists an isomorphism*

$$\phi : E_1[n] \to E_2[n]$$

*such that $s \circ \phi \circ s^{-1} = \phi$ for all $s \in G_K$.*

If $\{P, Q\}$ is a basis for $E_1[n]$ then $\{\phi(P), \phi(Q)\}$ is a basis for $E_2[n]$. Moreover, there exists $r \in (\mathbb{Z}/n\mathbb{Z})^*$ such that $e_n(P, Q)^r = e_n(\phi(P), \phi(Q))$. Note $r$ is independent of the choice of the basis for $E_1[n]$ by Proposition 1.3.1. Therefore we make the following definition

**Definition 1.5.5.** *Let $n \geq 1$ be a positive integer and $r \in (\mathbb{Z}/n\mathbb{Z})^*$. We say $E_1/K$ is n-congruent to $E_2/K$ with power $r$ if there exists a $G_K$-equivariant isomorphism*

$$\phi : E_1[n] \to E_2[n]$$

*such that $e_n(P,Q)^r = e_n(\phi(P),\phi(Q))$. We say $E_1$ is directly congruent to $E_2$ if $r=1$ and reversely congruent to $E_2$ if $r \equiv -1$ mod $n$.*

**Remark** In fact we only need to consider $r \in (\mathbb{Z}/n\mathbb{Z})^*$ mod squares because $[k] : E \to E$ induces an automorphism of $E[n]$ which switches the Weil pairing to the power of $k^2$, for any $k$ coprime to $n$.

**Remark** If $E_1, E_2$ are $r$ isogenous where $r$ is coprime to $n$, then the isogeny from $E_1$ to $E_2$ induces a Galois equivariant isomorphism between $E_1[n]$ and $E_2[n]$. This means that $E_1$ and $E_2$ are $n$-congruent. In particular, by Corollary 1.3.4, $E_1$ is $n$-congruent to $E_2$ with power $r$. Therefore, we are mostly interested in the pairs of $n$-congruent elliptic curves which are non-isogenous.

Now fix an elliptic curve $E : y^2 = x^3 + ax + b$. We want to find the formulae for the families of elliptic curves which are $n$-congruent to $E$. More precisely, the following theorem shows that the families of such curves are parametrised by twists of modular curves.

**Theorem 1.5.6.** *Let $E/K$ be an elliptic curve and $V = E[n]$, viewed as $G_K$-module. Define a bilinear pairing $\langle , \rangle$ on $\mathbb{Z}/n\mathbb{Z} \times \mu_n$ by*

$$\langle (a_1, \zeta_{n,1}), (a_2, \zeta_{n,2}) \rangle = \zeta_{n,1}^{a_2} / \zeta_{n,2}^{a_1}.$$

*Now fix an isomorphism $\phi : \mathbb{Z}/n\mathbb{Z} \times \mu_n \to V$ such that the above pairing is compatible with the Weil pairing under $\phi$. Then the cocycle*

$$\tau \mapsto ({}^{\tau}\phi^{-1})\phi$$

*take values in $Aut(\mathbb{Z}/n\mathbb{Z} \times \mu_n, \langle , \rangle)$ which is the set of automorphisms of $\mathbb{Z}/n\mathbb{Z} \times \mu_n$ which preserve the bilinear pairing.*

*For each $\psi \in Aut(\mathbb{Z}/n\mathbb{Z} \times \mu_n, \langle , \rangle)$, $\psi$ acts on $Y(n)$ by $\psi(F, \rho) = (F, \rho\psi)$ where $(F, \rho)$ is a point on $Y(n)$ by Lemma 1.4.4. So it induces an action on $Y(n)$ and $W(n)$ and so we have natural maps*

$$Aut(\mathbb{Z}/n\mathbb{Z} \times \mu_n, \langle , \rangle) \to Aut(W(n)),\ Aut(\mathbb{Z}/n\mathbb{Z} \times \mu_n, \langle , \rangle) \to Aut(X(n)).$$

*Thus, the cocycle above induces cocycles $c$ and $c_0$, taking values in $Aut(W(n))$ and $Aut(X(n))$ respectively. Then by Theorem 1.5.3, we obtain a surface $W$ and a curve $X$, and induced* *isomorphisms $\psi$ and $\psi_0$ defined over $\bar{K}$ together with a projection map $\pi : W \to X$ defined over $K$ such that the following diagram commutes*

$$\begin{array}{ccc} W & \xrightarrow{\psi} & W(n) \\ \Big\downarrow{\scriptstyle \pi} & & \Big\downarrow{\scriptstyle \pi_n} \\ X & \xrightarrow{\psi_0} & X(n) \end{array}$$

**Proof.** See [S1, Page 449]. □

The curve $X$ in the theorem above is denoted by $X_E(n)$, which parametrises families of elliptic curves which are directly congruent to $E$. In general, a similar method (replace the bilinear pairing we start with by its $r$th power) can be used to prove that the families of elliptic curves which are $n$-congruent to $E$ with power $r$ is parametrised by a modular curve $X_E^r(n)$, which is a twist of $X(n)$. We often write $X_E^-(n)$ for $X_E^{n-1}(n)$.

The above theorem also tells us that each point on $X_E^r(n)$ corresponds to a pair $(F, \phi_F)$ up to $K$-isomorphism where $F$ is an elliptic curve and $\phi_F : E[n] \to F[n]$ is Galois equivariant and $e_n(P,Q)^r = e_n(\phi_F(P), \phi_F(Q))$ for all $P, Q \in E[n]$.

**Remark** The above theorem shows that $X_E^r(n)$ exists, for each $r \in (\mathbb{Z}/n\mathbb{Z})^*$. However, in practise it is not easy to compute the equation for $X_E^r(n)$ if we follow the proof of the theorem, because in general it is not easy to compute explicitly the inverse of the bijection

$$\mathrm{Twist}(C/K) \to H^1(G_K, \mathrm{Aut}(C)).$$

## 1.6 Modular Diagonal Quotient Surfaces

Recall that $\mathrm{PSL}_2(\mathbb{Z}/n\mathbb{Z})$ acts on $X(n)$. Then $\mathrm{PSL}_2(\mathbb{Z}/n\mathbb{Z}) \times \mathrm{PSL}_2(\mathbb{Z}/n\mathbb{Z})$ acts on the product surface $X(n) \times X(n)$ and hence so does the graph subgroup $\Delta_\epsilon = \{(g, \alpha_\epsilon(g)) : g \in \mathrm{PSL}_2(\mathbb{Z}/n\mathbb{Z})\}$ associated to the automorphism $\alpha_\epsilon \in \mathrm{Aut}(\mathrm{PSL}_2(\mathbb{Z}/n\mathbb{Z}))$ which is defined by conjugation by the element $Q_\epsilon = \begin{pmatrix} \epsilon & 0 \\ 0 & 1 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. Kani and Schanz call the resulting quotient surface $Z_{n,\epsilon} = (X(n) \times X(n))/\Delta_\epsilon$ a modular diagonal quotient surface. Details can be found in [KS].

The modular diagonal quotient surfaces occur naturally as the compactifications of the moduli spaces associated to certain moduli problems. Indeed, by using the modular interpretation of $Y(n) = X(n)\backslash\{\text{cusps}\}$, each point on $(Y(n) \times Y(n))/\Delta_\epsilon$ corresponds to a triplet

$(E_1, E_2, \psi)$ where $E_1$ and $E_2$ are elliptic curves and $\psi : E_1[n] \cong E_2[n]$ is a Galois equivariant isomorphism such that

$$e_n(P, Q) = e_n(\psi(P), \psi(Q))^{\epsilon}, \text{ for all } P, Q \in E_1[n].$$

Furthermore, by Theorem 1.5.3, the surface $Z_{n,\epsilon}$ has a canonical model over $K$.

Kani and Schanz determined the classification type of the surfaces $Z_{n,r}$ and we list the classification in the following table (see [KS, Theorem 4])

| The Surface $Z_{n,r}$ | Classification |
|---|---|
| $Z_{n,r}, n \leq 5$ | Rational |
| $Z_{n,1}, n = 6, 7, 8$ | Rational |
| $Z_{6,5}, Z_{7,3}, Z_{8,r}(r = 3, 5), Z_{9,1}, Z_{12,1}$ | Elliptic K3 |
| $Z_{8,7}, Z_{9,2}, Z_{10,1}, Z_{10,3}, Z_{11,1}$ | Elliptic Surface With Kodaira dimension 1 |
| $Z_{11,2}, Z_{12,r}(r \neq 1), Z_{n,r}(n \geq 13)$ | General Type |

The purpose of studying the modular diagonal quotient surfaces is to find infinitely many pairs of non-isogenous elliptic curves over $\mathbb{Q}$ which are $n$-congruent. Indeed if we find a genus zero curve with a rational point or an elliptic curve with positive rank on the surface, then we obtain infinitely many pairs of elliptic curves which are $n$-congruent. The remaining issue is to make sure that all but finitely many of these points correspond to non-isogenous curves. To do this, we refer to the following theorem of Mazur [M].

**Theorem 1.6.1.** *There are only finitely many $l$ such that cyclic $l$-isogeny over $\mathbb{Q}$ exists.*

Recall that the points on $Y_0(l)$ correspond to pairs $(E, \phi)$ such that $\phi : E \to E'$ is an $l$-isogeny for some curve $E'$. Then $X_0(l)$ corresponds to a curve on the surface $Z_{n,l}$ for each $n$ coprime to $l$. If $C$ is a curve on $Z_{n,l}$, then since $X_0(l)$ is irreducible, the intersection of $C$ and $X_0(l)$ is either $X_0(l)$ or a finite set of points.

The above theorem of Mazur shows that $Y_0(l)$ has a rational point over $\mathbb{Q}$ for only finitely many $l$. Therefore, if we find a curve $C$ of genus zero with a rational point or genus one with positive rank on $Z_{n,l}$, and a rational point $P \in C$ which corresponds to a pair of non-isogenous elliptic curves, then we obtain infinitely many pairs of non-isogenous elliptic curves which are $n$-congruent. We also use our equations for $X_E^r(n)$ to construct birational models of $Z_{n,r}$ in Section 8. We will see in Section 8 that one usual trick to obtain a birational model of $Z_{n,r}$ is to set $b = a$ in the equations for $X_E^r(8)$ where we assume $E : y^2 = x^3 + ax + b$, and treat $a$ as a variable.

## 1.7 Statement of The Main Theorems

We now state the main theorems we are going to prove. Let $K$ be a field of characteristic not equal to $2, 3$ or $5$ and $E : y^2 = x^3 + ax + b$ be an elliptic curve over $K$.

**Theorem 1.7.1.** *The curve $X_E^5(6)$ is birational to the curve $C \subset \mathbb{A}^3_{x,y,v}/K$ with equations $f = g = 0$ where*

$$\begin{aligned} f =& y^2 - \Delta_E(ax^4 + 6bx^3 - 2a^2x^2 - 2abx + (-a^3/3 - 3b^2)), \\ g =& v^3 - (36ax^2 + 12a^2)v + 216bx^3 - 144a^2x^2 - 216abx - (16a^3 + 216b^2) \\ & + 27y(64abx + 96b^2)/\Delta_E. \end{aligned}$$

**Theorem 1.7.2.** *The curve $X_E(8) \subset \mathbb{P}^4_{x_0,x_1,x_2,x_3,x_4}/K$ has equations $f_1 = g_1 = h_1 = 0$ where*

$$\begin{aligned} f_1 &= -ax_3^2 + 2x_1x_3 + x_2^2 + 2x_4^2, \\ g_1 &= -2ax_2x_3 - bx_3^2 + 2x_1x_2 + 2x_0x_4, \\ h_1 &= -2bx_2x_3 + x_1^2 - x_0^2 + ax_4^2, \end{aligned}$$

**Theorem 1.7.3.** *The curve $X_E^3(8) \subset \mathbb{P}^4_{x_0,x_1,x_2,x_3,x_4}/K$ has equations $f_3 = g_3 = h_3 = 0$ where*

$$\begin{aligned} f_3 &= x_0^2 + 2bx_1x_3 + ax_2^2 - 6bx_2x_4 - a^2x_4^2, \\ g_3 &= 2x_0x_1 + 2ax_1x_3 + 4ax_2x_4 - bx_3^2 - 18bx_4^2, \\ h_3 &= 2x_0x_3 - x_1^2 + x_2^2 + ax_3^2 + 3ax_4^2. \end{aligned}$$

**Theorem 1.7.4.** *The curve $X_E^5(8) \subset \mathbb{P}^4_{x_0,x_1,x_2,x_3,x_4}/K$ has equations $f_5 = g_5 = h_5 = 0$ where*

$$\begin{aligned} f_5 &= -ax_3^2 + 2x_1x_3 + x_2^2 - (5ax_4^2 - 3x_0^2), \\ g_5 &= -2ax_2x_3 - bx_3^2 + 2x_1x_2 - (2ax_0x_4 - 6bx_4^2), \\ h_5 &= -2bx_2x_3 + x_1^2 - (4a^2x_4^2 - 4ax_0^2 - 2bx_0x_4). \end{aligned}$$

**Theorem 1.7.5.** *The curve* $X_E^7(8) \subset \mathbb{P}^4_{x_0,x_1,x_2,x_3,x_4}/K$ *has equations* $f_7 = g_7 = h_7 = 0$ *where*

$$\begin{aligned} f_7 &= 3x_0^2 + ax_4^2 - ax_3^2 + 2x_1x_3 + x_2^2, \\ g_7 &= 4ax_0x_4 + 6bx_4^2 - 2ax_2x_3 - bx_3^2 + 2x_1x_2, \\ h_7 &= ax_0^2 + 6bx_0x_4 - a^2x_4^2 - 2bx_2x_3 + x_1^2. \end{aligned}$$

We fix the parametrisations of the curves $X_E(3), X_E^2(3), X_E(4)$ and $X_E^3(4)$ in Section 3. Using these we specify the forgetful maps from the level six structure to the level three structure and the forgetful maps from the level eight structure to the level four structure. This allows us to write down the families of elliptic curves parametrised by $X_E^r(6)$ where $r = 1, 5$ and $X_E^r(8)$ where $r = 1, 3, 5, 7$.

We give explicit equations of the modular diagonal quotient surfaces $Z_{8,r}, r = 1, 3, 5, 7$ by the following theorems.

**Theorem 1.7.6.** *The surface* $Z_{8,1}$ *is a rational surface. The family of pairs of elliptic curves (up to isomorphism) parametrised by* $Z_{8,1} \cong \mathbb{A}^2_{p,q}$ *is* $(E^{\{p,q\}}, F^{\{p,q\}})$ *where* $E^{\{p,q\}} : y^2 = x^3 + a(p,q) + b(p,q)$ *with*

$$\begin{aligned} a(p,q) &= -p^3 - 3p^2q^2 + 9pq^2 + p, \\ b(p,q) &= p^4q - p^4 + 2p^3q^3 - 6p^3q - 9p^2q^3 - 9p^2q^2 - p^2q - p^2 \end{aligned}$$

*and* $F^{\{p,q\}}$ *is the curve which corresponds to the point* $(x_0^{\{p,q\}} : x_1^{\{p,q\}} : x_2^{\{p,q\}} : x_3^{\{p,q\}} : 1)$ *on* $X_{E^{\{p,q\}}}(8)$ *where*

$$\begin{aligned} x_1^{\{p,q\}} &= \frac{1}{2}(-p^2 - 4pq^2 - 2p + 9q^2 + 1), \\ x_2^{\{p,q\}} &= q, \\ x_3^{\{p,q\}} &= \frac{1}{p}, \\ x_0^{\{p,q\}} &= \frac{1}{2}(-p^2 - 4pq - 9q^2 - 1). \end{aligned}$$

**Theorem 1.7.7.** *The surface* $Z_{8,3}$ *is birational to the elliptic K3 surface*

$$y^2 = x^3 + (3T^2+1)x^2 + (-16T^6 + 76T^2 - 16)x + (-32T^8 + 240T^6 + 472T^4 + 484T^2 + 20).$$

**Theorem 1.7.8.** *The surface $Z_{8,5}$ is birational to the elliptic K3 surface*

$$y^2 = x^3 + (-18T^2 - 38)x^2 + (-2916T^6 + 5913T^4 - 3546T^2 + 1225)x.$$

**Theorem 1.7.9.** *The surface $Z_{8,7}$ is birational to the elliptic surface of Kodaira dimension one*

$$y^2 = x^3 + (8T^6 - 30T^4 + 28T^2 - 2)x^2 + (16T^{12} - 88T^{10} + 193T^8 - 212T^6 + 118T^4 - 28T^2 + 1)x.$$

For the case $n = 12$, we obtain the following result

**Theorem 1.7.10.** *The curve $X_E(12)$ is birational to the curve $C \subset \mathbb{A}^5_{X,Y,u_0,u_1,u_2}/\mathbb{Q}$ with equations $F = F_1 = F_2 = F_3 = 0$ where*

$$\begin{aligned}
F &= -X^2 + aXY^2 + 6bY^3 - 6aY^2 - 12,\\
F_1 &= (X^2 + 12X + 36) - (-au_2^2 + 2u_0u_2 + u_1^2),\\
F_2 &= (4aXY + 36bY^2 - 24aY) - (-2au_1u_2 - bu_2^2 + 2u_0u_1),\\
F_3 &= (8aX - 4a^2Y^2) - (-2bu_1u_2 + u_0^2).
\end{aligned}$$

We further show that

**Proposition 1.7.11.** *There are infinitely many pairs of non-isogenous elliptic curves over $\mathbb{Q}$ which are*

*(i) directly* 10*-congruent.*

*(ii) directly* 12*-congruent.*

*In particular, we have proved the following conjecture: For all $n \leq 12$, there exist infinitely many pairs of non-isogenous elliptic curves which are $n$-congruent.*

**Remark** For the cases $n = 12$, one could argue that the equations for $X_E(12)$ can be obtained by taking the fiber product of $X_E(3)$ and $X_E(4)$ over the $j$-line. But this leads to equations which are much messier than the ones we have found and it is very hard to search for rational points on the curve, as well as to find infinitely many pairs of non-isogenous elliptic curves which are 12-congruent. Therefore, we try to find the simplest equations as possible. The same comment should be made on the equations for $X_E^5(6)$.

# 2 Equations of Modular Curves $X(n)$

In this section we give a list of equations of modular curves $X(n)$ for several values of $n$ which we will need later. It is well-known that when $n \leq 5$, $X(n)$ has genus 0 and when $n \geq 7$, $X(n)$ has genus greater than 1. $X(6)$ has genus 1. We shall fix the following convention. Let $X(1) \cong \mathbb{A}^1_j$, then the family of elliptic curves parametrised by $X(1)$ is

$$y^2 = x^3 - \frac{27j}{j-1728}x + \frac{54j}{j-1728}.$$

## 2.1 Level $n$ Structure, $2 \leq n \leq 5$

Most of the results in this section can be found in Klein's *Lectures on the icosahedron* [K]. Let $n = 2, 3, 4, 5$.

**Definition 2.1.1.** *For each $n$, we define a polynomial $D \in \mathbb{Z}[u, v]$ associated to $n$,*

$$\begin{aligned} n &= 2 \qquad D = u(64u^2 - v^2) \\ n &= 3 \qquad D = -u(27u^3 + v^3) \\ n &= 4 \qquad D = uv(16u^4 - v^4) \\ n &= 5 \qquad D = uv(u^{10} - 11u^5v^5 - v^{10}) \end{aligned}$$

*Further, define*

$$c_4(u, v) = \frac{-1}{((\deg D) - 1)^2} \begin{vmatrix} \frac{\partial^2 D}{\partial u^2} & \frac{\partial^2 D}{\partial v^2} \\ \frac{\partial^2 D}{\partial u \partial v} & \frac{\partial^2 D}{\partial v^2} \end{vmatrix}$$

*and*

$$c_6(u, v) = \frac{1}{\deg c_4} \begin{vmatrix} \frac{\partial D}{\partial u} & \frac{\partial D}{\partial v} \\ \frac{\partial c_4}{\partial u} & \frac{\partial c_4}{\partial v} \end{vmatrix}.$$

**Theorem 2.1.2.** *For each $n$, the family of elliptic curves parametrised by $X(n) \cong \mathbb{P}^1_{[u:v]}$ is*

$$E_{n,[u:v]} : y^2 = x^3 - 27c_4(u, v)x - 54c_6(u, v).$$

*In particular, if $\zeta_n$ is a primitive $n$th root of unity, then*

*(i) each point on $Y(2) \cong \mathbb{P}^1_{[u:v]}$ corresponds to a triple $(E_{2,[u:v]}, P_2, C_2)$ where*

$$E_{2,[u:v]} : y^2 = x^3 - 27(192u^2 + v^2)x - 54(576u^2v - v^3),$$

$P_2 = (-6v, 0)$ *and* $C_2$ *is generated by* $Q_2 = (72u + 3v, 0)$.

*(ii) each point on on* $Y(3) \cong \mathbb{P}^1_{[u:v]}$ *corresponds to a triple* $(E_{3,[u:v]}, P_3, C_3)$ *where*

$$E_{3,[u:v]} : y^2 = x^3 - 27(-216u^3v + v^4)x - 54(5832u^6 - 540u^3v^3 - v^6),$$

$P_3 = (108u^2 - 36uv + 3v^2, -972u^3 + 324u^2v - 108uv^2)$ *and* $C_3$ *is generated by* $Q_3 = (-9b^2, (2\zeta_3 + 1)324u^3 + 12v^3)$.

*(iii) each point on on* $Y(4) \cong \mathbb{P}^1_{[u:v]}$ *corresponds to a triple* $(E_{4,[u:v]}, P_4, C_4)$ *where*

$$E_{4,[u:v]} : y^2 = x^3-27(256u^8+224u^4v^4+v^4)x-54(-4096u^{12}+8448u^8v^4+528u^4v^8-v^{12}),$$

$P_4 = (48u^4-144u^3v+72u^2v^2-36uv^3+3v^4, 1728u^5v-1728u^4v^2+864u^3v^3-432u^2v^4+108uv^5)$ *and* $C_4$ *is generated by* $Q_4 = (48u^4 - 15v^4, i(864u^4v^2 - 54v^6))$.

*(iv) each point on on* $Y(5) \cong \mathbb{P}^1_{[u:v]}$ *corresponds to a triple* $(E_{5,[u:v]}, P_5, C_5)$ *where*

$$\begin{aligned} E_{5,[u:v]} : y^2 &= x^3 - 27(u^{20} + 228u^{15}v^5 + 494u^{10}v^{10} - 228u^5v^{15} + v^{20})x \\ &- 54(-u^{30} + 522u^{25}v^5 + 10005u^{20}v^{10} + 10005u^{10}v^{20} - 522u^5v^{25} - v^{30}), \end{aligned}$$

$P_5 = (x_{5,1}, y_{5,1})$ *and* $C_5$ *is generated by* $Q_5 = (x_{5,2}, y_{5,2})$. *We will give the expressions of* $x_{5,1}, x_{5,2}, y_{5,1}, y_{5,2}$ *in the Appendix.*

**Proof.** For each $n$, the points $P_n, Q_n$ given above generate the $n$-torsion subgroup of $E_{n,[u:v]}$ and a direct computation shows that the Weil pairing $e_n(P_n, Q_n) = \zeta_n$ is satisfied. The degree of the composition

$$[u : v] \mapsto (E_{n,[u:v]}, P_n, Q_n) \mapsto j(E_{n,[u:v]})$$

is $\frac{12n}{6-n}$, which is the same as the size of $\mathrm{PSL}_2(\mathbb{Z}/n\mathbb{Z})$. Therefore, the map $[u : v] \mapsto (E_{n,[u:v]}, P_n, Q_n)$ has degree 1 and is an isomorphism. □

Note that the cusps of $X(n)$ are the points on $E_{n,[u:v]}$ such that $\Delta_{E_{n,[u:v]}} = 0$.

**Proposition 2.1.3.** *Take an affine coordinate* $[1 : v]$ *for* $X(3)$ *For each* $u \in Y(3)$, *the curve*

$$E_{3,[\frac{1}{3}:-v]} : y^2 = x^3 - 27(8v + v^4)x - 54(8 + 20v^3 - v^6)$$

*is isomorphic to the Hesse cubic*

$$A_v : X^3 + Y^3 + Z^3 = 3vXYZ.$$

**Proof.** The Hesse cubic is a genus one curve with a rational point $[X : Y : Z] = [0 : 1 : -1]$. Therefore it is isomorphic to its Jacobian

$$y^2 - 3vxy + 9y = x^3 + (-27v^3 - 27)$$

which is isomorphic to $E_{3,[\frac{1}{3}:-v]}$. □

The above proposition shows that we can also take $A_v$ to be the family of elliptic curves parametrised by $Y(3)$. Taking $[0 : 1 : -1]$ to be the identity point, we have a rational three torsion point $(-1, -1, 0)$ on $A_v$ and a $G_{\mathbb{Q}}$-invariant cyclic group of order 3 which does not contain $(-1, 1, 0)$, generated by $(0, \zeta_3, -1)$.

## 2.2 Level Six Structure

The result in this section can be found in [P]. As 2 is coprime to 3, we have $E[6] = E[2] \oplus E[3]$. Thus, specifying a rational 6-torsion point is the same as specifying a rational 2-torsion point and a rational 3-torsion point. In other words, $X(6)$ is the fiber product of $X(2)$ and $X(3)$ over the $j$-line. Based on this observation, we conclude

**Lemma 2.2.1.** *$X(6)$ is birational to the affine curve in $\mathbb{A}^2_{\sigma,\tau}$ with equation $2\sigma^2\tau^2 = \sigma + \tau$ and the forgetful map $X(6) \to X(3)$ is given by $(\sigma, \tau) \mapsto (2\sigma + \sigma^{-2})/3$ where we identify the family of elliptic curves parametrised by $Y(3)$ with $A_v$ in Proposition 2.1.3. In particular the family of elliptic curves parametrised by $Y(6)$ is*

$$E_{6,(\sigma,\tau)} : X^3 + Y^3 + Z^3 = 3(2\sigma + \sigma^{-2})XYZ.$$

**Proof.** The non-trivial two torsion points on $A_v$ are $(\lambda_i, \lambda_i, 1), i = 1, 2, 3$ where $\lambda_i, i = 1, 2, 3$ are roots of $2x^3 - 3vx^2 + 1 = 0$. Let $\sigma$ and $\tau$ be two (distinct) roots of this polynomial and so

$$\frac{2\sigma + \sigma^{-2}}{3} = \frac{2\tau + \tau^{-2}}{3} = v.$$

This implies $2\sigma + \sigma^{-2} = 2\tau + \tau^{-2}$ and so $2\sigma^2\tau^2 = \sigma + \tau$. Conversely, for each $(\sigma, \tau)$ satisfying $2\sigma^2\tau^2 = \sigma + \tau$, if $v = (2\sigma + \sigma^{-2})/3$ then $\sigma$ and $\tau$ are roots of $2x^3 - 3vx^2 + 1 = 0$.

Let $C$ be the curve with equation $2\sigma^2\tau^2 - \sigma - \tau = 0$. Since for each $v \in \mathbb{Q}$, $A_v$ has a rational 3-torsion point and a $G_{\mathbb{Q}}$-invariant cyclic subgroup of order 3, we have a rational 6-torsion point $P_6$ and a $G_{\mathbb{Q}}$-invariant cyclic subgroup $C_6$ of order 6 on $A_v$ for any $v = (2\sigma + \sigma^{-2})/3$ with $(\sigma, \tau) \in C/\mathbb{Q}$. Then the degree of the composition

$$C \to X(6) \to X(3), \quad (\sigma, \tau) \mapsto (A_{(2\sigma+\sigma^{-2})/3}, P_6, C_6) \mapsto (2\sigma + \sigma^{-2})/3$$

is 6. By Corollary 1.4.6, the degree of the forgetful map $\chi_{6,3} : X(6) \to X(3)$ is the size of $\mathrm{PSL}_2(\mathbb{Z}/2\mathbb{Z})$, which is 6. Therefore, the map $C \to X(6)$ has degree 1 and hence is an isomorphism. $\square$

**Corollary 2.2.2.** *$X(6)$ has equation $Y^2 = X^3 + 1$.*

**Proof.** This follows from a change of variable $X = 2\sigma$ and $Y = 4\sigma^2\tau - 1$, with inverse $\sigma = \frac{X}{2}, \tau = \frac{Y+1}{4\sigma^2}$. $\square$

**Corollary 2.2.3.** *The family of elliptic curves parametrised by $X(6)$ is*

$$E_{6,(X,Y)} : y^2 = x^3 - 27v(v^3 + 8)x - 54(-v^6 + 20v^3 + 8)$$

*where $(X, Y)$ is a point on $Y^2 = X^3 + 1$ and $v = (X + 4/X^2)/3$. The cusps of $X(6)$ are*

$$(0, \pm 1), (-\zeta_3, 0), (-\zeta_3^2, 0), (-1, 0), (2\zeta_3, \pm 3), (2\zeta_3^2, \pm 3), (2, \pm 3), O$$

*where $O$ is the point of infinity on $X(6) : Y^2 = X^3 + 1$.*

**Proof.** The first part follows from Proposition 2.1.3 and Corollary 2.2.2. The coordinates of cusps can be found by computing the discriminant of $E_{6,(X,Y)}$. $\square$

## 2.3 Level Eight Structure

We start with the family of elliptic curves parametrised by $X(4)$ in Theorem 2.1.2(iii),

$$E_{4,[u:v]} : y^2 = x^3 - 27(256u^8 + 224u^4v^4 + v^4)x - 54(-4096u^{12} + 8448u^8v^4 + 528u^4v^8 - v^{12}),$$

together with 4-torsion points $P_4$ and $Q_4$. We firstly compute the cusps of $X(4)$.

**Proposition 2.3.1.** *The cusps of $X(4)$ are $\pm\frac{1}{2}, 0, \infty, \pm\frac{i}{2}$.*

**Proof.** This follows from a direct computation of the discriminant of $E_{4,[u:v]}$. Note that the cusps are the points $[u : v]$ such that $\Delta_{E_{4,[u:v]}} = 0$. $\square$

For simplicity, we now take the affine coordinate with $v = 1$. and we consider the 8-division polynomial of $E_{4,[u:1]}$. In particular, if $x_1$ and $x_2$ are $x$-coordinates of any half point of $P_4$ and $Q_4$ respectively, then we have $f = g = 0$ where

$$\begin{aligned} f &= (x_1 - 48u^4 + 144u^3 - 72u^2 + 36u - 3)^4 \\ &\quad + 1296u(2u-1)^4(4u^2+1)(x_1 - 48u^4 - 72u^2 - 3)^2, \\ g &= (x_2 - 48u^4 + 15)^4 + 1296(16u^4 - 1)(x_2 + 96u^4 + 6)^2. \end{aligned}$$

By Section 1.4.3, the forgetful map $\chi_{8,4} : X(8) \to X(4)$ has degree 8 and the Galois group of the extension $K_8(\mathbb{C})/K_4(\mathbb{C})$ is the kernel $H_{8,4}$ of $\mathrm{PSL}_2(\mathbb{Z}/8\mathbb{Z}) \to \mathrm{PSL}_2(\mathbb{Z}/8\mathbb{Z})$, which is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^3$. This shows that the function field of $K_8(\mathbb{C})$ can be obtained from $K_4(\mathbb{C})$ by adjoining three square roots. This suggests that over $\mathbb{C}$, adjoining $x_1, x_2$ above is the same as adjoining three square roots. In fact, a direct computation shows that

$$K_8(L) = L(u, \sqrt{u^2 - 1/4}, \sqrt{-u}, \sqrt{u^2 + 1/4})$$

where $L = \mathbb{Q}(\mu_8)$. Therefore we obtain (affine) equations for $X(8) \subset \mathbb{A}^4_{u,X_1,X_2,X_3}/L$,

$$\begin{aligned} X_1^2 &= u^2 - 1/4, \\ X_2^2 &= -u, \\ X_3^2 &= u^2 + 1/4. \end{aligned}$$

The projective closure of this curve is a smooth curve of genus 5 and the family of elliptic curves parametrised by $X(8)$ is (as in Theorem 2.1.2(iii) with affine coordinate $v = 1$)

$$E_{8,(u,X_1,X_2,X_3)} : y^2 = x^3 - 27(256u^8 + 224u^4 + 1)x - 54(-4096u^{12} + 8448u^8 + 528u^4 - 1)$$

together with a $G_{\mathbb{Q}}$-equivariant point $P_8$ and a $G_{\mathbb{Q}}$-equivariant cyclic group generated by

$Q_8$ where $P_8 = (P_x, P_y), Q_8 = (Q_x, Q_y)$ and

$$\begin{aligned}
P_x &= -36(4X_3^5 + 4X_3^4 + 4X_3^3 + 2X_3^2 + X_3)X_2 + 48X_3^8 + 144X_3^7 + 144X_3^6 \\
&\quad + 72X_3^5 + 72X_3^4 + 36X_3^3 + 36X_3^2 + 18X_3 + 3, \\
P_y &= 108(16X_3^9 + 32X_3^8 + 32X_3^7 + 32X_3^6 + 24X_3^5 + 16X_3^4 + 8X_3^3 + 4X_3^2 \\
&\quad + X_3)X_2 - 1728X_3^{11} - 3456X_3^{10} - 4320X_3^9 - 3456X_3^8 - 2592X_3^7 \\
&\quad - 1728X_3^6 - 1296X_3^5 - 864X_3^4 - 540X_3^3 - 216X_3^2 - 54X_3, \\
Q_x &= -72\zeta_8^2 X_1X_2 + (72(\zeta_8^3 + \zeta_8)X_3^4 + 18(\zeta_8^3 + \zeta_8))X_1 + (72(\zeta_8^3 - \zeta_8)X_3^4 \\
&\quad - 18(\zeta_8^3 - \zeta_8))X_2 + 48X_3^8 - 15, \\
Q_y &= 432X_1X_2 + (864(-\zeta_8^3 + \zeta_8)X_3^8 + 432(\zeta_8^3 - \zeta_8)X3^4 + 162(\zeta_8^3 - \zeta_8))X_1 \\
&\quad + ((-864\zeta_8^3 - 864\zeta_8)X_3^8 + 432(-\zeta_8^3 - \zeta_8)X_3^4 + 162(\zeta_8^3 + \zeta_8))X_2 \\
&\quad + 1728\zeta_8^2X_3^8 - 108\zeta_8^2.
\end{aligned}$$

Therefore, we conclude that $(E_{8,(u,X_1,X_2,X_3)}, P_8, Q_8)$ is a point on $Y(8)$ and any point on $Y(8)$ has this form. Moreover, since we compute $X(8)$ as a cover of $X(4)$, we conclude that the forgetful map $\chi_{8,4} : X(8) \to X(4)$ is given by

$$(u, X_1, X_2, X_3) \mapsto u.$$

The following corollary gives a conclusion of our observations.

**Corollary 2.3.2.** *The forgetful map*

$$\chi_{8,4} : X(8) \to X(4), \quad (u, X_1, X_2, X_3) \mapsto u$$

*described above is only ramified above the cusps of $X(4)$ and each ramification point has ramification index 2. Consequently, each $X_j, j = 1, 2, 3$ above can be understood as a square root of a rational function on $X(4) \cong \mathbb{P}^1_{[u:1]}$ which has zeroes at two of the cusps of $X(4)$. In particular, we can pair up the cusps $P_1, \ldots, P_6$ of $X(4)$ so that the function field of $X(8)$ can be described as $K_8(L) = L(u, \sqrt{f_1}, \sqrt{f_2}, \sqrt{f_3})$ where*

$$div(f_1) = (P_1) + (P_2) - 2(\infty)$$

$$div(f_2) = (P_3) + (P_4) - 2(\infty)$$

$$div(f_3) = (P_5) + (P_6) - 2(\infty)$$

The group $\mathrm{PSL}_2(\mathbb{Z}/8\mathbb{Z})$ acts on $X(8)$ and we are now going to work out the action of a subgroup of it on $X(8)$. The group $H_{8,4}$ is the normal subgroup of $\mathrm{PSL}_2(\mathbb{Z}/8\mathbb{Z})$ such that the quotient map corresponding to the action of $H_{8,4}$ is the forgetful map $\chi_{8,4} : X(8) \to X(4)$ and $H_{8,4}$ is the kernel of $\mathrm{PSL}_2(\mathbb{Z}/8\mathbb{Z}) \to \mathrm{PSL}_2(\mathbb{Z}/4\mathbb{Z})$, which is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^3$.

**Lemma 2.3.3.** *Take generators $S_1, S_2, S_3$ for $H_{8,4}$ where*

$$S_1 = \begin{pmatrix} 1 & 4 \\ 4 & 1 \end{pmatrix}, S_2 = \begin{pmatrix} 3 & 4 \\ 4 & 3 \end{pmatrix}, S_3 = \begin{pmatrix} 1 & 0 \\ 4 & 1 \end{pmatrix}.$$

*Then the action of $H_{8,4}$ on $X(8)$ is given by*

$$\begin{aligned} S_1(u, X_1, X_2, X_3) =& (u, -X_1, X_2, -X_3), \\ S_2(u, X_1, X_2, X_3) =& (u, X_1, -X_2, X_3), \\ S_3(u, X_1, X_2, X_3) =& (u, X_1, X_2, -X_3). \end{aligned}$$

**Proof.** This follows from a direct computation of the coordinates of

$$P_8 + 4Q_8, \quad 4P_8 + Q_8, \quad 3P_8 + 4Q_8, \quad 4P_8 + 3Q_8.$$

□

## 2.4 Level Ten Structure

The result in this minor section is not very important in the sense that we will not use it to prove any of the main theorems. Nonetheless, we give a model of $X(10)$.

**Proposition 2.4.1.** *Let $L = \mathbb{Q}(\mu_{10})$. Then $X(10)$ is birational to the curve in $\mathbb{A}^3_{x,u,s}/L$ with equations $F = G = 0$ where*

$$\begin{aligned} F &= ux^3 - u^3x^2 + x + u^2, \\ G &= x^2u - 4xu^3 + s^2 - u^5, \end{aligned}$$

*with forgetful map $\chi_{10,5} : X(10) \to X(5)$ given by*

$$(x, s, u) \mapsto u.$$

*The family of elliptic curves parametrised by $X(10)$ is (the curve with the same equation in 2.1.2 (iv))*

$$\begin{aligned} E_{10,(x,s,u)} : y^2 &= x^3 - 27(u^{20} + 228u^{15} + 494u^{10} - 228u^5 + 1) \\ &- 54(-u^{30} + 522u^{25} + 10005u^{20} + 10005u^{10} - 522u^5 - 1), \end{aligned}$$

*together with non-trivial $G_{\mathbb{Q}}$-equivariant 2-torsion points $R_2 = (R_x, 0)$ and $T_2 = (T_x, 0)$ where*

$$\begin{aligned} R_x &= \frac{90u^5 - 45}{18u^5+1}s^4 + \frac{-504u^{10} - 306u^5 + 54}{18u^5+1}s^2 + \frac{468u^{15} + 858u^{10} + 216u^5 - 6}{18u^5+1}, \\ T_x &= \frac{27u^5 + 189}{72u^5+4}s^5 + \frac{-90u^5 + 45}{36u^5+2}s^4 + \frac{-135u^{10} - 990u^5 - 315}{72u^5+4}s^3 + \frac{252u^{10} + 153u^5 - 27}{18u^5+1}s^2 \\ &+ \frac{27u^{15} - 333u^{10} + 369u^5 + 36}{18u^5+1}s + \frac{-234u^{15} - 429u^{10} - 108u^5 + 3}{18u^5+1}. \end{aligned}$$

*Coordinates of the 5-torsion points of $E_{10,(x,s,u)}$ can be read off from Theorem 2.1.2(iv).*

**Proof.** The map $(x, s, u) \mapsto u$ has degree 6 which is the same as the size of $\mathrm{PSL}_2(\mathbb{Z}/2\mathbb{Z})$. By Theorem 2.1.2(iv) and Corollary 1.4.6, we conclude that $X(10)$ has equations $F = G = 0$ because the kernel of $\mathrm{PSL}_2(\mathbb{Z}/10\mathbb{Z}) \to \mathrm{PSL}_2(\mathbb{Z}/5\mathbb{Z})$ is isomorphic to $\mathrm{PSL}_2(\mathbb{Z}/2\mathbb{Z})$. $\square$

## 2.5 Level Twelve Structure

We will compute a model for $X(12)$ by using the equation for $X(6)$ in Section 2.2. Recall the family of elliptic curves parametrised by

$$X(6) : Y^2 = X^3 + 1$$

is

$$E_{6,(X,Y)} : y^2 = x^3 - 27v(v^3 + 8)x - 54(-v^6 + 20v^3 + 8).$$

Since $E[6] = E[2] \oplus E[3]$ and $E[12] = E[4] \oplus E[3]$, to get $X(12)$, we need to adjoin the coordinates of the 4-torsion points of $E_{6,(X,Y)}$. By Corollary 1.4.6, the Galois group of the extension $K_{12}(\mathbb{C})/K_6(\mathbb{C})$ is

$$H_{12,6} = \ker(\mathrm{PSL}_2(\mathbb{Z}/12\mathbb{Z}) \to \mathrm{PSL}_2(\mathbb{Z}/6\mathbb{Z})) \cong (\mathbb{Z}/2\mathbb{Z})^3.$$

So in theory we can obtain $K_{12}(\mathbb{C})$ as an extension of $K_6(\mathbb{C})$ by adjoining 3 square roots of rational functions on $X(6)$.

By looking at the 4-division polynomial of $E_{6,(X,Y)}$ and considering the $y$-coordinates of the 4-torsion points of $E_{6,(X,Y)}$, we conclude that

$$K_{12}(L) = K_6(L)(\sqrt{(Y+1)(Y-3)}, \sqrt{Y}, \sqrt{(Y-1)(Y+3)})$$

where $L = \mathbb{Q}(\mu_{12})$. Therefore, $X(12)$ is birational to a curve in $\subset A^5_{X,Y,u_1,u_2,u_3}/L$ with equations

$$\begin{aligned}
Y^2 &= X^3 + 1, \\
u_1^2 &= (Y+1)(Y-3), \\
u_2^2 &= Y, \\
u_3^2 &= (Y-1)(Y+3).
\end{aligned}$$

This is a curve of genus 25. Moreover,

**Proposition 2.5.1.** *The family of elliptic curves parametrised by $X(12)$ is*

$$E_{12,(X,Y,u_1,u_2,u_3)} : y^2 = x^3 - 27v(v^3+8)x - 54(-v^6 + 20v^3 + 8)$$

*where $v = (X + 4/X^2)/3$, together with a primitive $G_{\mathbb{Q}}$-equivariant 4-torsion point $R_4 = (R_x, R_y)$ and a $G_{\mathbb{Q}}$-equviariant group of order 4 generated by $T_4 = (T_x, T_y)$ where*

$$\begin{aligned}
R_x &= \frac{4u_2^5 + 12u_2^3}{u_2^8 - 2u_2^4 + 1}X^2u_3 + \frac{\frac{1}{3}u_2^8 + 8u_2^6 + 6u_2^4 - 9}{u_2^8 - 2u_2^4 + 1}X^2, \\
R_y &= \frac{16u_2^8 + 48u_2^6}{u_2^8 - 2u_2^4 + 1}u_3 + \frac{4u_2^9 + 36u_2^7 + 108u_2^5 + 108u_2^3}{u_2^6 + u_2^4 - u_2^2 - 1}, \\
T_x &= \frac{4iu_2^5 - 12iu_2^3}{u_2^8 - 2u_2^4 + 1}X^2u_1 + \frac{\frac{1}{3}u_2^8 - 8u_2^6 + 6u_2^4 - 9}{u_2^8 - 2u_2^4 + 1}X^2, \\
T_y &= \frac{16u_2^8 - 48u_2^6}{u_2^8 - 2u_2^4 + 1}u_1 + \frac{-4iu_2^9 + 36iu_2^7 - 108iu_2^5 + 108iu_2^3}{u_2^6 - u_2^4 - u_2^2 + 1}.
\end{aligned}$$

*Coordinates of the 3-torsion points of $E_{12,(X,Y,u_1,u_2,u_3)}$ can be read off from Theorem 2.1.2(ii). The forgetful map $\chi_{12,6} : X(12) \to X(6)$ is*

$$(X, Y, u_1, u_2, u_3) \mapsto (X, Y).$$

*It is only ramified above the cusps $X(6)$ and each ramified point has ramification index 2. In particular, $K_{12}(L)$ is an extension of $K_6(L)$ by adjoining three square roots of rational functions which have zeroes at cusps of $X(6)$.*

**Proof.** The coordinates of $R_4$ and $T_4$ can be obtained from a direct computation by factorising the 4-division polynomial over $X(12)$. The ramification behavior can be read off from Corollary 2.2.3 which describes explicitly the coordinates of the cusps of $X(6)$. Since we obtain $X(12)$ as a cover of $X(6)$ so it is clear that the forgetful map $\chi_{12,6} : X(12) \to X(6)$ is given by $(X, Y, u_1, u_2, u_3) \mapsto (X, Y)$. $\square$

# 3 Equations of Twists of Modular Curves

In this section we give equations of modular elliptic curves $X_E^r(n)$ for $n \leq 5$. These are already known and references can be found in [RS1], [S1], [F1], [F2]. Since $X_E^r(n)$ has genus zero for $n \leq 5$ so each curve is geometrically isomorphic to $\mathbb{P}^1$. Therefore, it is understood that we should give the families of elliptic curves parametrised by $X_E^r(n)$ if we fix an isomorphism $X_E(n) \to \mathbb{P}^1$. Throughout, let $E : y^2 = x^3 + ax + b$ be an elliptic curve over $K$ where $K$ is a field of characteristic not equal to $2, 3$ or $5$ and $c_4 = -a/27$ and $c_6 = -b/54$.

## 3.1 Level Two Structure

We give the formula for the families of elliptic curves parametrised by $X_E(2)$. Fix an isomorphism

$$X_E(2) \cong \mathbb{P}^1_v.$$

**Theorem 3.1.1.** *The families of elliptic curves parametrised by $X_E(2)$ are*

$$F_{2,v} : y^2 = x^3 + 3(3av^2 + 9bv - a^2)x + 27bv^3 - 18a^2v^2 - 27abv - (2a^3 + 27b^2).$$

*In other words, each elliptic curve which is two congruent to $E$ is a quadratic twist of $F_{2,v}$. Further,*

$$j(F_{2,v}) = \frac{(3av^2 + 9bv - a^2)^3 j(E)}{27a^3(v^3 + av + b)^2}, \quad \Delta_{F_{2,v}} = 3^6(v^3 + av + b)^2 \Delta_E.$$

**Proof.** See [RS1]. Note that the point $v = \infty$ corresponds to the curve $E$ itself. □

## 3.2 Level Three Structure

We give formulas for the families of elliptic curves parametrised by $X_E(3)$ and $X_E^2(3)$ in [F1]. Other formulas can be found in [S1].

**Theorem 3.2.1.** *Fix an isomorphism $X_E(3) \cong \mathbb{P}^1_\lambda$ (for simplicity we take affine coordinates). The families of elliptic curves parametrised by $X_E(3)$ are*

$$F_{3,\lambda} : y^2 = x^3 + A_3(\lambda)x + B_3(\lambda)$$

*where*

$$
\begin{aligned}
A_3(\lambda) &= a\lambda^4 + 2b\lambda^3 - \frac{2}{9}a^2\lambda^2 - \frac{2}{27}ab\lambda - \frac{1}{243}a^3 - \frac{1}{27}b^2, \\
B_3(\lambda) &= b\lambda^6 - \frac{4}{9}a^2\lambda^5 - \frac{5}{9}ab\lambda^4 - \frac{10}{27}b^2\lambda^3 + \frac{5}{243}a^2b\lambda^2 + (-\frac{4}{2187}a^4 - \frac{2}{243}ab^2)\lambda \\
&\quad - \frac{1}{2187}a^3b - \frac{2}{729}b^3.
\end{aligned}
$$

*Further,*

$$\Delta_{F_{3,\lambda}} = \left(\lambda^4 + \frac{2}{9}a\lambda^2 + \frac{4}{27}b\lambda - \frac{1}{243}a^2\right)^3 \Delta_E.$$

*The cusps of $X_E(3)$ are the points such that $\lambda^4 + \frac{2}{9}a\lambda^2 + \frac{4}{27}b\lambda - \frac{1}{243}a^2 = 0$.*

**Proof.** See [F4, Theorem 1.1]. □

**Theorem 3.2.2.** *Fix an isomorphism $X_E^2(3) \cong \mathbb{P}^1_\lambda$ (for simplicity we take affine coordinates). The families of elliptic curves parametrised by $X_E^2(3)$ are*

$$F^2_{3,\lambda} : y^2 = x^3 + A_{3,2}(\lambda)x + B_{3,2}(\lambda)$$

*where*

$$
\begin{aligned}
A_{3,2}(\lambda) &= \frac{1}{3} \cdot \frac{-243\lambda^4 - 54a\lambda^2 - 36b\lambda + a^2}{4a^3 + 27b^2}, \\
B_{3,2}(\lambda) &= -2 \cdot 3^6 \frac{B_3(\lambda)}{(4a^3 + 27b^2)^2}.
\end{aligned}
$$

*Further,*

$$\Delta_{F^2_{3,\lambda}} = 2^{24}3^{12} \frac{\left(a\lambda^4 + 2b\lambda^3 - \frac{2}{9}a^2\lambda^2 - \frac{2}{27}ab\lambda - \frac{1}{243}a^3 - \frac{1}{27}b^2\right)^3}{\Delta_E^4}.$$

**Proof.** See [F4, Theorem 1.1]. The curves $F^2_{3,\lambda}$ are isomorphic to the ones given in [F4]. □

## 3.3 Level Four Structure

We give formulae for the families of elliptic curves parametrised by $X_E(4)$ and $X_E^3(4)$ in [F1]. Moreover, we will describe the isomorphisms $X_E(4) \cong \mathbb{P}^1$ and $X_E^3(4) \cong \mathbb{P}^1$ which we will use later. Recall $X_E(4)$ is geometrically isomorphic to $\mathbb{P}^1$. The following theorem describes an explicit isomorphism from $X(4)$ to $X_E(4)$ and the family of elliptic curves parametrised by $X_E(4)$ under this isomorphism.

**Theorem 3.3.1.** *Define*

$$\begin{aligned} c_4(u,v) =& 256u^8 + 224u^4v^4 + v^8, \\ c_6(u,v) =& -4096u^{12} + 8448u^8v^4 + 528u^4v^8 - v^{12}. \end{aligned}$$

*Let $T = uv(16u^4 - v^4)$ and $T_u, T_v$ be the partial derivatives of $T$ with respect to $u, v$ respectively. Now pick $U, V \in \mathbb{C}$ such that $c_4(U,V) = c_4$ and $c_6(U,V) = c_6$. Then the isomorphism $X_E(4) \to X(4)$ is given by fractional linear map represented by the matrix*

$$\begin{pmatrix} U & -T_v(U,V) \\ V & T_u(U,V) \end{pmatrix}$$

*and so the isomorphism $X(4) \to X_E(4)$ is given by fractional linear map represented by the matrix*

$$\begin{pmatrix} T_u(U,V) & T_v(U,V) \\ -V & U \end{pmatrix}.$$

*Under this isomorphism the point $\infty$ on $X_E(4)$ corresponds to $E$ itself. Further, take affine coordinate $t$ for $X_E(4)$, the families of elliptic curves parametrised by $X_E(4)$ are*

$$F_{4,t} : y^2 = x^3 - 27A_4(t)x - 54B_4(t)$$

*where*

$$\begin{aligned} A_4(t) =& c_4t^8 + 8c_6t^7 + 28c_4^2t^6 + 56c_4c_6t^5 + (-42c_4^3 + 112c_6^2)t^4 \\ &+ 56c_4^2c_6t^3 + (252c_4^4 - 224c_4c_6^2)t^2 + (264c_4^3c_6 - 256c_6^3)t + (81c_4^5 - 80c_4^2c_6^2), \\ B_4(t) =& c_6t^{12} + 12c_4^2t^{11} + 66c_4c_6t^{10} + (44c_4^3 + 176c_6^2)t^9 + 495c_4^2c_6t^8 \\ &+ 792c_4^4t^7 + 924c_4^3c_6t^6 + (-2376c_4^5 + 3168c_4^2c_6^2)t^5 + (-5841c_4^4c_6 + 6336c_4c_6^3)t^4 \\ &+ (-1188c_4^6 - 4224c_4^3c_6^2 + 5632c_6^4)t^3 + (-4158c_4^5c_6 + 4224c_4^2c_6^3)t^2 \\ &+ (-2916c_4^7 + 4464c_4^4c_6^2 - 1536c_4c_6^4)t + (-1215c_4^6c_6 + 2240c_4^3c_6^3 - 1024c_6^5). \end{aligned}$$

*In particular, the point $t = \infty$ corresponds to $(E, [1])$ itself.*

**Proof.** See [F1, Lemma 8.4 and Theorem 13.2]. □

**Theorem 3.3.2.** *The curve $X_E^3(4)$ can be identified with $X_E(4)$. In other words, the isomorphism $X_E(4) \to X_E^3(4)$ can be chosen to be the identity map on $\mathbb{P}^1$ and if*

$$F_{4,t} : y^2 = x^3 - 27A_4(t)x - 54B_4(t)$$

*is the family of elliptic curves parametrised by* $X_E(4)$*, then*

$$F^3_{4,t} : y^2 = x^3 - 27\Delta_E^2 A_4(t)x - 54\Delta_E^3 B_4(t)$$

*is the family of elliptic curves parametrised by* $X^3_E(4)$*. Note that* $F^3_{4,t}$ *is the quadratic twist of* $F_{4,t}$ *by* $\Delta_E$ *for each* $t$*.*

**Proof.** [F1, Lemma 8.4 and Theorem 13.2]. □

In fact, the above theorem can also be explained by the following proposition, which can be found in [BD, Section 7].

**Proposition 3.3.3.** *Let* $E$ *be an elliptic curve and* $E^{\Delta_E}$ *be the quadratic twist of* $E$ *by its discriminant* $\Delta_E$*. Let* $\{p, q\}$ *be a basis for* $E[4]$*. Let* $\gamma : E \to E^{\Delta_E}$ *be the natural isomorphism*

$$(x, y) \mapsto (x\Delta_E, y\Delta_E^{\frac{3}{2}}).$$

*and* $p', q'$ *be the image of* $p, q$ *respectively. Then the map* $\phi : E[4] \to E^{\Delta_E}[4]$

$$\phi(p) = p' + 2q', \phi(q) = 2p' + 3q'$$

*is a* $G_{\mathbb{Q}}$*-equivariant isomorphism.*

The isomorphism $X(4) \to X_E(4) = X^3_E(4)$ specifies a basis for $E[4]$. Let $\{P, Q\}$ be the basis for $E[4]$ such that $(E, P, \langle Q\rangle) \mapsto (E, [1])$.

## 3.4 Level Five Structure

We give the families of elliptic curves parametrised by $X_E(5)$ in [F2].

**Theorem 3.4.1.** *Let* $c_4 = -\frac{a}{27}, c_6 = -\frac{b}{54}$*. The families of elliptic curves parametrised by* $X_E(5) \cong \mathbb{P}^1_t$ *are*

$$F_{5,t} : y^2 = x^3 + A_5(t)x + B_5(t)$$

*where the polynomials* $-\frac{A_5(t)}{27}, -\frac{B_5(t)}{54}$ *are the second and third outputs of the MAGMA code* **HessePolynomials**$(5, 1, [c_4, c_6])$*. The outputs are homogenous polynomials in two variables and by convention we set* $-\frac{A_5(t)}{27}, -\frac{B_5(t)}{54}$ *to be the polynomial by setting the second variable to be* $1$*. In particular,*

$$\Delta_{F_{5,t}} = \Delta_E D(t)^5$$

*where*

$$\begin{aligned}D(t) = {} & t^{12} - 66c_4t^{10} - 440c_6t^9 - 1485c_4^2t^8 - 3168c_4c_6t^7 + (5940c_4^3 - 10560c_6^2)t^6 \\ & - 4752c_4^2c_6t^5 + (-66825c_4^4 + 63360c_4c_6^2)t^4 + (-142560c_4^3c_6 + 140800c_6^3)t^3 \\ & + (-133650c_4^5 + 133056c_4^2c_6^2)t^2 + (-61560c_4^4c_6 + 61440c_4c_6^3)t \\ & + 91125c_4^6 - 193536c_4^3c_6^2 + 102400c_6^4.\end{aligned}$$

The formula for the families of elliptic curves parametrised by $X_E^2(5)$ can be found in [F2, Lemma 5.6 and Theorem 5.8]. In particular, it was shown that if we fix an isomorphism $X_E^2(5) \cong \mathbb{P}^1_{\lambda,\mu}$ then the family of elliptic curves parametrised by $X_E^2(5)$ is

$$y^2 = x^3 - 27c_4(\lambda,\mu)x - 54c_6(\lambda,\mu)$$

where

$$c_4(\lambda,\mu) = \frac{-1}{11^2 \cdot 12^2}\begin{vmatrix} \frac{\partial^2 D}{\partial \lambda^2} & \frac{\partial^2 D}{\partial \lambda \partial \mu} \\ \frac{\partial^2 D}{\partial \lambda \partial \mu} & \frac{\partial^2 D}{\partial \mu^2}\end{vmatrix} \quad \text{and} \quad c_6(\lambda,\mu) = \frac{-1}{12 \cdot 20}\begin{vmatrix} \frac{\partial D}{\partial \lambda} & \frac{\partial D}{\partial \mu} \\ \frac{\partial c_4(\lambda,\mu)}{\partial \lambda} & \frac{\partial c_4(\lambda,\mu)}{\partial \mu}\end{vmatrix}$$

and $D$ is a degree 12 polynomial in $\lambda$ and $\mu$ on page 14 of [F2]. We also have the following equality

$$c_4(\lambda,\mu)^3 - c_6(\lambda,\mu)^2 = (c_4^3 - c_6^2)^2 D^5.$$

# 4 Twist of Modular Curves: Level Six Structure

We will prove Theorem 1.7.1 in this section. We will give equations for $X_E(6)$ and $X_E^5(6)$ and the families of elliptic curves parametrised by them. The equation for $X_E(6)$ was found by K.Rubin and A.Silverberg [RS2]. I.Papadopoulos also found the equation for $X_E(6)$ using a different method [P]. The families of elliptic curves parametrised by $X_E(6)$ were computed by J.Roberts for some elliptic curve $E$ with specific $j$-invariant [R1]. We are going to compute $X_E(6)$ using a different method and give formulas for the families of elliptic curves parametrised by $X_E(6)$ for every elliptic curve $E : y^2 = x^3 + ax + b$.

Let $K$ be a field of characteristic not equal to 2 or 3 and $E : y^2 = x^3 + ax + b$ be an elliptic curve over $K$.

## 4.1 The General Setup

We establish some general setups for both $X_E(6)$ and $X_E^-(6)$. Our strategy to compute $X_E^{\pm}(6)$ is by using the fact that $X_E^{\pm}(6)$ is the fiber product of $X_E^{\pm}(3)$ and $X_E(2)$. This follows from the compatibility of the Weil pairing (Proposition 1.3.1 (v)). So we have the following commutative diagram

$$\begin{array}{ccc} X_E^{\pm}(6) & \xrightarrow{\chi_{6,2}^{\pm}} & X_E(2) \\ \downarrow{\scriptstyle \chi_{6,3}^{\pm}} & & \downarrow{\scriptstyle \chi_{2,1}} \\ X_E^{\pm}(3) & \xrightarrow{\chi_{3,1}^{\pm}} & X(1) \end{array}$$

where $\chi_{n,m}^{\pm}$ is the forgetful map $X_E^{\pm}(n) \to X_E^{\pm}(m)$. We are going to study carefully this commutative diagram and investigate how to build up the level six structure from the level two and the level three structures. If we give the equation of $X_E^{\pm}(6)$ in terms of the above commutative diagram (as the fiber product of $X_E(2)$ and $X_E^{\pm}(3)$), the equation will be very messy. Since $X_E^{\pm}(6)$ is a curve of genus one, we try to make the equation as simple as possible, as we will see later. We start with the following lemma.

**Lemma 4.1.1.** *Let $F_{3,\lambda}$ and $F_{3,\lambda}^2$ be the families of elliptic curves parametrised by $X_E(3)$ and $X_E^-(3)$ respectively, as in Theorem 3.2.1 and Theorem 3.2.2. Let $F_{2,v}$ be the families of elliptic curves parametrised by $X_E(2)$ as in 3.1.1. Then $\frac{\Delta_{F_{2,v}}}{\Delta_E}$ is a $K$-rational square, $\frac{\Delta_{F_{3,\lambda}}}{\Delta_E}$ and $\Delta_{F_{3,\lambda}^2}\Delta_E$ are $K$-rational cubes. In particular, this means that if two elliptic curves* *are 2-congruent, then the quotient of their discriminants is a $K$-rational square, and if two elliptic curves are 3-congruent with power 1 (resp. 2) then the quotient (resp. product) of their discriminants is a $K$-rational cube.*

**Proof.** This follows from a direct computation using Theorem 3.1.1, Theorem 3.2.1 and Theorem 3.2.2 $\square$

From the lemma above, we can now construct an intermediate curve between $X_E^{\pm}(6)$ and $X_E^{\pm}(3)$. In other words, the function field of this curve is an intermediate field between the function field of $X_E^{\pm}(6)$ and the function field of $X_E^{\pm}(3)$. Similarly, we also construct an intermediate curve between $X_E^{\pm}(6)$ and $X_E(2)$. Let $X^{\pm}$ be the modular curve between $X_E^{\pm}(6)$ and $X_E^{\pm}(3)$ such that if $F'_{3,\lambda}$ (resp. $F'^2_{3,\lambda}$) are families of elliptic curves parametrised by $X$ (resp. $X^-$), then $F'_{3,\lambda}$ (resp. $F'^2_{3,\lambda}$) is 3-congruent to $E$ with power 1 (resp. 2) and

$$\frac{\Delta_{F'_{3,\lambda}}}{\Delta_E}, \quad \frac{\Delta_{F'^2_{3,\lambda}}}{\Delta_E}$$

are both $K$-rational squares. Similarly, let $Y^{\pm}$ be the modular curve between $X_E^{\pm}(6)$ and $X_E(2)$ such that if $F'_{2,v}$ (resp. $F''_{2,v}$) are the families of elliptic curves parametrised by $Y$ (resp. $Y^-$), then $F'_{2,v}$ (resp. $F''_{2,v}$) is 2-congruent to $E$ and

$$\frac{\Delta_{F'_{2,v}}}{\Delta_E}, \quad \Delta_{F''_{2,v}}\Delta_E$$

are $K$-rational cubes. Let $\rho^{\pm} : X^{\pm} \to X_E^{\pm}(3)$ and $\psi^{\pm} : Y^{\pm} \to X_E(2)$ be the forgetful maps. We now compute the (simplified) equations for $X^{\pm}$ and $Y^{\pm}$.

**Lemma 4.1.2.** *The curve $X^{\pm}$ is a double cover of $\mathbb{P}^1$ and it is a curve of genus 1 in weighted projective space. The curve $Y^{\pm}$ is a cubic plane curve of genus 1. For simplicity, we give the affine equations for $X^{\pm}$ and $Y^{\pm}$.*

*The curve $X \subset \mathbb{A}^2_{y,\lambda}$ has equation*

$$y^2 = \lambda^4 + 2a\lambda^2 + 4b\lambda - \frac{1}{3}a^2$$

*and the curve $X^- \subset \mathbb{A}^2_{y,\lambda}$ has equation*

$$y^2 = \Delta_E(a\lambda^4 + 6b\lambda^3 - 2a^2\lambda^2 - 2ab\lambda - \frac{a^3}{3} - 3b^2)$$

*with forgetful maps*

$$\rho^{\pm} : X^{\pm} \to X_E^{\pm}(3), \quad \rho^{\pm}(y, \lambda) = \lambda/3.$$

*The curve* $Y \subset \mathbb{A}^2_{y,v}$ *has equation*

$$y^3 = v^3 + av + b$$

*and the curve* $Y^- \subset \mathbb{A}^2_{y,v}$ *has equation*

$$y^3 = \Delta_E(v^3 + av + b)$$

*with forgetful maps*

$$\psi^{\pm} : Y^{\pm} \to X_E(2), \quad \psi^{\pm}(y, v) = v.$$

*The forgetful map sends the points of infinity on* $X^{\pm}, Y^{\pm}$ *to the points of infinity on* $X_E^{\pm}(3), X_E(2)$ *respectively.*

**Proof.** Using the modular interpretation of $X$, an (affine) model of $X \subset \mathbb{A}^2_{y,\lambda}$ can be computed as

$$y^2\Delta_E = \Delta_{F_{3,\lambda}} = \left(\lambda^4 + \frac{2}{9}a\lambda^2 + \frac{4}{27}b\lambda - \frac{1}{243}a^2\right)^3 \Delta_E$$

and so we have

$$y^2 = \left(\lambda^4 + \frac{2}{9}a\lambda^2 + \frac{4}{27}b\lambda - \frac{1}{243}a^2\right)^3.$$

Writing the above equation in the form

$$\frac{81y^2}{\left(\lambda^4 + \frac{2a}{9}\lambda^2 + \frac{4}{27}b\lambda - \frac{1}{243}a^2\right)^2} = (3\lambda)^4 + 2a(3\lambda^2) + 4b(3\lambda) - \frac{1}{3}a^2$$

we see $X$ is isomorphic to the curve as stated in the lemma. The forgetful map is then $(y, \lambda) \mapsto \lambda/3$.

Similarly, an (affine) model of $X^- \subset \mathbb{A}^2_{y,\lambda}$ can be computed as

$$y^2\Delta_E = \Delta_{F^2_{3,\lambda}} = 2^{24}3^{12}\frac{\left(a\lambda^4 + 2b\lambda^3 - \frac{2}{9}a^2\lambda^2 - \frac{2}{27}ab\lambda - \frac{1}{243}a^3 - \frac{1}{27}b^2\right)^3}{\Delta_E^4}.$$

Writing the above equation in the form

$$\begin{aligned}\left(\frac{9y\Delta_E^3}{2^{12}3^6\left(a\lambda^4 + 2b\lambda^3 - \frac{2}{9}a^2\lambda^2 - \frac{2}{27}ab\lambda - \frac{1}{243}a^3 - \frac{1}{27}b^2\right)^2}\right)^2 &= \Delta_E((3\lambda)^4 + 6b(3\lambda)^3 - 2a^2(3\lambda)^2 \\ &- 2ab(3\lambda) - a^3/3 - 3b^2),\end{aligned}$$

we see $X^-$ is isomorphic to the curve as stated in the lemma. The forgetful map is then $(y, \lambda) \mapsto \lambda/3$.

Using the modular interpretation of $Y$, an (affine) model of $Y \subset \mathbb{A}^2_{y,v}$ can be computed as

$$y^3 \Delta_E = \Delta_{F_{2,v}} = 3^6(v^3 + av + b)^2 \Delta_E.$$

Writing the above equation in the form

$$\left(\frac{9(v^3 + au^2v + bu^3)}{y}\right)^3 = v^3 + au^2v + bu^3$$

we see $Y$ is isomorphic to the curve as stated in the lemma. The forgetful map is then $(y, v) \mapsto v$.

Similarly, an (affine) model of $Y^-$ can be computed as

$$y^3 = \Delta_E \Delta_{F_{2,v}} = 3^6(v^3 + av + b)^2 \Delta_E^2.$$

Writing the above equation in the form

$$\left(\frac{9\Delta_E(v^3 + au^2v + bu^3)}{y}\right)^3 = (v^3 + au^2v + bu^3)\Delta_E,$$

we see $Y^-$ is isomorphic to the curve as stated in the lemma. The forgetful map is then $(y, v) \mapsto v$. $\square$

**Corollary 4.1.3.** *Let $\mathbb{C}(X^\pm)$, $\mathbb{C}(Y^\pm)$, $\mathbb{C}(X_E^\pm(3))$, $\mathbb{C}(X_E(2))$ be the function fields of $X^\pm$, $Y^\pm$, $X_E^\pm(3)$, $X_E(2)$ respectively over $\mathbb{C}$. Then*

$$[\mathbb{C}(X^\pm) : \mathbb{C}(X_E^\pm(3))] = 2, \quad [\mathbb{C}(Y^\pm) : \mathbb{C}(X_E(2))] = 3.$$

**Proof.** This follows immediately from the previous lemma. $\square$

The above observations imply that the forgetful map $\chi_{6,3}^\pm$ factors through

$$X_E^\pm(6) \xrightarrow{\rho'^\pm} X^\pm \xrightarrow{\rho^\pm} X_E^\pm(3)$$

and the forgetful map $\chi_{6,2}^\pm$ factors through

$$X_E^\pm(6) \xrightarrow{\psi'^\pm} Y^\pm \xrightarrow{\psi^\pm} X_E(2)$$

where the degrees of the maps $\rho^{\pm}$ and $\psi^{\pm}$ are 2 and 3 respectively.

Recall that if $K_n(\mathbb{C})$ is the function field of $X(n)$ over $\mathbb{C}$, then for each $m|n$, $K_n(\mathbb{C})/K_m(\mathbb{C})$ has Galois group $H_{n,m}$ where $H_{n,m}$ is

$$\ker(\mathrm{PSL}_2(\mathbb{Z}/n\mathbb{Z}) \to \mathrm{PSL}_2(\mathbb{Z}/m\mathbb{Z})).$$

Therefore,

$$H_{6,3} \cong \mathrm{PSL}_2(\mathbb{Z}/2\mathbb{Z}) \cong S_3 \text{ and } H_{6,2} \cong \mathrm{PSL}_2(\mathbb{Z}/3\mathbb{Z}) \cong A_4.$$

Since $X_E^{\pm}(6)$, $X_E^{\pm}(3)$ and $X_E(2)$ are twists of $X(6)$, $X(3)$ and $X(2)$ respectively, we conclude that $\mathbb{C}(X_E^{\pm}(6))/\mathbb{C}(X_E^{\pm}(3))$ has Galois group $S_3$ and $\mathbb{C}(X_E^{\pm}(6))/\mathbb{C}(X_E(2))$ has Galois group $A_4$.

We have shown that $\chi_{6,3}^{\pm}$ has degree $|\mathrm{PSL}_2(\mathbb{Z}/2\mathbb{Z})| = 6$ and $\chi_{6,2}^{\pm}$ has degree $|\mathrm{PSL}_3(\mathbb{Z}/3\mathbb{Z})| = 12$, so $\rho'^{\pm}$ has degree 3 and $\psi'^{\pm}$ has degree 4. Moreover, we have

**Corollary 4.1.4.** *The forgetful map $\rho'^{\pm} : X_E^{\pm}(6) \to X^{\pm}$ is the quotient map by the action of $C_3 \subset S_3$. The forgetful map $\psi'^{\pm} : X_E^{\pm}(6) \to Y^{\pm}$ is the quotient map by the action of $V_4 \subset A_4$ where $V_4$ is the Klein four-group.*

**Proof.** This follows from the fact that $\rho'^{\pm}$ has degree 3 and $\psi'^{\pm}$ has degree 4, and the fact that the only subgroup of order 3 inside $S_3$ is $C_3$ and the only subgroup of order 4 inside $A_4$ is $V_4$. $\square$

The above corollary allows us to construct another intermediate curve between $X_E^{\pm}(6)$ and $X(1)$. Consider the quotient map by the action of $C_3 \times V_4 \subset \mathrm{PSL}_2(\mathbb{Z}/6\mathbb{Z})$ from $X_E^{\pm}(6)$ to an intermediate curve between $X_E^{\pm}(6)$ and $X(1)$. Write $Z^{\pm}$ for this curve. Then the forgetful map $\nu^{\pm} : X^{\pm} \to Z^{\pm}$ is the quotient map by the action of $V_4 \subset A_4$ and the forgetful map $\phi^{\pm} : Y^{\pm} \to Z^{\pm}$ is the quotient map by the action of $C_3 \subset S_3$. Therefore, we obtain the following big commutative diagram

$$\begin{tikzcd}
X_E^{\pm}(6) \arrow[r, "\psi'^{\pm}"] \arrow[d, "\rho'^{\pm}"] & Y^{\pm} \arrow[r, "\psi^{\pm}"] \arrow[d, "\phi^{\pm}"] & X_E(2) \\
X^{\pm} \arrow[r, "\nu^{\pm}"] \arrow[d, "\rho^{\pm}"] & Z^{\pm} & \\
X_E^{\pm}(3) & &
\end{tikzcd}$$

**Lemma 4.1.5.** *The curve $Z^{\pm}$ has genus* 1.

**Proof.** By Proposition 1.4.7, the forgetful map $X_E^{\pm}(6) \to X(1)$ is ramified at the points above $\infty, 0, 1728$ with ramification index $6, 2, 3$ respectively and the forgetful map $X_E(2) \to X(1)$ is ramified at the points above $\infty, 0, 1728$ with ramification index $2, 2, 3$ respectively. Since $\mathbb{C}(X_E^{\pm}(6))/\mathbb{C}(X_E(2))$ is Galois, by tower law, $\chi_{6,2}^{\pm} : X_E^{\pm}(6) \to X_E(2)$ is only ramified at the cusps of $X_E^{\pm}(6)$ with ramification index 3. Since $\bar{K}(X_E^{\pm}(6))/\bar{K}(Y^{\pm})/\mathbb{C}(X_E(2))$ is a tower of Galois extension, and the degree of $\psi'^{\pm} : X_E^{\pm}(6) \to Y^{\pm}$ is 4, which is coprime to 3, we conclude that $X_E^{\pm}(6) \to Y^{\pm}$ is unramified.

Similarly, $\chi_{6,3}^{\pm} : X_E^{\pm}(6) \to X_E^{\pm}(3)$ is only ramified at the cusps of $X_E^{\pm}(6)$ with ramification index 2. Since $\rho'^{\pm}$ has degree 3 which is coprime to 2, the map $\rho'^{\pm}$ is unramified. Therefore

$$\nu^{\pm} : X^{\pm} \to Z^{\pm}$$

is unramified by tower law. So $Z^{\pm}$ has genus 1 by using Riemann-Hurwitz formula. $\square$

Now we know that $X^{\pm}, Y^{\pm}$ and $Z^{\pm}$ are curves of genus one. This allows us to study the geometric interpretations of the forgetful maps $\rho'^{\pm}$ and $\psi'^{\pm}$.

**Lemma 4.1.6.** *The forgetful map $\rho'^{\pm}$ is geometrically a 3-isogeny. In other words, $\rho'^{\pm}$ : $X_E^{\pm}(6) \to X^{\pm}$ is a 3-isogeny over $\bar{K}$.*

**Proof.** Any morphism between genus one curves $E_1, E_2$ over $\bar{K}$ is an isogeny because we can pick the identity point on $E_2$ to be the image of the identity point on $E_1$. $\square$

**Lemma 4.1.7.** *Over $\bar{K}$, $X_E^{\pm}(6)$ is isomorphic to $Y^{\pm}$ and the forgetful map $\psi'^{\pm}$ is geometrically the multiplication-by-2 map. In particular, $X_E^{\pm}(6)$ and $Y^{\pm}$ have the same Jacobian.*

**Proof.** $\psi'^{\pm} : X_E^{\pm}(6) \to Y^{\pm}$ is the quotient map by the action of $V_4 \subset A_4$. We have shown in the proof of Corollary 4.1.5 that $\psi'^{\pm}$ is unramified. Therefore for all $1 \neq h \in V_4$, the action of $h$ on $X_E^{\pm}(6)$ does not have any fixed point. If we view $h$ as an isomorphism on $X_E^{\pm}(6)$, then the point $O$ (over $\bar{K}$) is not in the image of the morphism $h - 1$. This shows that $h - 1$ is not surjective and hence it must be a constant map. Therefore, $h$ acts as translation on $X_E^{\pm}(6)$. Since $h$ has order 2, we conclude that $h$ acts as translation by 2-torsion points. So the quotient map $\psi'^{\pm} : X_E^{\pm}(6) \to Y^{\pm}$ has kernel $X_E^{\pm}(6)[2]$.

By Theorem 1.2.2 (ii), there is a unique elliptic curve (up to $\bar{K}$-isomorphism) $E'$ and a separable isogeny

$$f : X_E^{\pm}(6) \to E'$$

such that $\ker(f) = X_E^{\pm}(6)[2]$. By uniqueness $E' \cong Y^{\pm}$. But $[2] : X_E^{\pm}(6) \to X_E^{\pm}(6)$ also has kernel $X_E^{\pm}(6)[2]$. So again by uniqueness we conclude that $X_E^{\pm}(6) \cong E'$ over $\bar{K}$ and hence

$$X_E^{\pm}(6) \cong Y^{\pm} \text{ over } \bar{K}.$$

□

Similarly, we have

**Corollary 4.1.8.** *The forgetful map $\phi^{\pm} : Y^{\pm} \to Z^{\pm}$ is a 3-isogeny over $\bar{K}$. Over $\bar{K}$, $X^{\pm}$ is isomorphic to $Z^{\pm}$ and the forgetful map $\nu^{\pm} : X^{\pm} \to Z^{\pm}$ is a multiplication-by-2 map. In particular, $X^{\pm}$ and $Z^{\pm}$ have the same Jacobian.*

Finally, we compute an equation for $Z^{\pm}$ in this section. We will show that $Z^{\pm}$ is actually an elliptic curve. In other words, it has a $K$-rational point.

**Proposition 4.1.9.** *The curve $Z^{\pm} \subset A^2_{x,y}$ has equation*

$$y^2 = x^3 - 27\Delta_E^{\pm}.$$

**Proof.** Recall from Lemma 4.1.2 that $X$ has equation $y^2 = f^+(\lambda)$ and $X^-$ has equation $y^2 = f^-(\lambda)$ where

$$f^+(\lambda) = \lambda^4 + 2a\lambda^2 + 4b\lambda - \frac{1}{3}a^2,$$

and

$$f^-(\lambda) = \Delta_E(a\lambda^4 + 6b\lambda^3 - 2a^2\lambda^2 - 2ab\lambda - \frac{a^3}{3} - 3b^2).$$

$X^{\pm}$ is an elliptic curve over $\bar{K}$ and we have shown that geometrically $\nu^{\pm}$ is multiplication-by-2. The kernel of multiplication-by-2 can be described as the set of points which have ramification index 2 under the covering map $(x, y) \mapsto x$. Therefore, the kernel of $\nu^{\pm}$ is precisely $\{(t_i^{\pm}, 0), i = 1, 2, 3, 4\}$ where $t_1^{\pm}, \ldots, t_4^{\pm}$ are the points such that $f(t_i) = 0$ and $f^-(t_i^-) = 0$. In particular, $t_1^{\pm}, \ldots, t_4^{\pm}$ have the same image under $\nu^{\pm}$, say $q$.

Note that $t_i^{\pm}, i = 1,2,3,4$ are Galois conjugates and so $G_K$ permute them. Since $\nu^{\pm}$ is defined over $K$,

$$s \circ q =^s \nu(s^{-1}t_i) =^s \nu^{\pm}(t_i) = \nu^{\pm}(t_i) = q, \text{ for all } s \in G_K.$$

So $q$ is a $K$-rational point on $Z^{\pm}$ and so $Z^{\pm}$ is an elliptic curve.

By Corollary 4.1.8, $Z^{\pm}$ and $X^{\pm}$ have the same Jacobian. Since $Z^{\pm}$ is an elliptic curve, we conclude that $Z^{\pm}$ is isomorphic to the Jacobian of $X^{\pm}$ over $K$. Therefore, by computing the Jacobian of $X^{\pm}$ using standard formula in [AKM$^3$P] we conclude that $Z^{\pm}$ is isomorphic to the curve in the statement (alternatively the MAGMA code nCovering does it for us). □

**Corollary 4.1.10.** *The Jacobian of $X^{\pm}$ has equation*

$$y^2 = x^3 + \Delta_E^{\pm}.$$

**Proof.** By Lemma 4.1.7, $X_E^{\pm}(6)$ and $Y^{\pm}$ have the same Jacobian and by Lemma 4.1.6, $Y^{\pm}$ is geometrically 3-isogenous to $Z^{\pm}$. By using the equation for $Z^{\pm}$ in Proposition 4.1.9, we conclude that the Jacobian of $Y^{\pm}$ has equation

$$y^2 = x^3 + \Delta_E^{\pm}$$

and so this can be taken to be the Jacobian of $X^{\pm}$. □

**Remark** We can also compute $Z^{\pm}$ by using its modular interpretation. Note that $Z$ parametrises families of elliptic curves $\mathcal{F}$ such that for each $F \in \mathcal{F}$, the quotient $\Delta_F/\Delta_E$ is a $K$-rational square and the quotient $\Delta_F/\Delta_E$ is a $K$-rational cube. $Z^-$ parametrises families of elliptic curves $\mathcal{F}^-$ such that for each $F \in \mathcal{F}^-$, the quotient $\Delta_F/\Delta_E$ is a $K$-rational square and the product $\Delta_F\Delta_E$ is a $K$-rational cube.

## 4.2 The Curve $X_E(6)$

We are going to compute a model for $X_E(6)$ over $K$ in this section, together with the forgetful map $\chi_{6,3}^+ : X_E(6) \to X_E(3)$. The equation for $X_E(6)$ can be obtained immediately from the above observation.

**Corollary 4.2.1.** *The curve $X_E(6) \subset \mathbb{A}^2_{x,y}$ has equation $y^2 = x^3 + \Delta_E$.*

**Proof.** Recall that each non-cuspidal point on $X_E(n)$ corresponds to a pair $(F, \phi_F)$ (up to $K$-isomorphism) where $F$ is an elliptic curve and $\phi_F : E[n] \to F[n]$ is a $G_K$-equivariant isomorphism such that $e_n(P,Q) = e_n(\phi_F(P), \phi_F(Q))$ for all $P, Q \in E[6]$. In particular, $(E, [1])$ is a $K$-rational point on $X_E(6)$. Therefore, $X_E(6)$ is isomorphic to its Jacobian, which is given in Corollary 4.1.10. $\square$

Moreover, in the proof above we see that by our convention the point of infinity $O$ on $X_E(6)$ always corresponds to $(E, [1])$. This gives us a way to compute the forgetful map $\rho'^{+} : X_E(6) \to X$ and hence the forgetful map $\chi^{+}_{6,3} : X_E(6) \to X_E(3)$.

**Theorem 4.2.2.** *Identify $X_E(3)$ with $\mathbb{P}^1_\lambda$ as in Theorem 3.2.1. Then the forgetful map $X_E(6) \to X_E(3)$ is*

$$(x, y) \mapsto \frac{x^3 y - 108 b x^3 - 8\Delta_E y}{18(x^4 + 12 a x^3 + 4\Delta_E x)}.$$

*Moreover, we have the following commutative diagram*

$$\begin{array}{ccc} X(6) & \xrightarrow{\psi_6} & X_E(6) \\ \Big\downarrow{\scriptstyle \chi_{6,3}} & & \Big\downarrow{\scriptstyle \chi^{+}_{6,3}} \\ X(3) & \xrightarrow{\psi_3} & X_E(3) \end{array}$$

*where $\psi_3$ is the isomorphism $X(3) \to X_E(3)$ in [F1, Lemma 8.4 and Theorem 13.2] and $\psi_6$ is the isomorphism $X(6) \to X_E(6)$ defined as*

$$\psi_6(x, y) = (\sqrt[3]{\Delta_E}\, x, \sqrt{\Delta_E}\, y) \ominus (\sqrt[3]{\Delta_E}\, x_0, \sqrt{\Delta_E}\, y_0)$$

*where $(x_0, y_0)$ is a point on $X(6)$ which corresponds to $E$. The $\oplus$ above is the usual group law on $X(6) : y^2 = x^3 + 1$ which is viewed as an elliptic curve.*

**Proof.** By Lemma 4.1.6 the forgetful map $\rho'^{+} : X_E(6) \to X$ is geometrically a 3-isogeny. Since $X_E(6)$ has a $K$-rational point, so does $X$. Therefore, $X$ is isomorphic to its Jacobian and by Corollary 4.1.8 and Proposition 4.1.9, $X$ is $K$-isomorphic to

$$J_X : y^2 = x^3 - 27\Delta_E.$$

We have more than 1 degree 3 morphism from $X_E(6)$ to $X$ because we can compose any such morphism with the involution $(x, y) \mapsto (x, -y)$. We will construct an explicit morphism of degree 3 and show it is the correct one with respect to the commutative diagram.

The map

$$(x,y)\mapsto\left(\frac{x^3+4\Delta_E}{x^2},\frac{-x^3y-8\Delta_E y}{x^3}\right)$$

is a morphism of degree 3 from $X_E(6)$ to $J_X$, which sends the point of infinity of $X_E(6)$ to the point of infinity on $J_X$. We also have the isomorphism

$$J_X\to X,\ (x,y)\mapsto\left(\frac{-y-108b}{6x+72a},\frac{-216by+x^3+36ax^2+54\Delta_E}{36(x+12a)^2}\right).$$

Taking composition of these two morphisms gives us the map $\rho'^{+}: X_E(6)\to X$. Since $\rho^+: X\to X_E(3)$ is given by $(\lambda,y)\mapsto\lambda/3$, the composition of these morphisms is

$$X_E(6)\to J_X\to X\to X_E(3),\quad (x,y)\mapsto\frac{x^3y-108bx^3-8\Delta_E y}{18(x^4+12ax^3+4\Delta_E x)}.$$

We now show that this forgetful map respects the commutative diagram in the statement. Note that our convention is that the point of infinity on $X_E(6)$ corresponds to $(E,[1])$ itself. Therefore, the isomorphism

$$\psi_6: X(6)\to X_E(6)$$

takes the point corresponding to $E$ on $X(6)$ to the point of infinity on $X_E(6)$. Let $(x_0,y_0)$ be a point on $X(6)$ which corresponds to $E$. Then the only isomorphism $X(6)\to X_E(6)$ which takes $(x_0,y_0)$ to $O\in X_E(6)$ are

$$(x,y)\mapsto(\zeta_3^i\sqrt[3]{\Delta_E}x,(-1)^j\sqrt{\Delta_E}y)\ominus(\zeta_3^i\sqrt[3]{\Delta_E}x_0,(-1)^j\sqrt{\Delta_E}y_0), i=0,1,2, j=0,1$$

because the only isomorphisms on $X_E(6)$ which fix $O$ are of the form

$$(x,y)\mapsto(\zeta_3^i x,(-1)^j y).$$

The map $\psi_3: X(3)\to X_E(3)$ determines the cusps of $X_E(3)$ explicitly, and the cusps of $X_E(6)$ are the points above the cusps of $X_E(3)$ under

$$(x,y)\mapsto\frac{x^3y-108bx^3-8\Delta_E y}{18(x^4+12ax^3+4\Delta_E x)}.$$

Finally, $\psi_6: X(6)\mapsto X_E(6)$ sends the cusps of $X(6)$ to the cusps of $X_E(6)$. Matching up the cusps allows us to conclude that the map

$$\psi_6: X(6)\to X_E(6): (x,y)\mapsto(\sqrt[3]{\Delta_E}x,\sqrt{\Delta_E}y)\ominus(\sqrt[3]{\Delta_E}x_0,\sqrt[3]{\Delta_E}y_0)$$

is the one such that the diagram in the statement commutes. □

**Remark** The above theorem shows that the families of elliptic curves parametrised by $X_E(6) : y^2 = x^3 + \Delta_E$ are $F_{3,\lambda}$ as in Theorem 3.2.1 with

$$\lambda = \frac{x^3y - 108bx^3 - 8\Delta_E y}{18(x^4 + 12ax^3 + 4\Delta_E x)}.$$

**Remark** To find the family of elliptic curves parametrised by $X_E(6)$, we do not need to study carefully the commutative diagram in the above theorem. However, we will see that it is very important to have this diagram when we compute $X_E(12)$ in Section 7.

Further, K.Rubin and A.Silverberg [RS2] showed that

**Proposition 4.2.3.** *For all but finitely many values of $a$ and $b$, the curve $X_E(6)$ has positive rank.*

**Proof.** The point

$$P_E = \left(\frac{4a^3 + 36b^2}{a^2}, \frac{-36a^3b - 216b^3}{a^3}\right)$$

is a point of infinite order for all but finitely many values of $a$ and $b$. $\square$

Here is an immediate consequence of the above proposition.

**Corollary 4.2.4.** *There are infinitely many pairs of non-isogenous directly 6-congruent elliptic curves.*

## 4.3 The Curve $X_E^-(6)$

In the previous section, we compute $X_E(6)$ by identifying it with its Jacobian. Let $K = \mathbb{Q}$. The following examples show that $X^-$ or $Y^-$ does not necessarily have rational points. In particular, this shows that $X_E^-(6)$ does not necessarily have a rational point.

**Example 4.3.1.** *Let $a = 1$ and $b = 0$. Then $X^-$ has equation*

$$3\lambda^4 - 6\lambda^2 + 3(y/8)^2 - 1 = 0$$

*and so it is isomorphic to the curve with equation*

$$3\lambda^4 - 6\lambda^2 + 3y^2 - 1 = 0.$$

*This is not locally soluble at 3, and so it has no rational point.*

**Example 4.3.2.** *Let $a = 0$ and $b = 3$. Then $Y^-$ has equation*

$$3888v^3 + y^3 + 11664 = 0.$$

*This is not locally soluble at 3, and so it has no rational point.*

We will use the equation for $X^-$ and Theorem 3.1.1 to compute equations for $X_E^-(6)$. The method is based on the fact that the function field of $X_E(2)$ is geometrically an $S_3$ extension over the function field of $X(1)$. We compute the function field of $X_E(2)$ as an extension of the function field of $X(1)$, and generalise this method to compute $X_E^-(6)$ from $X_E^-(3)$.

The following is an immediate consequence of Theorem 3.1.1.

**Lemma 4.3.3.** *The (affine) equations for $X_E(2) \subset \mathbb{A}^3_{j,s,v}/K$ are given by $F = G = 0$ where*

$$F = s^2 - (-4a^3 - 27b^2)(j - 1728),$$
$$G = (-s + 216b)v^3 - 144a^2v^2 - a(s + 216b)v - b(s + 216b) - 16a^3.$$

*In particular, if we identify the function field of $X(1)$ with $K(j)$, then the function field of $X_E(2)$ is $K(j, s, v)$ such that $v, s, j$ satisfy the above equations.*

**Proof.** Fix an isomorphism $X_E(2) \cong \mathbb{P}^1_v$ as in Theorem 3.1.1. Let $j(F_{2,v})$ be the same as in Theorem 3.1.1. Then we observe that

$$(-4a^3 - 27b^2)(j(F_{2,v}) - 1728) = \frac{(216bv^3 - 144a^2v^2 - 216abv - 16a^3 - 216b^2)^2}{(v^3 + av + b)^2}.$$

Let $s$ be a square root of this, say

$$s = \frac{216bv^3 - 144a^2v^2 - 216abv - 16a^3 - 216b^2}{v^3 + av + b},$$

then a direct computation shows that

$$(-s + 216b)v^3 - 144a^2v^2 - a(s + 216b)v - b(s + 216b) - 16a^3 = 0.$$

Theorem 3.1.1 shows that the forgetful map $X_E(2) \to X(1)$ is just given by $v \mapsto j(F_{2,v})$. Therefore, the result follows by identifying $X(1)$ with $\mathbb{P}^1_j$. □

**Remark** The above lemma shows that we can build up the curve $X_E(2)$ by the following diagram

$$X_E(2) \longrightarrow X' \longrightarrow X(1)$$

where the curve $X'$ has equation $s^2 - (-4a^3 - 27b^2)(j - 1728) = 0$. We also have forgetful maps

$$X_E(2) \to X' \to X(1), \quad (j, v, s) \mapsto (j, s) \mapsto j.$$

The following is a restatement of the previous lemma

**Lemma 4.3.4.** *Let $z = \sqrt{\frac{4a^3+27b^2}{27}}$. The (affine) equations for $X_E(2) \subset \mathbb{A}^3_{j,s,r}/K(z)$ are given by $F' = G' = 0$ where*

$$F' = s^2 - (-4a^3 - 27b^2)(j - 1728),$$
$$G' = 2(s - 216z)r^3 - (b + z)(s + 216z).$$

*In particular, the function field of $X_E(2)$ over $K(z)$ is*

$$K(z)\left(j, s, \sqrt[3]{\frac{(b+z)(s+216z)}{2(s-216z)}}\right).$$

**Proof.** Use the equations for $X_E(2)$ in the previous lemma. In particular, $v$ satisfies the cubic polynomial $G = 0$ over $K(j, s)$ where $s^2 = (-4a^3-27b^2)(j(F_{2,v})-1728)$. The quadratic resolvent of $G$ is

$$x^2 - (bs + 8D)tDx - \frac{a^3t^3D^3}{27} = 0$$

where $D = -4a^3 - 27b^2$. One of the roots is given by

$$u = \frac{(s - 216z)(s + 216z)(bs + 8D + (s - 216b)z)}{2}.$$

Therefore, the function field of $X_E(2)$ over $K(z)$ is given by $K(z)(j, s, \sqrt[3]{u})$. The result follows by setting $r = \frac{\sqrt[3]{u}}{(s-216z)}$ and so $K(z)(j, s, \sqrt[3]{r})$. $\square$

We will now use a similar method to build up the curve $X_E^-(6)$, as a cover of $X_E^2(3)$. We fix an elliptic curve $E$. Since the mod 2 representation of $E$ only depends on the $j$-invariant of $E$, it suffices to start with the family of elliptic curves $F^2_{3,\lambda}$ parametrised by $X_E^2(3) \cong \mathbb{P}^1_\lambda$, and give some condition on $\lambda$ so that $j(F^2_{3,\lambda}) = j(F_{2,v})$ for some $v$. This means that, we replace $j$ in the lemma above by $j(F^2_{3,\lambda})$. Therefore,

**Corollary 4.3.5.** *The (affine) equations for* $X_E^-(6) \subset \mathbb{A}^3_{\lambda,s,r}/K(z)$ *are given by* $f = g = 0$ *where*

$$f' = (4A_{3,2}(\lambda)^3 + 27B_{3,2}(\lambda)^2)s^2 + 46656(-4a^3 - 27b^2)B_{3,2}(\lambda)^2,$$
$$g' = 2(s - 216z)r^3 - (b + z)(s + 216z),$$

*and* $A_{3,2}(\lambda)$ *and* $B_{3,2}(\lambda)$ *are polynomials in* $\lambda$ *as in Theorem 3.2.2.*

**Proof.** This follows from Lemma 4.3.4 and replacing $j$ by $j(F^2_{3,\lambda})$. □

The above equations are in fact very messy if we go back and look at the expressions of $A_{3,2}(\lambda)$ and $B_{3,2}(\lambda)$. So the remaining task is to find simpler equations for $X_E^-(6)$.

**Remark** The curve in $\mathbb{A}^2_{\lambda,s}$ defined by $f = 0$ corresponds to the curve $X'$ above. Since there is a unique subgroup of order 3 inside $S_3$, we conclude that $X'$ must be isomorphic to the curve $X^-$ we computed in 4.1.2.

We now do some calculations to verify this. In fact we have

$$j(F^2_{3,\lambda}) - 1728 = \frac{46656B^2}{-4A_{3,2}(\lambda)^3 - 27B_{3,2}(\lambda)^2} = \frac{B_{3,2}(\lambda)^2 D^4}{2^{10}3^{30}h(\lambda)^3}$$

where $D = -4a^3 - 27b^2$ and

$$h(\lambda) = a\lambda^4 + 2b\lambda^3 - \frac{2}{9}a^2\lambda^2 - \frac{2}{27}ab\lambda + \left(-\frac{1}{243}a^3 - \frac{1}{27}b^2\right).$$

Therefore, we have

$$s^2 = D(j(F^2_{3,\lambda}) - 1728) = \frac{B_{3,2}(\lambda)^2 D^8}{2^{10}3^{30}(h(\lambda)D)^3}.$$

If we write

$$s = s'\frac{B_{3,2}(\lambda)D^4}{2^7 3^{15}(h(\lambda)D)^2}$$

then we have

$$s'^2 = 16Dh(\lambda) = \Delta_E\left(a\lambda^4 + 2b\lambda^3 - \frac{2}{9}a^2\lambda^2 - \frac{2}{27}ab\lambda + \left(-\frac{1}{243}a^3 - \frac{1}{27}b^2\right)\right).$$

We see that this curve is isomorphic to the curve $X^-$ in Lemma 4.1.2, if we replace $s'$ by $9s'$ and $\lambda$ by $3\lambda$.

The above remark suggests that we set $u^2 = Dh(\lambda)$ and the curve with equation $u^2 - Dh(\lambda) = 0$ is isomorphic to $X^-$. Taking square roots of the equation

$$s^2 = \frac{B_{3,2}(\lambda)^2 D^8}{2^{10}3^{30}(h(\lambda)D)^3},$$

we obtain

$$s = \frac{B_{3,2}(\lambda) D^4}{2^5 3^{15} u^3}.$$

The simpler equations for $X_E^-(6)$ is based on the following observation.

**Lemma 4.3.6.** *Let $D = -4a^3 - 27b^2$. Define rational functions $F_1, F_2$ on the curve with equation $u^2 - Dh(\lambda) = 0$, where*

$$F_1 = \left(-\frac{1}{4}a\lambda - \frac{1}{8}b\right)u + \frac{27}{8}b^2\lambda^3 - \frac{3}{4}a^2b\lambda^2 - \frac{3}{8}ab^2\lambda - \frac{1}{108}a^3b - \frac{1}{8}b^3,$$
$$F_2 = \left(\frac{1}{4}ab\lambda + \frac{1}{8}b^2\right)u + \left(-\frac{1}{2}a^3b - \frac{27}{8}b^3\right)\lambda^3 + \left(\frac{1}{9}a^5 + \frac{3}{4}a^2b^2\right)\lambda^2 + \left(\frac{1}{18}a^4b + \frac{3}{8}ab^3\right)\lambda$$
$$+ \frac{1}{729}a^6 + \frac{1}{36}a^3b^2 + \frac{1}{8}b^4.$$

*Let $h_1 = \frac{2^5 3^6 (F_2 + zF_1)}{D}$ and $h_2 = \frac{(b+z)(s+216z)}{2(s-216z)}$. Then $h_1h_2 = G^3$ for some rational function $G$. In particular, the function field of $X_E^-(6)$ over $K(z)$ is $K(z)(\lambda, u, \sqrt[3]{h_1})$.*

**Proof.** Define $H(\lambda) = \lambda^4 + \frac{2}{9}a\lambda^2 + \frac{4}{27}b\lambda - \frac{1}{243}a^2$ and

$$\begin{aligned} G_1 = {} & ((48a^5 + 324a^2b^2)\lambda^3 + (72a^4b + 486ab^3)\lambda^2 + (-\frac{16}{3}a^6 - 36a^3b^2)\lambda \\ & + (-\frac{8}{9}a^5b - 6a^2b^3))u + (648a^4b + 4374ab^3)z\lambda^5 + (-240a^6 - 1620a^3b^2)z\lambda^4 \\ & + (-240a^5b - 1620a^2b^3)z\lambda^3 + (-120a^4b^2 - 810ab^4)z\lambda^2 + (\frac{40}{9}a^6b + 30a^3b^3)z\lambda \\ & + \left(-\frac{16}{81}a^8 - \frac{20}{9}a^5b^2 - 6a^2b^4\right)z. \end{aligned}$$

Let $G = \frac{G_1}{H(\lambda)(4a^3+27b^2)^2}$ and a direct computation shows that $G^3 = h_1h_2$. $\square$

We can now prove Theorem 1.7.1.

**Proof.** The above lemma gives equations for $X_E^-(6)$ over $K(z)$. To obtain equations for $X_E^-(6)$ over $K$, it suffices to find the generating elements of the function field over $K$. Let $F_1, F_2, h_1$ be the functions as in the previous lemma and let $h_1'$ be the conjugate of $h_1$, i.e. $h_1' = \frac{2^5 3^6 (F_2 - zF_1)}{D}$ where $D = -4a^3 - 27b^2$. A direct computation shows that $h_1 h_1' = (4a(27x^2 + a))^3$. Therefore $h_1'$ is also contained in the function field of $X_E^-(6)$ over $K(z)$. Let $v = \sqrt[3]{h_1} + \sqrt[3]{h_1'}$. Then $v$ satisfies

$$v^3 - (324a\lambda^2 + 12a^2)v - \frac{2^6 3^6 F_2}{D} = 0$$

and so

$$v^3 - (324a\lambda^2 + 12a^2)v + 5832b\lambda^3 - 1296a^2\lambda^2 - 648ab\lambda - 16a^3 - 216b^2 + (186624ab\lambda + 93312b^2)u = 0.$$

Therefore, the function field of $X_E^-(6)$ over $K$ can be taken to be $K(\lambda, u, v)$ with $\lambda, u, v$ satisfying the above equation and $u^2 - Dh(\lambda) = 0$. Finally, let $x = \frac{\lambda}{3}$ and $y = \frac{u}{36}$ then we obtain the equations for $X_E^-(6)$ as in Theorem 1.7.1. In particular, by construction the forgetful map is given by

$$X_E^-(6) \to X_E^2(3), \; (x, y, z) \mapsto x/3.$$

□

## 4.4 Examples

The following example makes use of the equation for the Jacobian of $X_E^-(6)$.

**Example 4.4.1.** *Let $a = -27/8$ and $b = -27/8$ so that $E$ has equation $y^2 = x^3 - 27/8x - 27/8$. Then the curve $X_E^-(6)$ has a rational point*

$$(x, y, v) = (-3/4, 19683/128, 27/2).$$

*So $X_E^-(6)$ is an elliptic curve and so it is isomorphic to its Jacobian $y^2 = x^3 - 8/19683$. The curve $X_E^-(6)$ has positive rank. Therefore, we obtain infinitely many elliptic curves which are reversely 6-congruent to $E$.*

*For example, the point $(-3/4, 19683/128, 27/2)$ descends to the point $-1/4$ on $X_E^-(3)$, which corresponds to the elliptic curve*

$$y^2 = x^3 - 1944x - 46656.$$

*This curve is not isogenous to $E$.*

**Example 4.4.2.** *For each $v \in K$, let*

$$a = b = -\frac{27}{8}\frac{(24-v)^3(24+v)^3}{((576-24v+v^2)^2(576-24v-1/2v^2)}$$

*and $E : y^2 = x^3 + ax + b$. Then $(x, y, z)$ is a point on $X_E^-(6)$ where*

$$\begin{aligned} x &= -\frac{3}{2}\frac{(v-24)(v+24)^2}{(v-48)(v^2-24v+576)}, \\ y &= -2^{14}3^{13}\frac{(v-24)^6(v-12)^4(v+24)^6}{(v-48)^2(v^2-24v+576)^6(v^2+48v-1152)^3}, \\ z &= 1296\frac{(v-24)^2(v-12)(v+24)^2}{(v^2-24v+576)^2(v^2+48v-1152)}. \end{aligned}$$

*In particular, the point $v = 0$ corresponds to the curve $E : y^2 = x^3 - 27/8x - 27/8$ and the point $(-3/4, 19683/128, 27/2)$ on $X_E^-(6)$ as in the previous example, and this point corresponds to a curve which is non-isogenous to $E$. Therefore, we have infinitely many pairs of non-isogenous elliptic curves which are reversely* 6*-congruent.*

# 5 Twist of Modular Curves: Level Ten Structure

In this chapter we prove Theorem 1.7.11(i). The idea to build up the level ten structure from level five structure is similar to what we did in the previous section. Unfortunately we are not going to produce a simple equation for $X_E(10)$, but we are able to give explicitly infinitely many pairs of non-isogenous elliptic curves which are directly 10-congruent. Throughout, $K$ is a field of characteristic not equal to $2, 3$ or $5$ and $E : y^2 = x^3 + ax + b$ is an elliptic curve over $K$.

## 5.1 The General Setup

Since 5 is coprime to 2, we conclude that $E[10] = E[5] \oplus E[2]$. Then by compatibility of the Weil pairing, we can construct $X_E(10)$ as a fiber product of $X_E(2)$ and $X_E(5)$. So we have the following commutative diagram

$$\begin{array}{ccc} X_E(10) & \xrightarrow{\chi^+_{10,2}} & X_E(2) \\ \big\downarrow \chi^+_{10,5} & & \big\downarrow \chi^+_{2,1} \\ X_E(5) & \xrightarrow{\chi^+_{5,1}} & X(1) \end{array}$$

where $\chi^+_{10,5}$ is the quotient map by the action of $H_{10,5} \subset \mathrm{PSL}_2(\mathbb{Z}/10\mathbb{Z})$ and recall that

$$H_{10,5} = \ker(\mathrm{PSL}_2(\mathbb{Z}/10\mathbb{Z}) \to \mathrm{PSL}_2(\mathbb{Z}/5\mathbb{Z})) \cong \mathrm{PSL}_2(\mathbb{Z}/2\mathbb{Z}) \cong S_3.$$

The quotient map by the action of $C_3 \subset S_3$ gives us an intermediate modular curve between $X_E(10)$ and $X_E(5)$. By an argument which is similar to that in Lemma 4.1.1, we have a modular curve $X$ which parametrises families of elliptic curves $\mathcal{F}$ such that for each $F \in \mathcal{F}$, the curve $F$ is directly 5-congruent to $E$ and the quotient $\frac{\Delta_F}{\Delta_E}$ is a $K$-rational square. Therefore, the map $\chi^+_{10,5}$ factors through

$$X^{\pm}_E(10) \xrightarrow{\rho'} X \xrightarrow{\rho} X_E(5)$$

**Lemma 5.1.1.** *The curve $X$ is a hyperelliptic curve and it has equation*

$$y^2 = D(t)$$

*where $D(t)$ is the polynomial defined in Theorem 3.4.1.*

**Proof.** This follows immediately from the modular interpretation of $X$. By Theorem 3.4.1, we have $\Delta_{F_{5,t}} = \Delta_E D(t)^5$. So an equation for $X$ is

$$y^2 = \frac{\Delta_{F_{5,t}}}{\Delta_E} = D(t)^5.$$

Writing the above equation in the form

$$\left(\frac{y}{D(t)^2}\right)^2 = D(t)$$

we see that $X$ is isomorphic to the curve defined by

$$y^2 = D(t).$$

□

We now compute a model for $X_E(10)$, which is not as simple as what we did for the case $n = 6$. But we will see later that it is enough for us to get infinitely many pairs of non-isogenous directly 10-congruent elliptic curves.

**Theorem 5.1.2.** *The curve $X_E(10) \subset \mathbb{A}^3_{v,y,t}$ has equations $f = g = 0$ where*

$$f = y^2 - D(t),$$
$$g = B_5(t)(v^3 + av + b) - y^5\left(bv^3 - \frac{2}{3}a^2v^2 - abv - (\frac{2}{27}a^3 + b^2)\right).$$

*where $B_5(t)$ is the polynomial defined in Theorem 3.4.1. The forgetful map $\chi^+_{10,5} : X_E(10) \to X_E(5)$ is given by*

$$(v, y, t) \mapsto t.$$

**Proof.** Mod 2 representation is unchanged by taking quadratic twists. Based on this observation, we conclude that if $F$ is an elliptic curve which is 2-congruent to $E$, then $j(F) = \frac{(3av^2+9bv-a^2)^3 j(E)}{27a^3(v^3+av+b)^2}$ for some $v \in K$. Therefore, if we consider $X_E(10)$ as the fiber product of $X_E(5)$ and $X_E(2)$, then the equation for $X_E(10)$ is

$$j(F_{5,t}) = j(F_{2,v}).$$

This is equivalent of saying

$$\frac{B_5^2(t)}{\Delta_{F_{5,t}}} = \frac{\left(27bv^3 - 18a^2v^2 - 27abv - (2a^3 + 27b^2)\right)^2}{\Delta_{F_{2,v}}}$$

using Theorem 3.1.1. By previous lemma we know there is an intermediate curve with

$$\Delta_{F_{5,t}} = \Delta_E y^2$$

and by Theorem 3.1.1 we have $\Delta_{F_{2,v}} = 3^6(v^3 + av + b)^2 \Delta_E$. Then

$$\frac{B_5^2(t)}{y^{10}} = \frac{(27bv^3 - 18a^2v^2 - 27abv - (2a^3 + 27b^2))^2}{3^6(v^3 + av + b)^2}.$$

Taking square roots of both sides, we see that

$$\frac{B_5(t)}{y^5} = \frac{27bv^3 - 18a^2v^2 - 27abv - (2a^3 + 27b^2)}{27(v^3 + av + b)}.$$

Therefore, we have

$$B_5(t)(v^3 + av + b) - y^5 \left( bv^3 - \frac{2}{3}a^2v^2 - abv - (\frac{2}{27}a^3 + b^2) \right) = 0.$$

So the curve $X_E(10)$ can be defined by $f = g = 0$ as in the statement. Finally, since we construct $X_E(10)$ as a cover of $X_E(5)$ so the forgetful map is $(v, y, t) \mapsto t$. □

## 5.2 Examples of 10-Congruent Elliptic Curves

We now illustrate how to obtain infinitely many pairs of non-isogenous directly 10-congruent elliptic curves. Since the curve $X$ is a hyperelliptic curve of genus 5, so it only has finitely many $K$-rational points. Each $K$-rational point on $X_E(10)$ must descend to a $K$-rational point on $X$. Therefore to search for rational points on $X_E(10)$ we can firstly search for rational points on $X$.

We will use the idea in Section 1.6. We set $b = a$ in the equations of $X$ and $X_E(10)$ above and view $a$ as a variable. Then $f = g = 0$ defines a surface which is birational to the modular diagonal surface $Z_{10,1}$. We search for the rational points on this surface at $t = 0$. Then when $b = a$ and $t = 0$ we have

$$f = y^2 - \left( 91125 \left( \frac{-a}{27} \right)^6 - 193536 \left( \frac{-a}{27} \right)^3 \left( \frac{-a}{54} \right)^2 + 102400 \left( \frac{-a}{54} \right)^4 \right)).$$

Let $y' = \frac{27^2 y}{a^2}$. So we can rewrite $f = 0$ as

$$y'^2 - (125a^2 + 1792a + 6400) = 0$$

and so $f = 0$ defines a curve of genus zero with a rational point at infinity. So we can parametrise this curve and indeed, we have

$$a = \frac{8p^2 - 16p - 792}{-p^2 + 125}, \quad y = \frac{a^2(-8p^2 + 208p - 1000)}{3^6(-p^2 + 125)}.$$

Then we substitute these expressions into $g = 0$ where $g$ is the polynomial as in Theorem 5.1.2. We get a curve in $\mathbb{A}^2_{v,p}$ defined by

$$b_3(p)v^3 + b_2(p)v^2 + b_1(p)v + b_0(p) = 0$$

for some rational functions $b_3(p), b_2(p), b_1(p), b_0(p)$ in $p$. Divide the equation by $b_3(p)$. Then make a linear transformation in $v$ so that the equation is now in the form

$$v^3 + b_1'(p)v + b_0'(p) = 0.$$

A direct computation shows that the denominator of $b_1'(p)$ is $h(p)^2$ for some $h(p)$ and the denominator of $b_0'(p)$ is $h(p)^3$. Then replace $v$ by $v/h(p)$ and we can now reduce the equation to the form

$$v^3 + a_1(p)v + a_0(p) = 0$$

where

$$\begin{aligned}
a_1 &= -\frac{2^3 107^3}{3^3 7^2 31^2}(p-11)(p+9)^3(p^6 - \frac{3964}{107}p^5 + \frac{180721}{321}p^4 - \frac{1436000}{321}p^3 \\
&+ \frac{6243875}{321}p^2 - \frac{13887500}{321}p + \frac{11996875}{321})^3, \\
a_0 &= -\frac{2^3 \cdot 11 \cdot 107^3 \cdot 521}{3^6 7^3 31^3}(p-11)(p+9)^3(p^6 - \frac{3964}{107}p^5 + \frac{180721}{321}p^4 - \frac{1436000}{321}p^3 \\
&+ \frac{6243875}{321}p^2 - \frac{13887500}{321}p + \frac{11996875}{321})^3(p^{11} - \frac{265159}{5731}p^{10} + \frac{4424633}{5731}p^9 \\
&- \frac{1623487}{521}p^8 - \frac{443864802}{5731}p^7 + \frac{719927982}{521}p^6 - \frac{59913019598}{5731}p^5 + \frac{20902477250}{521}p^4 \\
&- \frac{271569140625}{5731}p^3 - \frac{111628015625}{521}p^2 + \frac{5146376953125}{5731}p - \frac{5982556640625}{5731}.
\end{aligned}$$

We can further simplify this by replacing $v$ by

$$\frac{2v}{5859}(p+9)(321p^6 - 11892p^5 + 180721p^4 - 1436000p^3 + 6243875p^2 - 13887500p + 11996875)$$

and so we obtain the equation $F(v,p)=0$ where

$$\begin{aligned}F(v,p) &= v^3 + (-642p^8 + 25068p^7 - 345452p^6 + 1240268p^5 + 17551008p^4 - 231577500p^3 \\ &+ 1156743500p^2 - 2701737500p + 2375381250)v + (-5731p^{12} + 328200p^{11} \\ &- 7341382p^{10} + 66529320p^9 + 247422875p^8 - 12801720624p^7 + 147024305420p^6 \\ &- 888970465328p^5 + 2800768887875p^4 - 1759352375000p^3 - 18653366843750p^2 \\ &+ 62592703125000p - 65808123046875).\end{aligned}$$

We now conclude that the curve we started with is isomorphic to $C \subset \mathbb{A}^2_{v,p}$ which has equation $F(v,p)=0$. In fact $C$ has genus one and $(v,p)=(2448,9)$ is a $K$-rational point on $C$. So we conclude that $C$ is an elliptic curve. The following map gives an isomorphism from the elliptic curve

$$C' : Y^2 - Y = X^3 + 5X^2 + X, \quad 121b1$$

to the curve $C$. Define

$$C' \to C, \quad (X,Y) \mapsto (v,p)$$

where

$$\begin{aligned}v &= ((-6400X^{10} - 25600X^9 - 55296X^8 - 82368X^7 - 78272X^6 - 47392X^5 - 24800X^4 \\ &- 11200X^3 + 240X^2 - 608X + 176)Y + 16000X^{11} + 78080X^{10} + 172160X^9 \\ &+ 228656X^8 + 228960X^7 + 188768X^6 + 97936X^5 + 33584X^4 + 14624X^3 - 336X^2 + 432X \\ &- 176)/(X^4(X^2+X-1)^4), \\ p &= \frac{-2Y + 11X^3 + 11X^2 - 7X + 2}{X^3 + X^2 - X}.\end{aligned}$$

The curve $C'$ has rank 1 and so we obtain a genus one curve with positive rank. Then as is shown in Section 1.6, to show that we actually have infinitely many pairs of non-isogenous 10-congruent elliptic curves, it suffices to show that we have a point on $C'$ which corresponds to a pair of non-isogenous elliptic curves. We now prove Theorem 1.7.11(i).

**Proof.** The above computation shows that we have a $K$-rational curve of genus one with positive rank on the surface which is birational to $Z_{10,1}$. Take a rational point $(X,Y) = (-4,-3)$ on $C'$, and this gives a point $(v,p) = \left(-\frac{42172272}{14641}, \frac{123}{11}\right)$ on $C$. Using

$$a = \frac{8p^2 - 16p - 792}{-p^2 + 125}, \quad y = \frac{a^2(-8p^2 + 208p - 1000)}{3^6(-p^2 + 125)}$$

we have $a = -888$ and $y = -\frac{862842368}{81}$. Recall that in the above computation we took $t = 0$ and $b = a$. So this means that we have a rational point on $X_E(10)$ when $E$ has equation $y^2 = x^3 - 888x - 888$ and under the forgetful map

$$\chi^+_{10,5} : X_E(10) \to X_E(5), \quad (v, y, t) \mapsto t$$

this rational point descends to $t = 0$ on $X_E(5)$. Therefore if we let $E'$ be the elliptic curve which corresponds to the point $t = 0$ on $X_E(5)$, then using the formula in Theorem 3.4.1 we conclude that $E'$ has equation

$$y^2 = x^3 - 202953498603672788288x + 5017791343940722107330892848.$$

We check that $E$ and $E'$ are non-isogenous. Therefore, on the curve $C'$, only finitely many points correspond to pairs of isogenous curves and so we have infinitely many pairs of non-isogenous directly 10-congruent elliptic curves. $\square$

**Remark** In the proof above, we did not give explicitly the rational point on $X_E(10)$ corresponding to $E'$ when $E$ has equation $y^2 = x^3 - 888x - 888$. We now illustrate how to do this, if we are interested in finding this point. Recall that this rational point is above $t = 0$ and we have computed that this point descends to $(y, t) = \left(-\frac{862842368}{81}, 0\right)$ on the curve $X$. Recall that $X$ has equation $y^2 - D(t) = 0$. When $b = a = -888$ we can check that $\left(-\frac{862842368}{81}, 0\right)$ is indeed a rational point on $X$. The rational point corresponding to the curve $E'$ on $X_E(10)$ should be a point above $\left(-\frac{862842368}{81}, 0\right)$ and so if we set $t = 0$ and $y = -\frac{862842368}{81}$, we should get a $K$-rational root of

$$B_5(t)(v^3 + av + b) - y^5 \left(bv^3 - \frac{2}{3}a^2v^2 - abv - (\frac{2}{27}a^3 + b^2)\right),$$

viewed as a cubic polynomial in $v$. Indeed, we have a root at $v = \frac{5546226}{695461}$. This shows that

$$(v, y, t) = \left(\frac{5546226}{695461}, -\frac{862842368}{81}, 0\right)$$

is the $K$-rational point on $X_E(10)$ which corresponds to $E'$.

The above computation allows us to give explicitly infinitely many examples of 10-congruent elliptic curves such that only finitely many pairs are isogenous.

**Corollary 5.2.1.** *The pairs of elliptic curves $E, E'$ are directly 10-congruent to each other where $E: y^2 = x^3 + ax + a$ with*

$$a = \frac{(-80X^3 - 80X^2 + 48X - 16)Y + 160X^4 + 1128X^3 + 872X^2 - 584X + 88}{(X^2 - 6X - 11)(X^2 + 4X - 1)^2}$$

*and $(X, Y)$ a $K$-rational point on $C' : Y^2 - Y = X^3 + 5X^2 + X$, and*

$$E' : y^2 = x^3 + A_5(0)x + B_5(0).$$

**Proof.** Since each rational point we found on curve $C$ corresponds to a rational point on $X_E(10)$ above $t = 0$, so we only need to work out the suitable values of $a$ and $b$. Recall we set $b = a$ and the isomorphism

$$C' \to C, \quad (X, Y) \mapsto (s, p)$$

has $p = \frac{-2Y+11X^3+11X^2-7X+2}{X^3+X^2-X}$. Finally, since $a = \frac{8p^2-16p-792}{-p^2+125}$, so we conclude that $a$ has the required expression in the statement. □

**Remark** We can work out the expressions of $A_5(0)$ and $B_5(0)$ in terms of $a$, and we have

$$A_5(0) = \frac{a^8(9375a^3 + 188375a^2 + 1261568a + 2816000)}{3^{21}}$$

and

$$\begin{aligned} B_5(0) = a^{11}(&7734375a^5 + 251446250a^4 + 3265084416a^3 + 21165619200a^2 \\ &+ 68485120000a + 88473600000)/(3^{33}). \end{aligned}$$

# 6 Twists Of Elliptic Curves: Level Eight Structure

We prove Theorem 1.7.2, 1.7.4, 1.7.3, 1.7.5 in this chapter. Let $K$ be a field of characteristic not equal to 2 or 3 and let $E : y^2 = x^3 + ax + b$ be an elliptic curve over $K$. We first fix a basis for $E[8]$ by the following lemma. Recall in Section 2.3 that the family of elliptic curves parametrised by $X(8)$ is

$$E_{u,X_1,X_2,X_3} : y^2 = x^3 - 27(256u^8 + 224u^4 + 1)x - 54(-4096u^{12} + 8448u^8 + 528u^4 - 1)$$

together with a $G_{\mathbb{Q}}$-invariant 8-torsion point $P_8$ and a $G_{\mathbb{Q}}$-invariant cyclic subgroup generated by $Q_8$.

**Lemma 6.0.2.** *We have*

$$4P_8 = (48u^4 + 72u^2 + 3, 0), \quad 4Q_8 = (-96u^4 - 6, 0).$$

*If $t_0$ is any point on $X(4)$ which corresponds to $E$, in the sense that the curve*

$$E_{t_0} : y^2 = x^3 - 27(256t_0^8 + 224t_0^4 + 1)x - 54(-4096t_0^{12} + 8448t_0^8 + 528t_0^4 - 1)$$

*is isomorphic to $E$ with isomorphism $f : E_{t_0} \to E$, then $f(48t_0^4+72t_0^2+3, 0)$ and $f(-96t_0^4-6, 0)$ are two non-trivial 2-torsion points of $E$. In particular, we fix a basis $\{P, Q\}$ for $E[8]$ such that*

$$4P = f(48t_0^4 + 72t_0^2 + 3, 0) := (\theta_1, 0), \quad 4Q = f(-96t_0^4 - 6, 0) := (\theta_2, 0)$$

**Proof.** A direct computation gives the coordinates of $4P_8$ and $4Q_8$. Since $t_0$ is a point such that $E_{t_0}$ has the same $j$-invariant as $E$, we conclude that $(48t_0^4+72t_0^2+3, 0)$ and $(-96t_0^4-6, 0)$ are two non-trivial 2-torsion points on $E_{t_0}$. The result follows because $f : E_{t_0} \to E$ is an isomorphism. □

We write $(\theta_3, 0)$ for the other non-trivial 2-torsion point of $E$. So the above lemma also implies that $\theta_j, j = 1, 2, 3$ are distinct roots of $x^3 + ax + b = 0$.

## 6.1 Extension of Function Fields

Let $r \in (\mathbb{Z}/8\mathbb{Z})^*$. Our strategy is to construct $X_E^r(8)$ as a cover of $X_E^{\bar{r}}(4)$ where $r \equiv \bar{r} \bmod 4$ by studying the function fields of these curves. In Section 2.3, we have seen that over $K(\zeta_8)$, the function field of $X(8)$ is a $(\mathbb{Z}/2\mathbb{Z})^3$ extension of the function field of $X(4)$. Explicitly, recall in Section 2.3 that if we fix an isomorphism $X(4) \cong \mathbb{A}^1_u$, then $X(8) \subset \mathbb{A}^1_{u,X_1,X_2,X_3}$ has equations

$$X_1^2 = u^2 - 1/4, \quad X_2^2 = -u, \quad X_3^2 = u^2 + 1/4 \qquad (\dagger)$$

and so the function field of $X(8)$ over $K(\zeta_8)$ is

$$K(\zeta_8)(u, \sqrt{u^2 - 1/4}, \sqrt{-u}, \sqrt{u^2 + 1/4}).$$

In particular, the zeroes of the rational functions

$$u^2 - 1/4, \quad -u, \quad u^2 + 1/4$$

are the cusps of $X(4)$. Explicitly,

$$\begin{aligned}
\operatorname{div}(u^2 - 1/4) &= (1/2) + (-1/2) - 2(\infty), \\
\operatorname{div}(-u) &= (0) - (\infty) = (0) + (\infty) - 2(\infty), \\
\operatorname{div}(u^2 + 1/4) &= (i/2) + (-i/2) - 2(\infty).
\end{aligned}$$

For each $r = 1, 3, 5, 7$, the curve $X_E^r(8)$ is a twist of $X(8)$. So the function field of $X_E^r(8)$ is isomorphic to the function field of $X(8)$ over $\bar{K}$. Explicitly, if we fix an isomorphism $X_E^{\bar{r}}(4) \cong \mathbb{P}^1_t$ as in Theorem 3.3.1 and 3.3.2 and identify the function field of $X_E^{\bar{r}}(4)$ over $\bar{K}$ with $\bar{K}(t)$, then the function field of $X_E^r(8)$ over $\bar{K}$ can be written as

$$\bar{K}(t, \sqrt{g_1}, \sqrt{g_2}, \sqrt{g_3})$$

for some rational functions $g_i \in \bar{K}(t)$ and the zeroes of $g_i$ are cusps of $X_E(4)$. This suggests we do the following computations.

**Lemma 6.1.1.** *Let $t_1, \ldots, t_6$ be the cusps of $X_E(4)$ which are the images of $\pm\frac{1}{2}, 0, \infty, \pm\frac{i}{2}$ respectively, under the isomorphism $X(4) \to X_E(4)$ in Section 3.3. Let*

$$m_j = t_{2j-1} + t_{2j} \text{ and } l_j = t_{2j-1}t_{2j}, \;\; j = 1, 2, 3.$$

*Then $m_j = \frac{2}{3}\theta_j$ and $l_j = -\frac{1}{9}(2\theta_j^2 + a)$ for each $j = 1, 2, 3$.*

**Proof.** Take $t_0$ as in the previous lemma and note that $t_1, \ldots, t_6$ depend on $t_0$. Then $\theta_j, j = 1, 2, 3$ can be written explicitly in terms of $t_0$. On the other hand, $t_1, \ldots, t_6$ can be computed using the algorithm introduced in Section 3.3. The result follows from a direct computation. $\square$

**Lemma 6.1.2.** *For each $r \in (\mathbb{Z}/8\mathbb{Z})^*$, the rational functions $g_i, i = 1, 2, 3$ above can be taken to be*

$$g_j = (t - t_{2j-1})(t - t_{2j}), \quad j = 1, 2, 3$$

*where $t_1, \ldots, t_6$ are images of $\pm\frac{1}{2}, 0, \infty, \pm\frac{i}{2}$ under the isomorphism $X(4) \to X_E(4)$ described in Theorem 3.3.1. Moreover,*

$$g_j = t^2 - \frac{2}{3}\theta_j - \frac{1}{9}(2\theta_j^2 + a)$$

*and each $g_j$ is defined over $K(\theta_j) \subset K(E[2])$. In particular, the function field of $X_E^r(8)$ over $K(E[2])$ is given by*

$$K(E[2])(t, \sqrt{\alpha_{r,1}g_1}, \sqrt{\alpha_{r,2}g_2}, \sqrt{\alpha_{r,3}g_3})$$

*for some scaling factors $\alpha_{r,i}, i = 1, 2, 3$.*

**Proof.** Theorem 3.3.2 identifies $X_E^3(4)$ with $X_E(4)$. The isomorphism $X(4) \to X_E^3(4)$ can be taken to be exactly the same as $X(4) \to X_E(4)$ and $X_E^3(4)$ has the same cusps as $X_E(4)$.

The isomorphism $X(4) \to X_E(4)$ induces an isomorphism of function fields $\bar{K}(X_E(4)) \to \bar{K}(X(4))$. In particular, $g_1, g_2, g_3$ are images of $u^2 - 1/4, -u, u^2 + 1/4$ respectively, and so

$$\begin{aligned}
\operatorname{div}(g_1) &= (t_1) + (t_2) - 2(t_4), \\
\operatorname{div}(g_2) &= (t_3) - (t_4), \\
\operatorname{div}(g_3) &= (t_5) + (t_6) - 2(t_4).
\end{aligned}$$

We are free to replace $g_i$ by $g_i h_i^2$ for some rational function $h_i \in \bar{K}(t)$ because

$$\bar{K}(t, \sqrt{g_1}, \sqrt{g_2}, \sqrt{g_3}) = \bar{K}\left(t, \sqrt{g_1 h_1^2}, \sqrt{g_2 h_2^2}, \sqrt{g_3 h_3^2}\right).$$

Since any degree zero divisor is principal over $\mathbb{P}^1$, we can take $g_j$ such that

$$\begin{aligned}
\operatorname{div}(g_1) &= (t_1) + (t_2) - 2(t_4) + 2D, \\
\operatorname{div}(g_2) &= (t_3) - (t_4) + 2D, \\
\operatorname{div}(g_3) &= (t_5) + (t_6) - 2(t_4) + 2D,
\end{aligned}$$

for some degree zero divisor $D$. Taking $D$ to be $2(t_4) - 2(\infty)$ gives the required rational functions $g_j$ up to scaling factors. The second part follows from the previous lemma. $\square$

**Corollary 6.1.3.** *For each $r \in (\mathbb{Z}/8\mathbb{Z})^*$, the equations of $X_E^r(8) \subset \mathbb{P}^4_{t,u_0,u_1,u_2,s}/K$ are determined by the scaling factors $\alpha_{r,j}, j = 1,2,3$. In particular, the equations of $X_E^r(8)$ over $K$ is obtained by comparing the coefficients of $1, \theta_j, \theta_j^2, j = 1,2,3$ in the equations*

$$\alpha_{r,j}(t - t_{2j-1}s)(t - t_{2j}s) = (u_0 + u_1\theta_j + u_2\theta_j^2)^2, j = 1,2,3.$$

*The forgetful map $X_E^r(8) \to X_E^{\bar{r}}(4)$ is $(t : u_0 : u_1 : u_2 : s) \mapsto (t : s)$.*

**Proof.** Let $L_1 = K(E[2])(X_E^r(8))$ and $L_2 = K(X_E^r(8))$. Then $L_1/L_2$ is Galois. Therefore to find a model of $X_E^r(8)$ over $K$, it suffices to find enough generating elements in the function field of $X_E^r(8)$ over $K(E[2])$ which are fixed by $\mathrm{Gal}(K(E[2])/K)$. Explicitly, we write $w_j := \sqrt{\alpha_{r,j}(t - t_{2j-1})(t - t_{2j})}$ and so $w_j^2 = \alpha_{r,j}(t - t_{2j-1})(t - t_{2j})$ for each $j = 1,2,3$.

By Lemma 6.1.2, $w_j = u_0 + u_1\theta_j + u_2\theta_j^2$ for some $u_0, u_1, u_2 \in K(X_E^r(8))$ for each $j = 1,2,3$. Therefore we obtain equations

$$\alpha_{r,j}(t - t_{2j-1})(t - t_{2j}) = (u_0 + u_1\theta_j + u_2\theta_j^2)^2, j = 1,2,3.$$

Taking homogenous coordinates gives

$$\alpha_{r,j}(t - t_{2j-1}s)(t - t_{2j}s) = (u_0 + u_1\theta_j + u_2\theta_j^2)^2, j = 1,2,3.$$

To find a model of $X_E^r(8)$ over $K$, it suffices to compare the coefficients of $1, \theta_j, \theta_j^2$, $j = 1,2,3$ on both sides of the equations above because these are invariant under the action of $\mathrm{Gal}(K(E[2])/K)$. □

**Remark** Note that we only need to compare the coefficients of $1, \theta_j, \theta_j^2$ for one of the three equations. In fact, we can understand the three equations in terms of one equation

$$\alpha_r(u_0 + u_1\theta + u_2\theta^2) = t^2 - \frac{2}{3}\theta - \frac{1}{9}(2\theta^2 + a)$$

together with the $K$-algebra homomorphisms $K[x]/\langle x^3 + ax + b\rangle \to \bar{K}$, where $\theta_1, \theta_2, \theta_3$ are the images of $\theta$ and $\alpha_{r,1}, \alpha_{r,2}, \alpha_{r,3}$ are the images of $\alpha_r$. Then equations for $X_E^r(8)$ can be obtained from comparing the coefficients of $1, \theta, \theta^2$.

We are free to multiply $\alpha_r$ by a non-zero squared factor of the form $(v_0 + v_1\theta + v_2\theta^2)^2$ for some $v_0, v_1, v_2 \in K$ because this leads to a change of coordinate in $u_0, u_1, u_2$.

## 6.2 The Curve $X_E(8)$

We now prove Theorem 1.7.2 by determining the scaling factors $\alpha_{1,j}, j = 1, 2, 3$.

**Proof.** There is always a tautological rational point on the curve $X_E(n)$ for any $n$ which corresponds to the pair $(E, [1])$. The point on $X_E(4)$ corresponding to $(E, [1])$ is given by the point of infinity under the isomorphism we described in Section 3. Since we construct $X_E(8)$ as a cover of $X_E(4)$, there is a point on $X_E(8)$ above $t = \infty$ which corresponds to $(E, [1])$. By a change of coordinate of $u_0, u_1, u_2$, we may take this point to be $t = \infty, u_0 = 1, u_1 = 0, u_2 = 0$.

By Corollary 6.1.3, the equations for the affine piece of $X_E(8)$ over $K$ are determined by comparing the coefficients of $1, \theta_j, \theta_j^2$ in the equations

$$\alpha_{1,j}(t - t_{2j-1})(t - t_{2j}) = (u_0 + u_1\theta_j + u_2\theta_j^2)^2, j = 1, 2, 3$$

Taking homogenous coordinates in the above equations we have

$$\alpha_{1,j}(t - t_{2j-1}s)(t - t_{2j}s) = (u_0 + u_1\theta_j + u_2\theta_j^2)^2, j = 1, 2, 3$$

and so the point $t = \infty, u_0 = 1, u_1 = 0, u_2 = 0$ is now $(t : u_0 : u_1 : u_2 : s) = (1 : 1 : 0 : 0 : 0)$. Substituting this point into the equations, we conclude that we can take $\alpha_{1,j}, j = 1, 2, 3$ to be 1. Finally, we make the substitution $(x_0 : x_1 : x_2 : x_3 : x_4) = (t : u_0 : u_1 : u_2 : \frac{s}{3})$ to get the equations in Theorem 1.7.2. $\square$

The following lemma will be useful when we compute $X_E^r(8)$ with $r = 3, 7$. Recall the group $H_{8,4}$ is the kernel of the reduction map $\mathrm{PSL}_2(\mathbb{Z}/8\mathbb{Z}) \to \mathrm{PSL}_2(\mathbb{Z}/4\mathbb{Z})$ and we have described the action of $H_{8,4}$ on the modular curve $X(8)$ in Section 2.3. We now consider the action of $H_{8,4}$ on $X_E(8)$.

**Lemma 6.2.1.** *Let* $Y_1 = \sqrt{(t - t_1)(t - t_2)}, Y_2 = \sqrt{(t - t_3)(t - t_4)}$, *and* $Y_3 = \sqrt{(t - t_5)(t - t_6)}$. *Then the action of* $H_{8,4}$ *on* $X_E(8)$ *can be read off from the action of* $H_{8,4}$ *on* $t, Y_1, Y_2, Y_3$. *In particular, if we take generators* $S_1, S_2, S_3$ *for* $H_{8,4}$ *where*

$$S_1 = \begin{pmatrix} 1 & 4 \\ 4 & 1 \end{pmatrix}, S_2 = \begin{pmatrix} 3 & 4 \\ 4 & 3 \end{pmatrix}, S_3 = \begin{pmatrix} 1 & 0 \\ 4 & 1 \end{pmatrix},$$

*then*

$$\begin{aligned} S_1(t,Y_1,Y_2,Y_3) &= (t,-Y_1,-Y_2,Y_3), \\ S_2(t,Y_1,Y_2,Y_3) &= (t,Y_1,Y_2,-Y_3), \\ S_3(t,Y_1,Y_2,Y_3) &= (t,Y_1,-Y_2,Y_3). \end{aligned}$$

**Proof.** $S_j, j = 1,2,3$ fixes the $t$-coordinate because $S_j \equiv I \bmod 4$ and the forgetful map from $X_E(8) \to X_E(4)$ is $(t,u_0,u_1,u_2) \mapsto t$. The action of $S_j$ on $X_E(8)$ can be computed by the composition

$$S_i \circ Y_k = \psi_8(S_i(\psi_8^{-1}(Y_k)))$$

where $\psi_8 : X(8) \to X_E(8)$ is the isomorphism which matches up each $X_k$ (see (†)) with $Y_k$, $k = 1,2,3$. Therefore the result follows from Lemma 2.3.3. □

**Remark** The rational points on $X_E^r(8)$, $r = 1,3,5,7$, appear in pairs. In other words, if $(t,x_0,x_1,x_2) \in X_E^r(8)$ then $(t,-x_0,-x_1,-x_2) \in X_E^r(8)$ because there is a non-trivial automorphism on $X_E^r(8)$ given by

$$(F,\phi) \mapsto (F,\phi \circ [3]).$$

## 6.3 The Curve $X_E^5(8)$

We will prove Theorem 1.7.4 in this section by determining the scaling factors $\alpha_{5,j}, j = 1,2,3$. By compatibility of the Weil pairing, $X_E^5(8)$ is also a cover of $X_E(4)$. The proof of Theorem 1.7.4 is based on the following observations.

**Lemma 6.3.1.** *Let $m$ be an even number. Let $E$ be an elliptic curve and fix any basis $\{P,Q\}$ for $E[2m]$. Then the map*

$$\phi : E[2m] \to E[2m],\ \phi(P) = (m+1)P,\ \phi(Q) = Q$$

*is $G_{L'}$-equivariant where $L' = K(E[2])$.*

**Proof.** The non-trivial 2-torsion points $mP, mQ$ and $mP+mQ$ are $L'$-rational. Let $s \in G_{L'}$ and write

$$s(P) = A_1P + A_2Q, \quad s(Q) = A_3P + A_4Q.$$

Then $s(mP) = mP$ and $s(mQ) = mQ$. So $A_2$ and $A_3$ are both even. Since the matrix $I + 4\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ commutes with matrices of the form $I + 2\begin{pmatrix} * & * \\ * & * \end{pmatrix}$ in $\mathrm{GL}_2(\mathbb{Z}/2m\mathbb{Z})$, we conclude that $\phi(s(P)) = s(\phi(P))$ and $\phi(s(Q)) = s(\phi(Q))$. $\square$

**Lemma 6.3.2.** *Let $m$ be an even number. If the modular curves $X_E^{m+1}(2m)$ and $X_E(2m)$ are isomorphic over a field extension $F$ of $K$, as covers of $X_E(m)$, then $\Delta_E$ is a square in $F$.*

**Proof.** Fix a basis $\{P, Q\}$ for $E[2m]$. If $X_E^{m+1}(2m) \cong X_E(2m)$ as covers of $X_E(m)$ then there exists a $G_F$-equivariant isomorphism $\phi : E[2m] \to E[2m]$, such that if we view $\phi$ as a $2 \times 2$ matrix in terms of its action on $P$ and $Q$, then $\det \phi = m + 1$ and $\phi$ acts trivially on $E[m]$ modulo $[-1]$. This shows that $\phi \equiv \pm I \bmod m$. The set

$$\{\phi \in \mathrm{GL}_2(\mathbb{Z}/2m\mathbb{Z}) : \phi \equiv \pm I(\bmod m), \det \phi = m + 1\}$$

has 8 elements, which are

$$M_1 = \begin{pmatrix} 1 & 0 \\ 0 & m+1 \end{pmatrix}, M_2 = \begin{pmatrix} 1 & m \\ 0 & m+1 \end{pmatrix}, M_3 = \begin{pmatrix} 1 & 0 \\ m & m+1 \end{pmatrix}, M_4 = \begin{pmatrix} 1 & m \\ m & m+1 \end{pmatrix}$$

and

$$M_5 = \begin{pmatrix} m+1 & 0 \\ 0 & 1 \end{pmatrix}, M_6 = \begin{pmatrix} m+1 & m \\ 0 & 1 \end{pmatrix}, M_7 = \begin{pmatrix} m+1 & 0 \\ m & 1 \end{pmatrix}, M_8 = \begin{pmatrix} m+1 & m \\ m & 1 \end{pmatrix}.$$

These elements are similar to either $M_1$ or $M_4$.

Let $\nu$ be the composition of the maps

$$\mathrm{GL}_2(\mathbb{Z}/2m\mathbb{Z}) \longrightarrow \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \xrightarrow{\cong} S_3 \xrightarrow{\mathrm{sgn}} \{\pm 1\}.$$

For each $s \in G_F$, we identify $s$ with its image under

$$\theta : G_F \to \mathrm{Aut}(E[2m]) \subset \mathrm{GL}_2(\mathbb{Z}/2m\mathbb{Z}).$$

Then the action of $s$ on $\sqrt{\Delta_E}$ is

$$s \circ \sqrt{\Delta_E} = \nu(\theta(s))\sqrt{\Delta_E}.$$

Since $s\phi = \phi s$, we conclude that $s$ is in the centraliser of either $M_1$ or $M_4$. A direct calculation shows the centraliser of $M_1$ is of the form $I + 2\begin{pmatrix} * & * \\ * & * \end{pmatrix}$ and the centraliser of $M_4$ is of the form $\begin{pmatrix} A_1 & A_2 \\ A_3 & A_4 \end{pmatrix}$ where $A_2 \equiv A_3 \bmod 2$ and $A_1+A_2+A_4 \equiv 0 \bmod 2$. Therefore, $\nu(\theta(s)) = 1$ and so $\Delta_E$ is a square in $F$. □

**Theorem 6.3.3.** *We can pick $\alpha_{5,j}$ to be $-4a^3 - 27b^2$ for each $j = 1, 2, 3$. In particular, we obtain the equation of $X_E^5(8)$ as stated in Theorem 1.7.4, together with the forgetful map $X_E^5(8) \to X_E(4)$ given by $(x_0 : x_1 : x_2 : x_3 : x_4) \mapsto \frac{x_0}{3x_4}$.*

**Proof.** By Lemma 6.3.1, there is a $K(E[2])$-rational point on $X_E^5(8)$ above $t = \infty$ which corresponds to $(E, \phi)$ where $\phi$ is the same map as in Lemma 6.3.1 with $m = 4$. Therefore $\alpha_{5,j}, j = 1, 2, 3$ are squares in $K(E[2])$. But there is at most one quadratic subfield inside $K(E[2])$ which is $K(\sqrt{D})$ where $D = -4a^3 - 27b^2$.

By the last remark in Section 6.1, $\alpha_{5,j}$ can be multiplied by any non-zero squared factor of the form $(v_0 + v_1\theta_j + v_2\theta_j^2)^2$. This shows that we may pick $\alpha_{5,j}, j = 1, 2, 3$ to be 1 or $D$. But by Lemma 6.3.2 with $m = 4$, if $\alpha_{5,j} = 1, j = 1, 2, 3$ then $D$ is a square in $K$ and so we should pick $\alpha_{5,j} = D$ for each $j$.

We now use the fact that $D = (\theta_1 - \theta_2)^2(\theta_1 - \theta_3)^2(\theta_2 - \theta_3)^2$ and so we can in fact take

$$\alpha_{5,1} = (\theta_2 - \theta_3)^2, \quad \alpha_{5,2} = (\theta_1 - \theta_3)^2, \quad \alpha_{5,3} = (\theta_1 - \theta_2)^2$$

because $(\theta_i - \theta_j)^2(\theta_i - \theta_k)^2$ is a square in $K(\theta_i)$ for $i \neq j \neq k$. Finally, we make the substitution $(x_0 : x_1 : x_2 : x_3 : x_4) = (t : u_0 : u_1 : u_2 : \frac{s}{3})$ to get the equations stated in Theorem 1.7.4. □

## 6.4 Some Cocycle Calculations

The proofs of Theorem 1.7.2 and Theorem 1.7.4 are based on the fact there is always a rational point on the curve $X_E(8)$. However this is not always true for $X_E^3(8)$ or $X_E^7(8)$, for any elliptic curve $E$. We will prove Theorem 1.7.3 and 1.7.5 by some cocycle computations. By Corollary 6.1.3, it suffices to compute $\alpha_{3,j}$ and $\alpha_{7,j}, j = 1, 2, 3$.

Recall from Theorem 1.5.6 that the curves $X_E^r(n)$ are twists of $X(n)$. In particular, the curves $X_E^r(8)$ are twists of $X_E(8)$ for each $r \in (\mathbb{Z}/8\mathbb{Z})^*$. By Theorem 1.5.3(ii), for each curve

$C/K$, there is a bijection between the twists of $C/K$ and $H^1(G_K, \mathrm{Aut}(C))$ where $\mathrm{Aut}(C)$ is the automorphism group of $C$. In this section, we will describe the relation between the scaling factors $\alpha_{r,j}, j = 1, 2, 3$ introduced in Lemma 3.3 and the element which corresponds to $X_E^r(8)$ in $H^1(G_K, \mathrm{Aut}(X_E(8)))$. For simplicity, we assume that $x^3 + ax + b$ is irreducible.

We note that each automorphism of $E[8]$ naturally gives rise to an automorphism of $X_E(8)$.

**Lemma 6.4.1.** *Fix $r \in (\mathbb{Z}/8\mathbb{Z})^*$. Let $\tau$ be an automorphism on $E[8]$ which switches the Weil pairing to the power of $r$. Then for each $s \in G_K$, $s \mapsto ({}^s\tau)\tau^{-1}$ defines a cocycle in $H^1(G_K, Aut(X_E(8)))$ which corresponds to $X_E^r(8)$.*

**Proof.** For each $s \in G_K$, $({}^s\tau)\tau^{-1}$ is an automorphism on $E[8]$ preserving the Weil pairing, which induces an automorphism on $X_E(8)$. Note $[-1]$ acts trivially on $X_E(8)$. By an argument similar to that in Theorem 1.5.6, we conclude that the curve corresponding to this cocycle is $X_E^r(8)$.

□

**Remark** If $({}^s\tau)\tau^{-1}$ acts trivially on $E[4]$ modulo $[-1]$ for all $s \in G_K$ then we have an isomorphism between $X_E(8)$ and $X_E^r(8)$ respecting the level four structure.

Recall that $H_{8,4} \cong (\mathbb{Z}/2\mathbb{Z})^3$ is the kernel of the reduction map $\mathrm{PSL}_2(\mathbb{Z}/8\mathbb{Z}) \to \mathrm{PSL}_2(\mathbb{Z}/4\mathbb{Z})$. We may also identify $H_{8,4}$ as a subgroup of $\mathrm{Aut}(X_E(8))$ and this makes $H_{8,4}$ a $G_K$-module. Define $H'$ to be the kernel of

$$\mathrm{GL}_2(\mathbb{Z}/8\mathbb{Z})/\{\pm I\} \to \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})/\{\pm I, \pm v\}$$

where

$$v = \begin{pmatrix} 1 & 2 \\ 2 & 3 \end{pmatrix}.$$

It can be checked that $H'$ is Abelian and is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^3 \times (\mathbb{Z}/4\mathbb{Z})$. By Proposition 3.3.3 the matrix $v$ induces a $G_K$-equivariant isomorphism between $E[4]$ and $E^{\Delta_E}[4]$ which switches the Weil pairing to the power of 3, and so $v$ identifies $X_E^3(4)$ with $X_E(4)$.

Since $H$ is a subgroup of $H'$, $\det v = -1$ and $\begin{pmatrix} 1 & 0 \\ 0 & 5 \end{pmatrix} \in H'$, the following sequence

$$0 \longrightarrow H_{8,4} \longrightarrow H' \xrightarrow{\det} (\mathbb{Z}/8\mathbb{Z})^* \longrightarrow 0$$

is exact.

We have a $\mathrm{GL}_2(\mathbb{Z}/8\mathbb{Z})$ action on $H'$ given by $g \mapsto^s g := sgs^{-1}$ for each $s \in \mathrm{GL}_2(\mathbb{Z}/8\mathbb{Z})$. By identifying $G_K$ with its image under $\rho_{E,8} : G_K \to \mathrm{Aut}(E[8]) \subset \mathrm{GL}_2(\mathbb{Z}/8\mathbb{Z})$, we obtain an action of $G_K$ on $H'$ and so $H'$ can be viewed as a $G_K$-module. Further we take the trivial action of $G_K$ on $(\mathbb{Z}/8\mathbb{Z})^*$.

Now viewing $H, H', (\mathbb{Z}/8\mathbb{Z})^*$ as $G_K$-modules we obtain a long exact sequence of $G_K$-modules and in particular we obtain the connecting map

$$(\mathbb{Z}/8\mathbb{Z})^* \to H^1(G_K, H_{8,4}) \tag{$\dagger$}$$

The image of $r \in (\mathbb{Z}/8\mathbb{Z})^*$ can be computed as follows. Pick a lift $v'$ of $r$ in $H'$. Then the image of $r$ in $H^1(G_K, H_{8,4})$ is $s \mapsto ({}^s v')v'^{-1}$ for each $s \in G_K$. Therefore, $X_E^r(8)$ is the curve corresponding to this cocycle by Lemma 6.4.1.

Recall that each non-cuspidal point on $X_E^r(n)$ corresponds to a pair $(F, \phi)$ where $F$ is an elliptic curve and $\phi : E[n] \to F[n]$ is a $G_K$-equivariant isomorphism which switches the Weil pairing to the power of $r$. We consider the image of 7 under the map ($\dagger$). Since we already obtain the image of 5 in Theorem 6.3.3 and the map ($\dagger$) is a group homomorphism, the image of 7 can be then used to compute the image of 3.

**Lemma 6.4.2.** *The image of* 7 *under* $(\mathbb{Z}/8\mathbb{Z})^* \to H^1(G_K, H_{8,4})$ *induces an isomorphism* $\psi : X_E^7(8) \to X_E(8)$ *subject to the following commutative diagram*

$$\begin{array}{ccc} X_E^7(8) & \xrightarrow{\psi} & X_E(8) \\ \big\downarrow & & \big\downarrow \\ X_E^3(4) & \xrightarrow{\eta} & X_E(4) \end{array}$$

*where* $\psi(F, \phi) = (F, \phi \circ v')$ *and* $\eta(F, \phi) = (F, \phi \circ v)$. *Moreover, we have*

$$\eta : X_E^3(4) \cong \mathbb{P}^1 \ni t \mapsto t \in \mathbb{P}^1 \cong X_E(4).$$

*The map* $\psi$ *induces an isomorphism*

$$t \mapsto t, \quad \sqrt{\alpha_{7,j}(t - t_{2j-1})(t - t_{2j})} \mapsto \sqrt{\alpha_{1,j}(t - t_{2j-1})(t - t_{2j})}, j = 1, 2, 3$$

*between the function field of* $X_E^7(8)$ *and* $X_E(8)$ *over* $K(E[2])$.

**Proof.** For each $s \in G_K$, we have

$$\begin{aligned}({}^s\psi)\psi^{-1}(F,\phi) &= s(\psi(s^{-1}(F,\phi\circ v'^{-1}) = s(\psi({}^{s^{-1}}F,\ {}^{s^{-1}}(\phi\circ v'^{-1}))) \\ &= s({}^{s^{-1}}F,\ {}^{s^{-1}}(\phi\circ v'^{-1})\circ v') = (F,\phi\circ(v'^{-1}\ {}^s v')).\end{aligned}$$

Similarly, $({}^s\eta)\eta^{-1}(F,\phi) = (F,\phi\circ(v^{-1}\ {}^s v))$. The Galois conjugate $({}^s\psi)\psi^{-1}$ induces an automorphism on $X_E(8)$ which can be read off from $v'^{-1}({}^s v')$. So $\psi$ corresponds to the cocycle $s \mapsto v'^{-1}({}^s v')$ which is the image of 7. The diagram commutes because $v' \equiv v \bmod 4$.

Proposition 3.3.3 shows that $\eta(t) = t$. Corollary 6.1.3 gives the corresponding statement for $\psi$. $\square$

Let $v' = \begin{pmatrix} 1 & 2 \\ 6 & 3 \end{pmatrix}$ be a lift of 7 in $H'$. For each $s \in G_K$, we identify $s$ with its image under $\rho_{E,8} : G_K \to \mathrm{Aut}(E[8]) \subset \mathrm{GL}_2(\mathbb{Z}/8\mathbb{Z})$. Then the action of $s$ on $v'$ is given by conjugation. The image of 7 can be read off from the following lemma.

**Lemma 6.4.3.** *Take generators $s_1, s_2, s_3, s_4$ for $\mathrm{GL}_2(\mathbb{Z}/8\mathbb{Z})$ where*

$$s_1 = \begin{pmatrix} 7 & 0 \\ 0 & 1 \end{pmatrix}, s_2 = \begin{pmatrix} 5 & 0 \\ 0 & 1 \end{pmatrix}, s_3 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, s_4 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

*Let $C_{s_j}$ be the image of $v'^{-1}({}^{s_j}v') := v'^{-1}s_j v' s_j^{-1}$ under $\mathrm{GL}_2(\mathbb{Z}/8\mathbb{Z}) \to \mathrm{PSL}_2(\mathbb{Z}/8\mathbb{Z})$. Then*

$$C_{s_1} = \begin{pmatrix} 1 & 4 \\ 4 & 1 \end{pmatrix}, C_{s_2} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, C_{s_3} = \begin{pmatrix} 3 & 4 \\ 4 & 3 \end{pmatrix}, C_{s_4} = \begin{pmatrix} 1 & 0 \\ 4 & 1 \end{pmatrix}.$$

**Proof.** This follows from a direct computation. $\square$

**Remark** It does not matter whether $\rho_{E,8} : G_K \to \mathrm{Aut}(E[8]) \subset \mathrm{GL}_2(\mathbb{Z}/8\mathbb{Z})$ is surjective or not because the image of $\rho_{E,8}$ is a subgroup of $\mathrm{GL}_2(\mathbb{Z}/8\mathbb{Z})$ and so the image of 7 under (†) in $H^1(G_K, H_{8,4})$ can be read off from $C_{s_j}, j = 1,2,3,4$. In other words, Lemma 5.3 specifies an element of $H^1(\mathrm{GL}_2(\mathbb{Z}/8\mathbb{Z}), H_{8,4})$, and via $\rho_{E,8}$ this determines an element of $H^1(G_K, H_{8,4})$.

Lemma 6.4.2 and 6.4.3 give concrete descriptions of $X_E^7(8)$ in terms of the image of 7 under (†). On the other hand, the equation of $X_E^7(8)$ is determined by the scaling factors $\alpha_{7,j}, j = 1,2,3$ by Corollary 6.1.3

The following lemmas show how these scaling factors are related to the image of 7 in $H^1(G_K, H_{8,4})$. Let $T_j = (\theta_j, 0), j = 1, 2, 3$ be the non-trivial 2-torsion points of $E$ where $\theta_j, j = 1, 2, 3$ were defined in Lemma 6.0.2. Let $M$ be the group $\mathrm{Map}(E[2]\backslash\{O\}, \mu_2)$ where the group operation is defined by $(\chi_1 \circ \chi_2)(T_j) = \chi_1(T_j)\chi_2(T_j), j = 1, 2, 3$. We identify each element $\chi \in M$ with a triple $(e_1, e_2, e_3)$ where $e_j \in \{\pm 1\}$ in the sense that $\chi(T_j) = e_j$.

**Lemma 6.4.4.** *For each $s \in G_K$, we define the action ${}^s\chi$ by $\chi s^{-1}$ as we have trivial action on $\mu_2$. Then*

$$\pi : H \to M,\ \pi(S_1) = (-1, -1, 1), \pi(S_2) = (1, 1, -1), \pi(S_3) = (1, -1, 1)$$

*is an isomorphism of $G_K$-modules where $S_j, j = 1, 2, 3$ are the matrices defined in Lemma 6.2.1. Hence $H^1(G_K, H_{8,4}) \cong L^*/(L^*)^2$ where $L = K[x]/(x^3 + ax + b)$.*

**Proof.** Recall in Lemma 6.0.2 that we have fixed a basis $\{P, Q\}$ for $E[8]$ such that $4P = T_1, 4Q = T_2$. $H$ is isomorphic as a Galois module to the group of automorphisms of $X_E(8)$ as a cover of $X_E(4)$. The explicit action of $H_{8,4}$ on $X_E(8)$ is given in Lemma 6.2.1. We show that $M$ is also isomorphic as a Galois module to the group of automorphisms of $X_E(8)$ as a cover of $X_E(4)$. For each $\chi = (e_1, e_2, e_3) \in M$, the action of $\chi$ on $X_E(8)$ is given by

$$\chi \circ (t, Y_1, Y_2, Y_3) = (t, e_1Y_1, e_2Y_2, e_3Y_3).$$

Therefore, the map $\pi$ gives a $G_K$-equivariant isomorphism by Lemma 6.2.1. In particular, $H^1(G_K, H_{8,4}) \cong H^1(G_K, M)$. Finally, by Shapiro's lemma and Hilbert's Theorem 90, $H^1(G_K, M) \cong L^*/(L^*)^2$. $\square$

Since we assume that $x^3 + ax + b$ is irreducible, $L \cong L_j$ for any $j = 1, 2, 3$ where $L_j = K(\theta_j)$, and we have an embedding $L \hookrightarrow \prod_{j=1}^3 L_j$.

**Lemma 6.4.5.** *The image of 7 under*

$$(\mathbb{Z}/8\mathbb{Z})^* \to H^1(G_K, H_{8,4}) \cong H^1(G_K, M) \cong L^*/(L^*)^2 \hookrightarrow \prod_{j=1}^{3} L_j^*/(L_j^*)^2 \qquad (\dagger\dagger)$$

*is $(\alpha_{7,1}, \alpha_{7,2}, \alpha_{7,3})$.*

**Proof.** By considering the function field of $X_E^7(8)$ and $X_E(8)$ over $K(E[2])$ (Section 6.1), the map $t \mapsto t, \sqrt{\alpha_{7,j}(t - t_{2j-1})(t - t_{2j})} \mapsto \sqrt{\alpha_{1,j}(t - t_{2j-1})(t - t_{2j})},\ j = 1, 2, 3$ gives an isomorphism between the function fields of $X_E^7(8)$ and $X_E(8)$. So it induces an isomorphism $\psi' : X_E^7(8) \to X_E(8)$ over $K(E[2])$. Moreover we have the following commutative diagram

$$\begin{array}{ccc} X_E^7(8) & \xrightarrow{\psi'} & X_E(8) \\ \downarrow & & \downarrow \\ X_E^3(4) & \xrightarrow{=} & X_E(4) \end{array}$$

For each $s \in G_K$, $s$ acts on $E[2]$ by permuting $\{T_1, T_2, T_3\}$. Let $\sigma_s$ be the element in the symmetric group of $\{1, 2, 3\}$ which corresponds to the action of $s$ on $\{T_1, T_2, T_3\}$. A direct computation shows that $({}^s\psi')\psi'^{-1}$ acts on $X_E(8)$ by

$$\sqrt{\alpha_{1,j}(t-t_{2j-1})(t-t_{2j})} \mapsto \frac{s\left(\sqrt{\frac{\alpha_{1,\sigma_s^{-1}(j)}}{\alpha_{7,\sigma_s^{-1}(j)}}}\right)}{\sqrt{\frac{\alpha_{1,j}}{\alpha_{7,j}}}}\sqrt{\alpha_{1,j}(t-t_{2j-1})(t-t_{2j})}, j = 1, 2, 3.$$

This induces a cocycle in $H^1(G_K, M)$,

$$s \mapsto \left( \frac{s\left(\sqrt{\frac{\alpha_{1,\sigma_s^{-1}(1)}}{\alpha_{7,\sigma_s^{-1}(1)}}}\right)}{\sqrt{\frac{\alpha_{1,1}}{\alpha_{7,1}}}}, \frac{s\left(\sqrt{\frac{\alpha_{1,\sigma_s^{-1}(2)}}{\alpha_{7,\sigma_s^{-1}(2)}}}\right)}{\sqrt{\frac{\alpha_{1,2}}{\alpha_{7,2}}}}, \frac{s\left(\sqrt{\frac{\alpha_{1,\sigma_s^{-1}(3)}}{\alpha_{7,\sigma_s^{-1}(3)}}}\right)}{\sqrt{\frac{\alpha_{1,3}}{\alpha_{7,3}}}} \right).$$

$\psi'$ is an isomorphism from $X_E^7(8)$ to $X_E(8)$ which fixes the level four structure. So by Lemma 3.3.3 and 6.4.2 this cocycle corresponds to the image of 7 under the connecting map $(\mathbb{Z}/7\mathbb{Z})^* \to H^1(G_K, H_{8,4})$. Then by Shapiro's lemma and Hilbert 90, we see that $\left(\frac{\alpha_{7,1}}{\alpha_{1,1}}, \frac{\alpha_{7,2}}{\alpha_{1,2}}, \frac{\alpha_{7,3}}{\alpha_{1,3}}\right)$ is the image of 7 under (††). Finally we have seen in Section 6.2 that we can set $\alpha_{1,j} = 1, j = 1, 2, 3$. $\square$

## 6.5 The Curve $X_E^7(8)$

Following the idea in previous section, we will prove Theorem 1.7.5 by the following procedure. We define

$$\delta_1 = (\theta_1 - \theta_2)(\theta_3 - \theta_1), \delta_2 = (\theta_1 - \theta_2)(\theta_2 - \theta_3), \delta_3 = (\theta_2 - \theta_3)(\theta_3 - \theta_1)$$

and we will show that $\alpha_{7,j}$ can be chosen to be $\delta_j$ for each $j$.

To check this, it suffices to compute the preimage of $(\delta_1, \delta_2, \delta_3)$ under

$$H^1(G_K, H_{8,4}) \cong H^1(G_K, M) \cong L^*/(L^*)^2 \hookrightarrow \prod_{j=1}^{3} L_j^*/(L_j^*)^2$$

and check it is the same as the image of 7 under $(\mathbb{Z}/8\mathbb{Z})^* \to H^1(G_K, H_{8,4})$ using Lemma 6.4.3 and 6.4.4. Then together we conclude that the image of 7 under (††) is $(\delta_1, \delta_2, \delta_3)$.

**Lemma 6.5.1.** *The $x$-coordinates of the primitive 4-torsion points of $E$ are given by*

$$\theta_1 \pm i\sqrt{\delta_1}, \theta_2 \pm i\sqrt{\delta_2}, \theta_3 \pm i\sqrt{\delta_3}.$$

**Proof.** This follows immediately from factorising the 4-division polynomial of $E$ over $K(E[2])$. □

Recall that we fix a basis $\{P, Q\}$ for $E[8]$ such that $4P = (\theta_1, 0)$ and $4Q = (\theta_2, 0)$. So we take $P$ and $Q$ such that $2P, 2Q$ and $2P + 2Q$ have $x$-coordinates $\theta_1 + i\sqrt{\delta_1}$, $\theta_2 + i\sqrt{\delta_2}$, and $\theta_3 + i\sqrt{\delta_3}$ respectively by Lemma 6.5.1. Let $T_1 = 4P, T_2 = 4Q$ and $T_3 = 4P + 4Q$ so $T_j = (\theta_j, 0)$ for each $j$.

**Lemma 6.5.2.** *For each $s \in G_K$, we identify $s$ with its image under $\rho_{E,8} : G_K \to$ Aut$(E[8]) \subset \mathrm{GL}_2(\mathbb{Z}/8\mathbb{Z})$. Fix generators $s_1, s_2, s_3, s_4$ for $\mathrm{GL}_2(\mathbb{Z}/8\mathbb{Z})$ as in Lemma 6.4.3. If $\rho_{E,8}$ is surjective, then*

$$\begin{array}{lll}
s_1(\sqrt{\delta_1}) = -\sqrt{\delta_1}, & s_1(\sqrt{\delta_2}) = -\sqrt{\delta_2}, & s_1(\sqrt{\delta_3}) = \sqrt{\delta_3}, \\
s_2(\sqrt{\delta_1}) = \sqrt{\delta_1}, & s_2(\sqrt{\delta_2}) = \sqrt{\delta_2}, & s_2(\sqrt{\delta_3}) = \sqrt{\delta_3}, \\
s_3(\sqrt{\delta_1}) = \sqrt{\delta_2}, & s_3(\sqrt{\delta_2}) = \sqrt{\delta_1}, & s_3(\sqrt{\delta_3}) = -\sqrt{\delta_3} \\
s_4(\sqrt{\delta_1}) = \sqrt{\delta_1}, & s_4(\sqrt{\delta_2}) = \sqrt{\delta_3}, & s_4(\sqrt{\delta_3}) = -\sqrt{\delta_2}.
\end{array}$$

*If $\theta$ is not surjective, then we can read off the action of $G_K$ on $\sqrt{\delta_j}, j = 1, 2, 3$ by the above results.*

**Proof.** Recall that

$$s_1 = \begin{pmatrix} 7 & 0 \\ 0 & 1 \end{pmatrix}, s_2 = \begin{pmatrix} 5 & 0 \\ 0 & 1 \end{pmatrix}, s_3 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, s_4 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Since $s_j(\zeta_8) = \zeta_8^{\det s_j}$ so $s_1(\zeta_8) = \zeta_8^7, s_2(\zeta_8) = \zeta_8^5, s_3(\zeta_8) = \zeta_8, s_4(\zeta_8) = \zeta_8$. Therefore $s_1(i) = -i, s_2(i) = i, s_3(i) = i, s_4(i) = i$. The actions of $s_j, j = 1, 2, 3, 4$ on $E[4]$ are given by

$$\begin{array}{lll}
s_1(2P) = -2P, & s_1(2Q) = 2Q, & s_1(2P + 2Q) = -2P + 2Q, \\
s_2(2P) = 2P, & s_2(2Q) = 2Q, & s_2(2P + 2Q) = 2P + 2Q, \\
s_3(2P) = -2Q, & s_3(2Q) = 2P, & s_3(2P + 2Q) = 2P - 2Q, \\
s_4(2P) = 2P, & s_4(2Q) = 2P + 2Q, & s_4(2P + 2Q) = 4P + 2Q.
\end{array}$$

By considering the $x$-coordinates of these points, we have

$$\begin{aligned}
&s_1(\theta_1+i\sqrt{\delta_1})=\theta_1+i\sqrt{\delta_1}, && s_1(\theta_2+i\sqrt{\delta_2})=\theta_2+i\sqrt{\delta_2}, && s_1(\theta_3+i\sqrt{\delta_3})=\theta_3-i\sqrt{\delta_3},\\
&s_2(\theta_1+i\sqrt{\delta_1})=\theta_1+i\sqrt{\delta_1}, && s_2(\theta_2+i\sqrt{\delta_2})=\theta_2+i\sqrt{\delta_2}, && s_2(\theta_3+i\sqrt{\delta_3})=\theta_3+i\sqrt{\delta_3},\\
&s_3(\theta_1+i\sqrt{\delta_1})=\theta_2+i\sqrt{\delta_2}, && s_3(\theta_2+i\sqrt{\delta_2})=\theta_1+i\sqrt{\delta_1}, && s_3(\theta_3+i\sqrt{\delta_3})=\theta_3-i\sqrt{\delta_3},\\
&s_4(\theta_1+i\sqrt{\delta_1})=\theta_1+i\sqrt{\delta_1}, && s_4(\theta_2+i\sqrt{\delta_2})=\theta_3+i\sqrt{\delta_3}, && s_4(\theta_3+i\sqrt{\delta_3})=\theta_2-i\sqrt{\delta_2}.
\end{aligned}$$

By considering the actions of $s_j, j=1,2,3,4$ on $E[2]$ we have

$$\begin{aligned}
&s_1(\theta_1)=\theta_1, && s_1(\theta_2)=\theta_2, && s_1(\theta_3)=\theta_3,\\
&s_2(\theta_1)=\theta_1, && s_2(\theta_2)=\theta_2, && s_2(\theta_3)=\theta_3,\\
&s_3(\theta_1)=\theta_2, && s_3(\theta_2)=\theta_1, && s_3(\theta_3)=\theta_3,\\
&s_4(\theta_1)=\theta_1, && s_4(\theta_2)=\theta_3, && s_4(\theta_3)=\theta_2.
\end{aligned}$$

Therefore the result follows. □

Each $s_j, j=1,2,3,4$ acts on $E[2]$ by permuting $\{T_1,T_2,T_3\}$. So for each $j$ we write $\sigma_{s_j}$ to be the element in the symmetric group of $\{1,2,3\}$ which corresponds to the action of $s_j$ on $\{T_1,T_2,T_3\}$.

**Lemma 6.5.3.** *We have*

$$\begin{aligned}
&\frac{s_1\left(\sqrt{\delta_{\sigma_{s_1}^{-1}(1)}}\right)}{\sqrt{\delta_1}}=-1, && \frac{s_1\left(\sqrt{\delta_{\sigma_{s_1}^{-1}(2)}}\right)}{\sqrt{\delta_2}}=-1, && \frac{s_1\left(\sqrt{\delta_{\sigma_{s_1}^{-1}(3)}}\right)}{\sqrt{\delta_3}}=1,\\
&\frac{s_2\left(\sqrt{\delta_{\sigma_{s_2}^{-1}(1)}}\right)}{\sqrt{\delta_1}}=1, && \frac{s_2\left(\sqrt{\delta_{\sigma_{s_2}^{-1}(2)}}\right)}{\sqrt{\delta_2}}=1, && \frac{s_2\left(\sqrt{\delta_{\sigma_{s_2}^{-1}(3)}}\right)}{\sqrt{\delta_3}}=1,\\
&\frac{s_3\left(\sqrt{\delta_{\sigma_{s_3}^{-1}(1)}}\right)}{\sqrt{\delta_1}}=1, && \frac{s_3\left(\sqrt{\delta_{\sigma_{s_3}^{-1}(2)}}\right)}{\sqrt{\delta_2}}=1, && \frac{s_3\left(\sqrt{\delta_{\sigma_{s_3}^{-1}(3)}}\right)}{\sqrt{\delta_3}}=-1,\\
&\frac{s_4\left(\sqrt{\delta_{\sigma_{s_4}^{-1}(1)}}\right)}{\sqrt{\delta_1}}=1, && \frac{s_4\left(\sqrt{\delta_{\sigma_{s_4}^{-1}(2)}}\right)}{\sqrt{\delta_2}}=-1, && \frac{s_4\left(\sqrt{\delta_{\sigma_{s_4}^{-1}(3)}}\right)}{\sqrt{\delta_3}}=1.
\end{aligned}$$

**Proof.** This follows from a direct computation by using Lemma 6.5.2. □

We now prove Theorem 1.7.5.

**Proof.** We identify each $s \in G_K$ with its image under $\rho_{E,8} : G_K \to \mathrm{Aut}(E[8]) \subset \mathrm{GL}_2(\mathbb{Z}/8\mathbb{Z})$ and pick generators $s_1, s_2, s_3, s_4$ for $\mathrm{GL}_2(\mathbb{Z}/8\mathbb{Z})$ as in Lemma 6.4.3. Then by Lemma 6.5.3 and Shapiro's Lemma, the preimage of $(\delta_1, \delta_2, \delta_3)$ under $H^1(G_K, M) \cong L^*/(L^*)^2 \hookrightarrow \prod_{j=1}^3 L_j^*/(L_j^*)^2$ is a cocycle $c_s$ which can be described as

$$c_{s_1} = (-1, -1, 1), c_{s_2} = (1, 1, 1), c_{s_3} = (1, 1, -1), c_{s_4} = (1, -1, 1).$$

By Lemma 6.4.4, the preimage of $c_{s_j}$ under $H^1(G_K, H_{8,4}) \cong H^1(G_K, M)$ is $C_{s_j}$ for each $j = 1, 2, 3, 4$, where $C_{s_j}, j = 1, 2, 3, 4$ are matrices given in Lemma 6.4.3. But by Lemma 6.4.3, $C_{s_j}, j = 1, 2, 3, 4$ are used to describe the image of 7 under $(\mathbb{Z}/8\mathbb{Z})^* \to H^1(G_K, H_{8,4})$. This shows that the image of 7 under

$$(\mathbb{Z}/8\mathbb{Z})^* \to H^1(G_K, H_{8,4}) \cong H^1(G_K, M) \cong L^*/(L^*)^2 \hookrightarrow \prod_{j=1}^{3} L_j^*/(L_j^*)^2$$

is $(\delta_1, \delta_2, \delta_3)$. Then by Lemma 6.4.5, $\alpha_{7,j}$ can be chosen to be $\delta_j$ for each $j$. Equations for $X_E^7(8)$ can be obtained by comparing the coefficients of $1, \theta_j, \theta_j^2$ in the equations

$$\alpha_{7,j}(t - t_{2j-1}s)(t - t_{2j}s) = (u_0 + u_1\theta_j + u_2\theta_j^2)^2, j = 1, 2, 3.$$

Finally, we make the substitution $(x_0 : x_1 : x_2 : x_3 : x_4) = (t : u_0 : u_1 : u_2 : \frac{s}{3})$ to get the equations stated in Theorem 1.7.5.

□

## 6.6 The Curve $X_E^3(8)$

We now prove Theorem 1.7.3 as a corollary of Theorem 1.7.5

**Proof.** The connecting map $(\mathbb{Z}/8\mathbb{Z})^* \to H^1(G_K, H_{8,4})$ is a group homomorphism. Therefore, the image of 3 under

$$(\mathbb{Z}/8\mathbb{Z})^* \to H^1(G_K, H_{8,4}) \cong H^1(G_K, M) \cong L^*/(L^*)^2 \hookrightarrow \prod_{j=1}^{3} L_j^*/(L_j^*)^2$$

is the product of the image of 5 and the image of 7. So $\alpha_{3,j} = \alpha_{5,j} \cdot \alpha_{7,j}$ in $L_j^*/(L_j^*)^2$. We have shown in Section 6.3 that $\alpha_{5,j} = D$ for each $j = 1, 2, 3$ where $D = -4a^3 - 27b^2$. Therefore,

$$\alpha_{3,1} = D \cdot \alpha_{7,1} = (\theta_2 - \theta_3)^2(\theta_1 - \theta_2)^3(\theta_3 - \theta_1)^3.$$

Since $((\theta_1-\theta_2)(\theta_3-\theta_1))^2$ is a square in $L_1$ so we can take $\alpha_{3,1}$ to be $(\theta_2-\theta_3)^2(\theta_1-\theta_2)(\theta_3-\theta_1)$. Similarly we can rescale $\alpha_{3,2}$ and $\alpha_{3,3}$ so that

$$\alpha_{3,2} = (\theta_3-\theta_1)^2(\theta_1-\theta_2)(\theta_2-\theta_3), \alpha_{3,3} = (\theta_1-\theta_2)^2(\theta_3-\theta_1)(\theta_2-\theta_3).$$

Comparing the coefficients of $1, \theta_j, \theta_j^2$ in the equation

$$\alpha_{3,j}(t-t_{2j-1}s)(t-t_{2j}s) = (u_0+u_1\theta_j+u_2\theta_j^2)^2, j = 1,2,3,$$

we obtain a model of $X_E^3(8) \subset \mathbb{P}^4_{(t,u_0,u_1,u_2,s)}$ given by $F_3 = G_3 = H_3 = 0$ where

$$\begin{aligned}
F_3 &= -\frac{2}{9}a^2s^2 + 6at^2 + 6bts - (-au_2^2 + 2u_0u_2 + u_1^2),\\
G_3 &= \frac{4}{3}a^2ts + \frac{1}{3}abs^2 - 9bt^2 - (-2au_1u_2 - bu_2^2 + 2u_0u_1),\\
H_3 &= -\frac{4}{9}a^3s^2 + 4a^2t^2 + 4abts - 2b^2s^2 - (-2bu_1u_2 + u_0^2),
\end{aligned}$$

with forgetful map $X_E^3(8) \to X_E^3(4) : (t : u_0 : u_1 : u_2 : s) \mapsto (t : s)$.

We make the following substitution to obtain the simplified equations for $X_E^3(8)$ as stated in Theorem 1.7.3

$$\begin{pmatrix} t \\ u_0 \\ u_1 \\ u_2 \\ s \end{pmatrix} = \begin{pmatrix} 0 & 0 & -3b & 0 & -2a^2 \\ 4a^2 & -6ab & 0 & -9b^2 & 0 \\ -9b & -2a^2 & 0 & -3ab & 0 \\ 6a & -9b & 0 & 2a^2 & 0 \\ 0 & 0 & 6a & 0 & -27b \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix}$$

Then $f_3, g_3, h_3$ are given by

$$\begin{pmatrix} f_3 \\ g_3 \\ h_3 \end{pmatrix} = \frac{1}{D^2} \begin{pmatrix} -9b^2 & -3ab & -a^2 \\ -12ab & -4a^2 & 9b \\ 4a^2 & -9b & -3a \end{pmatrix} \begin{pmatrix} F_3 \\ G_3 \\ H_3 \end{pmatrix}$$

where $D = -4a^3 - 27b^2$. So the forgetful map is

$$(t : u_0 : u_1 : u_2 : s) \mapsto \frac{t}{s} = \frac{-3bx_2 - 2a^2x_4}{6ax_2 - 27bx_4}.$$

The $5 \times 5$ matrix and $3 \times 3$ matrices have determinants $3D^3$ and $-D^2$ respectively. So the substitution is invertible.

□

**Remark** The above substitution minimises the equations for $X_E^3(8)$ at the place $-4a^3 - 27b^2$. We will need this simpler equation in Chapter 8 to find the elliptic fibration of the modular diagonal quotient surface $Z_{8,3}$.

## 6.7 Examples

For simplicity, we now assume $K = \mathbb{Q}$. In [KS], Theorem 4 shows that $Z_{8,1}$ is a rational surface and so $Z_{8,1}$ is birational to $\mathbb{P}^2$ over $\mathbb{Q}$ because $(E, E, [1])$ is always a $\mathbb{Q}$-rational point on $Z_{8,1}$. Since there are only finitely many $l$ such that cyclic $l$-isogeny exist over $K$, they only correspond to finitely many curves on $Z_{8,1}$. Therefore,

**Corollary 6.7.1.** *There are infinitely many pairs of non-isogenous directly 8-congruent elliptic curves.*

In fact, we will give later an explicit parametrisation of the rational surface $Z_{8,1}$.

We now prove similar statements for $r = 3, 5, 7$.

**Proposition 6.7.2.** *There are infinitely many pairs of non-isogenous elliptic curves which are 8-congruent with power 3.*

**Proof.** For each $p \in \mathbb{Q}$, define

$$a = -\frac{27}{4}\frac{(2p^2 - 8p + 21)(2p^2 + 1)^2(10p^2 + 24p + 17)}{(2p^2 - 4p + 11)(2p^2 + 4p + 3)(2p^2 + 8p - 1)^2},$$

and $E : y^2 = x^3 + ax + a$. Then the followings define a point on $X_E^3(8)$

$$\begin{aligned}
x_0 &= (8p^4 + 40p^3 + 48p^2 + 76p - 10)a, \\
x_1 &= -36p^4 - 144p^3 - 72p + 9, \\
x_2 &= -54p^4 - 72p^3 - 198p^2 - 36p - \frac{171}{2}, \\
x_3 &= -24p^3 - 144p^2 - 180p + 24, \\
x_4 &= -4p^4 - 32p^3 - 60p^2 + 16p - 1.
\end{aligned}$$

where the equations for $X_E^3(8)$ were given in Theorem 1.7.3. When $p = 1$ we obtain a pair of non-isogenous curves. $\square$

**Proposition 6.7.3.** *There exists infinitely many pairs of non-isogenous elliptic curves which are 8-congruent with power* 5.

**Proof.** For each $p \in \mathbb{Q}$, define

$$a = \frac{9(p^2 - 18p + 75)(p^2 - 2p - 53)^3}{4(p-13)^2(p-7)^2(p^2 - 8p + 25)(5p^2 - 88p + 389)},$$

and $E : y^2 = x^3 + ax + a$. Then the followings define a point on $X_E^5(8)$

$$\begin{aligned}
x_0 &= 0, \\
x_1 &= \frac{-9(p^2 - 18p + 75)(p^2 - 2p - 53)^2(p^4 - 28p^3 + 354p^2 - 2356p + 6457)}{2(x-13)^2(x-7)^2(p^2 - 16p + 69)(p^2 - 8p + 25)(5p^2 - 88p + 389)}, \\
x_2 &= \frac{3(p^2 - 18p + 75)(p^2 - 2p - 53)}{2(p-13)(p-7)(p^2 - 16p + 69)}, \\
x_3 &= -12\frac{p-8}{p^2 - 16p + 69}, \\
x_4 &= 1
\end{aligned}$$

where the equations for $X_E^5(8)$ were given in Theorem 1.7.4. When $p = 8$, we obtain a pair of elliptic curves (up to isomorphism) $129600je1$ and

$$y^2 = x^3 + 5764500x - 119346750000$$

which are non-isogenous and 8-congruent with power 5. □

**Proposition 6.7.4.** *There are infinitely many pairs of non-isogenous elliptic curves which are 8-congruent with power 7.*

**Proof.** Set $a = b$ in the equations of $X_E^7(8)$ in Theorem 1.7.5 and consider the affine piece with $s = \frac{1}{3}$. The section $x_0 = 0$ defines a curve $C$ which has 2 irreducible components. One of the components is contained in the component $a = 0$. We take the one with $a \neq 0$, say $C_1$, which is a genus 1 curve and it has a rational point

$$p : a = -9, x_0 = 0, x_1 = 3, x_2 = 1, x_3 = 0, x_4 = \frac{1}{3}$$

Putting $C_1$ into Weierstrass form we conclude that $C_1$ is isomorphic to

$$C' : y^2 = x^3 + x^2 - 538x + 4628$$

which has rank 1. Finally, we find a point on $C_1$ given by

$$a = -\frac{135}{32}, x_0 = 0, x_1 = \frac{75}{32}, x_2 = \frac{5}{4}, x_3 = \frac{-1}{3}, x_4 = \frac{1}{3}$$

and this point gives a pair of non-isogenous curves

$$E_1 : y^2 = x^3 - 1080x - 17280, \quad E_2 : y^2 = x^3 + 7931250x - 8519850000.$$

$\square$

**Remark** The surface $Z_{8,7}$ has geometric genus 2 ([KS] Theorem 4(c)), and one might expect to take more effort to find rational points on $Z_{8,7}$. In fact we will see later that it is still possible to find rational curves isomorphic to $\mathbb{P}^1$ on the surface $Z_{8,7}$ which give pairs of non-isogenous elliptic curves.

# 7 Twists of Elliptic Curves: Level Twelve Structure

In this chapter we prove Theorem 1.7.10 and 1.7(ii). Let $K$ be a field of characteristic not equal to 2 or 3 and $E : y^2 = x^3 + ax + b$ be an elliptic curve over $K$.

## 7.1 Extension of Function Fields

Our strategy is very similar to what we did in the previous section (i.e. for $n = 8$) and is based on the fact that the group

$$H_{12,6} = \ker(\mathrm{PSL}_2(\mathbb{Z}/12\mathbb{Z}) \to \mathrm{PSL}_2(\mathbb{Z}/6\mathbb{Z})) \cong (\mathbb{Z}/2\mathbb{Z})^3$$

is a subgroup inside $\mathrm{PSL}_2(\mathbb{Z}/12\mathbb{Z})$ whose action on $X(12)$ fixes the level six structure. We have seen in Section 2.5 that the function field of $X(12)$ over $K(\zeta_{12})$ can be described as

$$K(\zeta_{12})(X, Y, \sqrt{Y}, \sqrt{(Y-3)(Y+1)}, \sqrt{(Y+3)(Y-1)})$$

where $X, Y$ satisfy $Y^2 = X^3 + 1$. Equivalently, we have

$$K(\zeta_{12})(X, Y, \sqrt{Y}, \sqrt{(Y-3)/(Y+1)}, \sqrt{(Y+3)/(Y-1)}).$$

We have seen in Corollary 2.2.3 that the cusps of $X(6)$ are

$$(0, \pm 1), (-\zeta_3, 0), (-\zeta_3^2, 0), (-1, 0), (2\zeta_3, \pm 3), (2\zeta_3^2, \pm 3), (2, \pm 3), O.$$

On the curve $X(6) : Y^2 = X^3 + 1$, we have

$$\begin{aligned}
\mathrm{div}(Y) &= -3O + (-1, 0) + (-\zeta_3, 0) + (-\zeta_3^2, 0), \\
\mathrm{div}((Y-3)/(Y+1)) &= -3(0, -1) + (2, 3) + (2\zeta_3, 3) + (2\zeta_3^2, 3), \\
\mathrm{div}((Y+3)/(Y-1)) &= -3(0, 1) + (2, -3) + (2\zeta_3, -3) + (2\zeta_3^2, -3).
\end{aligned}$$

Therefore, over $\bar{K}$, we can write the function field of $X(12)$ as

$$\bar{K}(X, Y, \sqrt{f_1}, \sqrt{f_2}, \sqrt{f_3})$$

where $Y^2 = X^3 + 1$ and $f_1, f_2, f_3$ are rational functions on the curve $Y^2 = X^3 + 1$ such that

$$\begin{aligned}
\mathrm{div}(f_1) &= -3O + (-1, 0) + (-\zeta_3, 0) + (-\zeta_3^2, 0) + 2D_1, \\
\mathrm{div}(f_2) &= -3(0, -1) + (2, 3) + (2\zeta_3, 3) + (2\zeta_3^2, 3) + 2D_2, \\
\mathrm{div}(f_3) &= -3(0, 1) + (2, -3) + (2\zeta_3, -3) + (2\zeta_3^2, -3) + 2D_3,
\end{aligned}$$

where $D_1, D_2, D_3$ are divisors of some rational functions on the curve $Y^2 = X^3 + 1$.

Since $X_E(12)$ is a twist of $X(12)$, so they are isomorphic over $\bar{K}$ and they have the same ramification behavior under the forgetful map to the level six structure. Let $t_1, \ldots, t_{12}$ be the images of

$$O, (-1, 0), (-\zeta_3, 0), (-\zeta_3^2, 0), (0, -1), (2, 3), (2\zeta_3, 3), (2\zeta_3^2, 3), (0, 1), (2, -3), (2\zeta_3, -3), (2\zeta_3^2, -3)$$

respectively, under the isomorphism $\psi_6 : X(6) \to X_E(6)$ in Theorem 4.2.2, which is defined as

$$\psi_6(x, y) = (\sqrt[3]{\Delta_E} x, \sqrt{\Delta_E} y) \ominus (\sqrt[3]{\Delta_E} x_0, \sqrt{\Delta_E} y_0)$$

where $(x_0, y_0)$ is a point on $X(6)$ corresponding to $E$.

The curve $X_E(6)$ has equation $y^2 = x^3 + \Delta_E$ by Corollary 4.2.1. This implies that the function field of $X_E(12)$ over $\bar{K}$ has the form

$$\bar{K}(x, y, \sqrt{g_1}, \sqrt{g_2}, \sqrt{g_3})$$

where $y^2 = x^3 + \Delta_E$ and $g_1, g_2, g_3$ are rational functions on $X_E(6) : y^2 = x^3 + \Delta_E$ such that

$$\begin{aligned}
\operatorname{div}(g_1) &= -3(t_1) + (t_2) + (t_3) + (t_4) + 2D_1, \\
\operatorname{div}(g_2) &= -3(t_5) + (t_6) + (t_7) + (t_8) + 2D_2, \\
\operatorname{div}(g_3) &= -3(t_9) + (t_{10}) + (t_{11}) + (t_{12}) + 2D_3,
\end{aligned}$$

where $D_1, D_2, D_3$ are divisors of some rational functions on $X_E(6)$. We briefly describe how to find the cusps $t_1, \ldots, t_{12}$ explicitly. Take a point $(x_0, y_0)$ on $X(6)$ which corresponds to $E$. We can consider the $j$-map $X(6) \to X(1)$ and take a point such that $j(x_0, y_0) = j(E)$. Such point $(x_0, y_0)$ is defined over $K(E[6])$. Then the cusps of $X_E(6)$ are the images of the cusp of $X(6)$ under $\psi_6$.

The absolute Galois group $G_{K(E[2])}$ acts on the the cusps $t_1, \ldots, t_{12}$ by permutation. A direct computation shows that

**Lemma 7.1.1.** *$G_{K(E[2])}$ fixes $\{t_1, t_2, t_3, t_4\}, \{t_5, t_6, t_7, t_8\}, \{t_9, t_{10}, t_{11}, t_{12}\}$.*

**Proof.** We can find the coordinates of $t_i, i = 1, \ldots, 12$ explicitly. They are defined over $K(E[6])$. Let $t_i^x$ and $t_i^y$ be the $x$-coordinate and $y$-coordinate of $t_i$ for each $i$. To prove the statement, it suffices to show that $G_{K(E[2])}$ permutes $t^x_{3j}, t^x_{3j+1}, t^x_{3j+2}, t^x_{3j+3}$ for each $j = 1, 2, 3$ and $t^y_{3j}, t^y_{3j+1}, t^y_{3j+2}, t^y_{3j+3}$ for each $j = 1, 2, 3$. This can be done by checking the elementary symmetric polynomials in $t^x_{3j}, t^x_{3j+1}, t^x_{3j+2}, t^x_{3j+3}$ and the elementary symmetric polynomials in $t^y_{3j}, t^y_{3j+1}, t^y_{3j+2}, t^y_{3j+3}$ are defined over $K(E[2])$. $\square$

These observations help us to find a model of $X_E(12)$ over $K(E[2])$. Since $X_E(12)$ has a model over $K$, we then deduce a model of $X_E(12)$ over $K$ from that over $K(E[2])$.

## 7.2 The Curve $X_E(12)$

We outline the strategy to compute a model for $X_E(12)$ over $K$ explicitly. By Lemma 7.1.1, we know that the cusps of $X_E(6)$ can be partitioned into three $G_K$-invariant subsets, each having four elements. So we search for principal divisor $D_1, D_2, D_3$ supported on $\{t_1, t_2, t_3, t_4\}, \{t_5, t_6, t_7, t_8\}, \{t_9, t_{10}, t_{11}, t_{12}\}$ respectively, such that $g_1, g_2, g_3$ are rational functions on $X_E(6)$ over $K(E[2])$, where

$$\begin{aligned}
\mathrm{div}(g_1) &= -3(t_1) + (t_2) + (t_3) + (t_4) + 2D_1,\\
\mathrm{div}(g_2) &= -3(t_5) + (t_6) + (t_7) + (t_8) + 2D_2,\\
\mathrm{div}(g_3) &= -3(t_9) + (t_{10}) + (t_{11}) + (t_{12}) + 2D_3.
\end{aligned}$$

Then we are in a similar situation as in the case $n = 8$, which allows us to find a model for $X_E(12)$ over $K$. For the moment assume $a \neq 0$. We will see the reason for doing this in the next lemma.

**Lemma 7.2.1.** *Let $P = \left(\frac{4a^3+36b^2}{a^2}, \frac{-36a^3b-216b^3}{a^3}\right)$ be a point on $X_E(6)$. Then the divisors*

$$(t_{4i-3}) + (t_{4i-2}) + (t_{4i-1}) + (t_{4i}) + 2(T_i) - 2(P) - 4(O), \quad i = 1, 2, 3$$

*are principal where $T_i = t_{4i-3} \oplus t_{4i-2} \oplus t_{4i-1} \oplus t_{4i}$ is a $K(E[2])$-rational point on $X_E(6)$ for each $i$ and $\oplus$ is the usual addition law on $X_E(6) : y^2 = x^3 + \Delta_E$ which is viewed as an elliptic curve.*

**Proof.** This follows from a direct computation that

$$3T_i \ominus 2P = O$$

and the fact that each of the divisors in the statement has degree 0. Since $X_E(6)$ is an elliptic curve, a divisor $D$ is principal if and only if $\deg D = 0$ and $\sum D = O$. $\square$

We see that $P$ is not defined when $a = 0$, though one can argue $P = O$ when $a = 0$. We will firstly consider the case $a \neq 0$, and then we will show how to recover the case $a = 0$ later.

**Lemma 7.2.2.** *Let $T_i, P$ be the points defined in the previous lemma. Then the divisors*

$$D_i = 2(t_{4i-3}) + (T_i) - (P) - 2(O), \quad i = 1, 2, 3$$

*are principal.*

**Proof.** For each $i$, a direct computation shows that

$$\sum D_i = 3t_{4i-3} \oplus t_{4i-2} \oplus t_{4i-1} \oplus t_{4i} \ominus P = O$$

and so $D_i$ is principal because $\deg D_i = 0$. $\square$

Lemma 7.2.1 and 7.2.2 show that we can pick $D_i = 2t_{4i-3} + T_i - P - 2O$ such that there exist rational functions $g_1, g_2, g_3$ with

$$\operatorname{div}(g_i) = (t_{4i-3}) + (t_{4i-2}) + (t_{4i-1}) + (t_{4i}) + 2(T_i) - 2(P) - 4(O), \quad i = 1, 2, 3.$$

Moreover, since $G_{K(E[2])}$ acts trivially on $\{t_{4i-3}, t_{4i-2}, t_{4i-1}, t_{4i}\}, T_i$ and $P$, so $g_i$ is defined over $K(E[2])$ for each $i$.

Let $\theta_i, i = 1, 2, 3$ be the roots of $x^3 + ax + b = 0$. Then we compute the rational functions $g_i$ (see Appendix) up to scaling factors, defined over $K(\theta_i)$. We will briefly illustrate how to compute this efficiently.

In general, the MAGMA function **IsPrincipal**(D) will return the rational function $g$ with $\operatorname{div}(g) = D$. However, in this case, the cusps $t_1, \ldots, t_{12}$ are defined over $K(E[6])$ and it is not efficient to work out the rational functions $g_i$ by using this MAGMA function. But we can write the divisor $(t_{4i-3}) + (t_{4i-2}) + (t_{4i-1}) + (t_{4i}) + 2(T_i) - 2(P) - 4(O)$ as

$$((t_{4i-3}) + (t_{4i-2}) + (t_{4i-1}) + (t_{4i}) - (T_i) - 3(O)) + (3(T_i) - 2(P) - (O))$$

where both $(t_{4i-3}) + (t_{4i-2}) + (t_{4i-1}) + (t_{4i}) - (T_i) - 3(O)$ and $3(T_i) - 2(P) - (O)$ are principal. The MAGMA function **IsPrincipal** computes the rational function with divisor

$3(T_i) - 2(P) - (O)$ efficiently. For the first one, there is a standard way to work out the rational function (up to scaling factor) which has divisor $(P) + (Q) - (P \oplus Q) - (O)$. This gives us a way to compute the rational function (up to scaling factor) which has divisor $(t_{4i-3}) + (t_{4i-2}) + (t_{4i-1}) + (t_{4i}) - (T_i) - 3(O)$.

**Remark** If we look at the expressions of $g_i$ in the Appendix, we see that it works for all values of $a, b$ with $4a^3 + 27b^2 \neq 0$ except $a = 0$.

The following lemma tells us the rational function we should search for when $a = 0$.

**Lemma 7.2.3.** *When $a = 0$, the divisors*

$$(t_{4i-3}) + (t_{4i-2}) + (t_{4i-1}) + (t_{4i}) - 4(O), \quad i = 1, 2, 3$$

*are principal. Further, $T_i = O$ when $a = 0$ and so the above divisors agree with*

$$(t_{4i-3}) + (t_{4i-2}) + (t_{4i-1}) + (t_{4i}) + 2(T_i) - 2(P) - 4(O)$$

*when $T_i = O$ and $P = O$.*

**Proof.** This follows from a direct computation. □

To recover the case $a = 0$, we use the following isomorphism to map $X_E(6)$ into a cubic plane curve. We will explain the reason for doing this later.

**Lemma 7.2.4.** *Let $C_E \subset \mathbb{A}^2_{X,Y}$ be the curve which has equation $F = 0$ where*

$$F = -X^2 + aXY^2 + 6bY^3 - 6aY^2 - 12.$$

*Then the map*

$$\psi : C_E \to X_E(6),\ (X, Y) \mapsto (aX + 6bY - 2a, a^2XY + 6bX + 6abY^2 - 6a^2Y)$$

*is an isomorphism of curves.*

**Proof.** This again follows from a direct computation. Note that the isomorphism works for all $a, b$ with $4a^3 + 27b^2 \neq 0$. □

**Lemma 7.2.5.** *The isomorphism $\psi : C_E \to X_E(6)$ induced an isomorphism between the function fields $\psi^* : K(X_E(6)) \to K(C_E)$. Let $G_i = \psi^*(g_i)$, then*

$$\begin{aligned} G_i &= (a\theta_i^2Y^2 + 4a\theta_iY + (12\theta_i^2 + 8a))X + 6b\theta_i^2Y^3 + (-6a\theta_i^2 + 36b\theta_i - 4a^2)Y^2 - 24a\theta_iY + 24\theta_i^2 \\ &= (X^2 + 12X + 36)\theta_i^2 + (4aXY + 36bY^2 - 24aY)\theta_i + 8aX - 4a^2Y^2. \end{aligned}$$

*In particular, $G_i$ works for all values of $a, b$ with $4a^3 + 27b^2 \neq 0$.*

**Proof.** The functions $G_i$ can be found by setting

$$x = aX + 6bY - 2a, \quad y = a^2XY + 6bX + 6abY^2 - 6a^2Y$$

in $g_i$. The second equality above follows by using the equation of $C_E$. □

**Remark** The above lemma shows that through the isomorphism $\psi^{-1} : X_E(6) \to C_E(6)$, we take the rational functions $g_i$ to $G_i$ for each $i$ such that $G_i$ also works for the case $a = 0$. This recovers the case $a = 0$ and so we can use $G_i$ to work out a model for $X_E(12)$ for all values of $a, b$ with $4a^3 + 27b^2 \neq 0$.

The isomorphism $\psi : C_E \to X_E(6)$ induces an automorphism (over $\bar{K}$) of the function fields of $X_E(12)$. Therefore, over $\mathbb{C}$ we can now interpret the function field of $X_E(12)$ as

$$\bar{K}(X, Y, \sqrt{G_1}, \sqrt{G_2}, \sqrt{G_3}).$$

where $-X^2 + aXY^2 + 6bY^3 - 6aY^2 - 12 = 0$. Since $G_1, G_2, G_3$ are defined over $K(E[2])$, and are conjugates to each other. The function field of $X_E(12)$ over $K(E[2])$ is

$$K(E[2])(x, y, \sqrt{\alpha_1 G_1}, \sqrt{\alpha_2 G_2}, \sqrt{\alpha_3 G_3})$$

for some scaling factors $\alpha_1, \alpha_2, \alpha_3 \in K(E[2])$. This allows us to compute the equations for $X_E(12)$ over $K(E[2])$. Indeed,

**Lemma 7.2.6.** *The (affine) equations for $X_E(12) \subset \mathbb{A}^5_{X,Y,x_0,x_1,x_2}$ over $K(E[2])$ are given by $F = f_1 = f_2 = f_3 = 0$ where*

$$F = -X^2 + aXY^2 + 6bY^3 - 6aY^2 - 12,$$

*and*

$$f_i = (X^2 + 12X + 36)\theta_i^2 + (4aXY + 36bY^2 - 24aY)\theta_i + 8aX - 4a^2Y^2 - x_i^2$$

*for each $i = 1, 2, 3$.*

**Proof.** Following the above discussion we have

$$\alpha_i G_i = x_i^2.$$

Use the expressions of $G_i$ computed in Lemma 7.2.5 and so the equations for $X_E(12)$ over $K(E[2])$ are $F = 0$ and

$$\frac{x_i^2}{\alpha_i} = (X^2 + 12X + 36)\theta_i^2 + (4aXY + 36bY^2 - 24aY)\theta_i + 8aX - 4a^2Y^2 \qquad (\dagger)$$

There is a $K$-rational point $(E, [1])$ on $X_E(12)$, which descends to the $K$-rational point on $X_E(6)$ corresponding to $(E, [1])$. By our convention and Theorem 4.2.2, the point $O$ on $X_E(6)$ corresponds to $(E, [1])$. Taking homogenous coordinates of the equations of $C_E$ we have

$$-X^2Z + aXY^2 + 6bY^3 - 6aY^2Z - 12Z^3 = 0.$$

A direct computation using Lemma 7.2.4 shows that the point $(1 : 0 : 0)$ on $C_E$ corresponds to $O$ on $X_E(6)$. Therefore, $(1 : 0 : 0)$ is the point on $C_E$ corresponding to $(E, [1])$. Taking homogenous coordinate for $(\dagger)$ we have

$$\frac{x_i^2}{\alpha_i} = (X^2 + 12XZ + 36Z^2)\theta_i^2 + (4aXY + 36bY^2 - 24aYZ)\theta_i + 8aXZ - 4a^2Y^2.$$

The point on $X_E(12)$ corresponding to $(E, [1])$ is the point above $(1 : 0 : 0)$, say

$$(X : Y : Z : x_1 : x_2 : x_3) = (1 : 0 : 0 : x_1' : x_2' : x_3')$$

for some $x_1', x_2', x_3' \in K$. Substituting these into the equations above we have

$$x_i'^2 = \alpha_i \theta_i^2$$

and so $\alpha_i = (x_i'/\theta_i)^2$ for each $i$. We are free to replace $\alpha_i$ by $\alpha_i u_i^2$ for any non-zero $u_i \in K(\theta_i)$ because

$$K(E[2])(X, Y, \sqrt{\alpha_1 G_1}, \sqrt{\alpha_2 G_2}, \sqrt{\alpha_3 G_3}) = K(E[2])\left(X, Y, \sqrt{\alpha_1 u_1^2 G_1}, \sqrt{\alpha_2 u_2^2 G_2}, \sqrt{\alpha_3 u_3^2 G_3}\right).$$

Therefore we can take $\alpha_i$ to be 1 for each $i$, which gives the required equations for $X_E(12)$ over $K(E[2])$. $\square$

Since $X_E(12)$ has naturally a model over $K$, we can now compute a model for $X_E(12)$ over $K$ by comparing the coefficients of $1, \theta_i, \theta_i^2$ above for each $i$. Note that we only need to do this for one of $f_i$ because $f_1, f_2, f_3$ are conjugates to each other. In particular, we write $x_i = u_0 + u_1\theta_i + u_2\theta_i^2$ for each $i$. Then we can understand $f_1, f_2, f_3$ in terms of one equation

$$f = (X^2 + 12X + 36)\theta^2 + (4aXY + 36bY^2 - 24aY)\theta + 8aX - 4a^2Y^2 - (u_0 + u_1\theta + u_2\theta^2)^2$$

together with the $K$-algebra homomorphisms $K[x]/\langle x^3 + ax + b\rangle \to \bar{K}$, where $\theta_1, \theta_2, \theta_3$ are the images of $\theta$. We can now prove Theorem 1.7.10.

**Proof.** This follows from the above discussion and comparing the coefficients of $1, \theta, \theta^2$ in $f$. $\square$

**Corollary 7.2.7.** *Fix a model for $X_E(6) : y^2 = x^3 + \Delta_E$ over $K$ and the forgetful map $\chi^+_{12,6} : X_E(12) \to X_E(6)$ is*

$$(X, Y, u_0, u_1, u_2) \mapsto (aX + 6bY - 2a, a^2XY + 6bX + 6abY^2 - 6a^2Y).$$

*Moreover, fix an isomorphism $X_E(3) \cong \mathbb{P}^1_\lambda$ as in Theorem 3.2.1, then the forgetful map $\chi^+_{12,3} : X_E(12) \to X_E(3)$ is*

$$(X, Y, u_0, u_1, u_2) \mapsto \frac{x^3y - 108bx^3 - 8\Delta_E y}{18(x^4 + 12ax^3 + 4\Delta_E x)}$$

*where*

$$x = aX + 6bY - 2a, \quad y = a^2XY + 6bX + 6abY^2 - 6a^2Y.$$

*In particular, this allows us to read off the families of elliptic curves parametrised by $X_E(12)$ by the families of elliptic curves parametrised by $X_E(3)$ in Theorem 3.2.1 together with the above forgetful map.*

**Proof.** The forgetful map $\chi^+_{12,6} : X_E(12) \to X_E(6)$ can be computed through the composition

$$X_E(12) \to C_E \to X_E(6)$$

where $C_E$ is the curve defined in 7.2.4. It is clear that the forgetful map $X_E(12) \to C_E$ is

$$(X, Y, u_0, u_1, u_2) \mapsto (X, Y)$$

and the isomorphism between $C_E$ and $X_E(6)$ was computed in 7.2.4.

Recall that our computation of $X_E(12)$ starts with the isomorphism $\psi_6 : X(6) \to X_E(6)$ as in Theorem 4.2.2. Therefore, the forgetful map $\chi^+_{12,3} : X_E(12) \to X_E(3)$ can be computed through the composition

$$X_E(12) \xrightarrow{\chi^+_{12,6}} X_E(6) \xrightarrow{\chi^+_{6,3}} X_E(3)$$

and $\chi^+_{6,3} : X_E(6) \to X_E(3)$ is the map

$$(x,y) \mapsto \frac{x^3y - 108bx^3 - 8\Delta_E y}{18(x^4 + 12ax^3 + 4\Delta_E x)}$$

in Theorem 4.2.2. $\square$

**Remark** We have seen that one of the reasons we identify $X_E(6)$ with $C_E$ is to recover the case $a = 0$. The other reason is that, by using the rational functions $G_i$ instead of $g_i$, we obtain simpler equations for $X_E(12)$ in the sense that the equations for $X_E(12)$ now is a cubic form together with three quadratic forms in $\mathbb{P}^5$.

Finally, we explain briefly how we come up with the idea to find the isomorphism $C_E \to X_E(6)$ in order to recover the case $a = 0$. We firstly consider the divisor map $\phi$ determined by the complete linear system of the divisor $2O + P$. Then $\phi$ is an isomorphism. Then $\phi$ is given by

$$\phi : (x,y) \mapsto \left( x + \frac{4a^3 + 36b^2}{a^2}, \frac{y + \frac{-36a^3b - 216b^3}{a^3}}{x + \frac{-4a^3 - 36b^2}{a^2}} \right)$$

and the image of $\phi$, say $B_E$, is defined by the equation $F' = 0$, where

$$\begin{aligned} F' &= -a^4X^2 + a^4XY^2 + (4a^3 + 36b^2)a^2XZ^2 + (-8a^3 - 72b^2)a^2Y^2 + (72a^3b + 432b^3)aY \\ &+ (-16a^6 - 288a^3b^2 - 1296b^4). \end{aligned}$$

Homogenize $F'$ and so $F'$ is a ternary cubic form. The curve $B_E$ defined by $F' = 0$ is singular at the point of infinity when $a = 0$. Using standard minimisation algorithm we find an isomorphism $C_E \to B_E$ given by

$$(X,Y) \mapsto \left( aX + 6bY + \frac{2a^3 + 36b^2}{a^2}, aY + 6\frac{b}{a} \right).$$

Composing this map with $\phi^{-1}$ we obtain the isomorphism $\psi : C_E \to X_E(6)$ as in Lemma 7.2.5.

## 7.3 Examples of 12-Congruent Elliptic Curves

We now prove Proposition 1.7.11 (ii) by using the model for $X_E(12)$ we got. We will use the idea in Section 1.6. We set $b = a$ in the equations of $X_E(12)$ and view $a$ as a variable. Then we obtain a birational model of the modular diagonal surface $Z_{12,1}$. By our discussion in Section 1.6 and Theorem 1.6.1, it suffices to find a curve $C$ of genus zero on $Z_{12,1}$ and a point on $C$ which corresponds to a pair of non-isogenous elliptic curves. We now prove the Theorem.

**Proof.** If we set $b = a$ then we have

$$\begin{aligned} F &= -X^2 + aXY^2 + 6aY^3 - 6aY^2 - 12, \\ F_1 &= (X^2 + 12X + 36) - (-aa_2^2 + 2u_0u_2 + u_1^2), \\ F_2 &= (4aXY + 36aY^2 - 24aY) - (-2au_1u_2 - au_2^2 + 2u_0u_1), \\ F_3 &= (8aX - 4a^2Y^2) - (-2au_1u_2 + u_0^2). \end{aligned}$$

Then we obtain the following genus zero curve $C$ with parameter $p$ on the above surface

$$\begin{aligned} X &= \frac{25p^2 - 1110p + 12546}{25p - 555}, \\ Y &= \frac{-250p^3 + 20400p^2 - 533880p + 4553712}{3375p^2 - 149850p + 1673460}, \\ a &= \frac{3^8(25p^2 - 1110p + 12396)^4}{2^2(25p - 555)(5p^2 - 216p + 2340)(125p^3 - 10200p^2 + 266940p - 2276856)^2}, \\ u_0 &= -\frac{81(25p^2 - 1110p + 12396)^2(5p - 96)^2}{5(25p - 555)(5p^2 - 216p + 2340)(125p^3 - 10200p^2 + 266940p - 2276856)}, \\ u_1 &= \frac{25p^2 - 960p + 9216}{25p - 555}, \\ u_2 &= 0. \end{aligned}$$

Finally, we check that the pair of curves corresponding to $p = -1$ are not isogenous. □

## 7.4 The Curve $X_E^7(12)$

We briefly explain how we can compute the equations for $X_E^7(12)$. This can be done by Lemma 6.3.1 and 6.3.2, with $m = 6$. In particular, we have

**Theorem 7.4.1.** *The curve $X_E(12)$ is birational to the curve $C \subset \mathbb{A}^5_{X,Y,u_0,u_1,u_2}/\mathbb{Q}$ with equations $G = G_1 = G_2 = G_3 = 0$ where*

$$\begin{aligned} G &= -X^2 + aXY^2 + 6bY^3 - 6aY^2 - 12, \\ G_1 &= (X^2 + 12X + 36) - D(-au_2^2 + 2u_0u_2 + u_1^2), \\ G_2 &= (4aXY + 36bY^2 - 24aY) - D(-2au_1u_2 - bu_2^2 + 2u_0u_1), \\ G_3 &= (8aX - 4a^2Y^2) - D(-2bu_1u_2 + u_0^2) \end{aligned}$$

*and $D = -4a^3 - 27b^2$.*

**Proof.** By Lemma 6.3.1, there is a $K(E[2])$-rational point on $X_E^7(12)$ above $t = \infty$ which corresponds to $(E, \phi)$ where $\phi$ is the same map as in Lemma 6.3.1 with $m = 6$. Therefore $\alpha_j, j = 1, 2, 3$ are squares in $K(E[2])$. But there is at most one quadratic subfield inside $K(E[2])$ which is $K(\sqrt{D})$ where $D = -4a^3 - 27b^2$.

We are free to multiply $\alpha_j$ by any non-zero squared factor of the form $(v_0 + v_1\theta_j + v_2\theta_j^2)^2$. This shows that we may pick $\alpha_j, j = 1, 2, 3$ to be 1 or $D$. But by Lemma 6.3.2 with $m = 6$, if $\alpha_j = 1, j = 1, 2, 3$ then $D$ is a square in $K$ and so we should pick $\alpha_j = D$ for each $j$. □

**Remark** The proof of the above theorem is very similar to the one for Theorem 6.3.3. In fact, Lemma 6.3.1 and 6.3.2 describe the function field of $X_E^{m+1}(2m)$ in terms of the function field of $X_E(2m)$, where $m > 2$ is an even number.

**Remark** Recall that one of the important properties we used to compute $X_E^3(8)$ and $X_E^5(8)$ is that $X_E(4) \cong X_E^3(4)$ over $K$. However, we have seen that $X_E(6)$ is not always isomorphic to $X_E^5(6)$ over $K$. For this reason, the curves $X_E^5(12)$ and $X_E^{11}(12)$ are much harder to compute.

# 8 Modular Diagonal Quotient Surfaces

In this chapter, we give some examples of modular diagonal quotient surfaces introduced in [KS]. Roughly speaking, for each $n \geq 2$ and $r \in (\mathbb{Z}/n\mathbb{Z})^*$, each point on the modular diagonal quotient surface $Z_{n,r}$ corresponds to a triple $(E_1, E_2, \phi)$ where $E_1, E_2$ are elliptic curves and

$$\phi : E_1[n] \to E_2[n]$$

is a Galois equivariant isomorphism such that

$$e_n(\phi(P), \phi(Q)) = e_n(P, Q)^r.$$

Geometric descriptions of these surfaces were given in [KS] Theorem 4. We now give some explicit equations of some of the surfaces and verify Theorem 4 in terms of the equations we give.

We will introduce two ad hoc methods to find equations for the surface $Z_{n,r}$ by using the equation of $X_E^r(n)$. The first method is the one we described in the previous chapters: let $b = a$ and treat $a$ as a variable. We will assume $K = \mathbb{Q}$. We start with some simple examples.

## 8.1 The Cases $n \leq 6$

**Proposition 8.1.1.** *For each $n = 2, 3, 4, 5$ and $r \in (\mathbb{Z}/n\mathbb{Z})^*$, the surface $Z_{n,r}$ is a rational surface and $Z_{n,r}$ is birational to $\mathbb{A}^2$ by taking coordinates $(t, a)$ where $t$ is the affine coordinate of $X_E^r(n)$.*

Since $X_E^r(n) \cong \mathbb{P}_t^1$, the above proposition is clear. We now consider the case for $n = 6$.

**Proposition 8.1.2.** *The surface $Z_{n,6}$ is a rational surface.*

**Proof.** The equation of $X_E(6)$ is $y^2 = x^3 - 16(4a^3 - 27b^2)$ for every elliptic curve $E : y^2 = x^3 + ax + b$. Therefore, setting $a = b$ and write

$$\frac{y^2}{8^2a^2} = a\frac{x^3}{4^3a^3} - (a - \frac{27}{4}).$$

Setting $y' = \frac{y}{8a}$ and $x' = \frac{x}{4a}$ we have

$$Z : y'^2 = ax'^3 - a + \frac{27}{4}$$

and so

$$Z \to \mathbb{A}^2, \quad (x, y, a) \mapsto (x, y)$$

is a birational map. $\square$

**Proposition 8.1.3.** *The surface $Z_{6,5}$ is an elliptic surface.*

This is clear because $X_E^5(6)$ itself is a genus one curve. In fact, it was shown in [KS] that $Z_{n,6}^5$ is a K3 surface. Unfortunately, we did not manage to find an elliptic fibration of $Z_{6,5}$ with a rational section.

## 8.2 The Case $n = 7$

We now briefly explain another method to find equations of modular diagonal quotient surfaces based on the following remark.

**Remark** If $E_1$ and $E_2$ are quadratic twists then it is easy to see that the modular curves $X_{E_1}^r(n)$ and $X_{E_2}^r(n)$ are isomorphic. In practice, it is often the case that if we replace $a$ by $\lambda^2 a$ and $b$ by $\lambda^3 b$, then there exists a change of coordinate of $X_E^r(n)$ such that if each coordinate of $X_E^r(n)$ is multiplied by some suitable powers of $\lambda$, then the equations for $X_E(n)$ are multiplied by some powers of $\lambda$. This allows us to define the weight of each coordinate. In particular, the weight of $a$ is 2 and the weight of $b$ is 3 for all $n, r$.

We treat both $a$ and $b$ as variables in the equation of $X_E^r(n)$, and obtain a variety of dimension 3. We then need to quotient out by the actions $a \mapsto \lambda^2 a, b \mapsto \lambda^3 b$ for all $\lambda \in K$. We will illustrate how this works in the following example.

**Proposition 8.2.1.** *$Z_{7,1}$ is a rational surface.*

**Proof.** Recall in [HK] that $X_E(7) \subset \mathbb{P}^2$ has equation $F = 0$ where

$$F = ax^4 + 7bx^3z + 3x^2y^2 - 3a^2x^2z^2 - 6bxyz^2 - 5abxz^3 + 2y^3z + 3ay^2z^2 + 2a^2yz^3 - 4b^2z^4.$$

Take the affine coordinate $z = 1$. A direct computation shows that

$$F(\lambda^2 a, \lambda^3 b, \lambda x, \lambda^2 y, 1) = \lambda^6 F(a, b, x, y, 1).$$

This suggests that the weights of $x$ and $y$ are 1 and 2 respectively. We make the following substitution. Let

$$a = uv - 3w^2,\ b = urw - uvw + 2w^3,\ x = w,\ y = w^2 + uw$$

and so $u, v, w, r$ all have weight 1. This means that if we replace $a$ by $\lambda^2 a$ and $b$ by $\lambda^3 b$, then we should replace $u, v, w, r$ by $\lambda u, \lambda v, \lambda w, \lambda r$ respectively. So $Z_{7,1}$ is birational to the surface in $\mathbb{P}^3_{u,v,w,r}$ with equation $G = 0$ where

$$G(u, v, w, r) = F(a, b, x, y, 1) = u^2 w(2uv^2 + 3uvw + 2uw^2 + 3vwr - 6w^2 r - 4wr^2).$$

Since $-4a^3 - 27b^2 \neq 0$, we have $u \neq 0$ and so we take the affine coordinate with $u = 1$. Then a birational model of $Z_{7,1}$ is given by $G(1, v, w, r) = 0$. We also take the open subvariety with $w \neq 0$. Therefore, the surface $Z_{7,1}$ is birational to the surface in $\mathbb{A}^3_{v,w,r}$ with equation

$$2v^2 + 3vw + 2w^2 + 3vwr - 6w^2 r - 4wr^2 = 0.$$

This can be viewed as a curve of genus 0 over $\mathbb{Q}(r)$ with equation

$$2v^2 + (3r + 3)vw + (-6r + 2)w^2 - 4r^2 w = 0$$

with a rational point $(v, w) = (0, 0)$. Therefore we conclude that $Z_{7,1}$ is a rational surface. $\square$

**Remark** A useful trick we used to find the substitution

$$a = uv - 3w^2, \quad b = urw + 2w^3, \quad x = w, \quad y = uw + w^2$$

in the proof above is to study the singular subscheme of $X_E(7)$ when $a = -3w^2, b = 2w^3$.

We will use the following statement, which can be found in [MT], to deduce whether an elliptic surface in Weierstrass form is K3.

**Remark** Let $X$ be an elliptic surface with Weierstrass form

$$X : y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6, a_i \in K[t], \deg a_i \leq 2i$$

then $X$ is a K3 surface.

**Proposition 8.2.2.** *$Z_{7,6}$ is an elliptic K3-surface and it has equation*

$$y^2 = x^3 + (4u^4 + 4u^3 - 51u^2 - 2u - 50)x^2 + (312u^3 + 1276u^2 + 50u + 625)x \ (\dagger).$$

**Proof.** Recall that in [PSS] $X_E^6(7) \subset \mathbb{P}^2$ has equation $G = 0$ where

$$\begin{aligned} G &= -a^2x^4 + 2abx^3y - 12bx^3z - (6a^3 + 36b^2)x^2y^2 + 6ax^2z^2 + 2a^2bxy^3 - 12abxy^2z \\ &+ 18bxyz^2 + (3a^4 + 9ab^2)y^4 - (8a^3 + 42b^2)y^3z + 6a^2y^2z^2 - 8ayz^3 + 3z^4. \end{aligned}$$

Let $b = a$ and divide $G$ by $a^6$ and set $x' = \frac{x}{a}, y' = \frac{y}{a}, z' = \frac{z}{a}$ and $a' = \frac{1}{a}$. Then

$$\begin{aligned} G' &= -x'^4 + 2x'^3y' - 12x'^3z' - (6a' + 36)x'^2y'^2 + 6a'x'^2z'^2 + 2a'x'y'^3 - 12a'x'y'^2z' + 18a'x'y'z'^2 \\ &+ (3a'^2 + 19a')y'^4 - (8a'^2 + 42a')y'^3z' + 6a'^2y'^2z'^2 - 8a'^2y'z'^3 + 3a'^2z'^4. \end{aligned}$$

The equation $G' = 0$ defines a birational model of $Z_{7,6}$ in $\mathbb{A}^1 \times \mathbb{P}^2$. Now take the affine coordinate $z' = 1$ and consider this as a curve over the function field $\mathbb{Q}(y')$. Then we have

$$\begin{aligned} G' &= (3y'^4 - 8y'^3 + 6y'^2 - 8y' + 3)a'^2 + (-6y'^2 + 6)a'x'^2 + (2y'^3 - 12y'^2 + 18y')a'x' \\ &+ (19y'^4 - 42y'^3)a' - x'^4 + (2y' - 12)x'^3 - 36y'^2x'^2. \end{aligned}$$

So $G' = 0$ defines a genus 1 curve over $\mathbb{Q}(y')$ with a rational point $(a', x') = (0, 0)$. Put this into Weierstrass form, and make the substitution $t = \frac{3}{4} \cdot \frac{2u-1}{u+1}$. Then we conclude that $Z_{7,6}$ is isomorphic to the elliptic surface $(\dagger)$. As an elliptic curve over $\mathbb{Q}(u)$, this has Mordell-Weil group $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}^2$ with a primitive 2-torsion point $(0, 0)$ and two points of infinite order

$$P_1 = (4u^2 + 20u + 25, -8u^4 - 44u^3 - 22u^2 + 95u), \quad P_2 = (6u + 25, 12u^3 + 56u^2 + 25u).$$

The previous remark shows that this is an elliptic K3-surface. □

**Remark** The above computation actually only showed that the Mordell-Weil rank is at least 2. To prove that the rank is exactly 2, we recall the following theorem. Let $Z$ be the above elliptic surface together with the projection $\pi : Z \to \mathbb{P}^1_u$. Then the Picard number $\rho$ of $Z$ is given by

$$\rho = r + 2 + \sum_{u \in \mathbb{P}^1} (r_u - 1)$$

where $r$ is the rank of $Z$ (as an elliptic curve over $\mathbb{Q}(u)$ and $r_t$ is the number of irreducible components in the fiber $Z_u$. A more general form of the theorem can be found in [S2, Corollary 1.5]. The Kodaira symbols of the elliptic surface $Z$ are give by

$$\langle I2,2\rangle, \langle I2,2\rangle, \langle I10,1\rangle, \langle I3,1\rangle, \langle I1,1\rangle, \langle I2,1\rangle$$

and so

$$\sum_{u\in\mathbb{P}^1}(r_u-1) = 2+2+9+2+1 = 16.$$

By [M1, Theorem 2.3], the Picard number $\rho$ of a K3 surface over a field of characteristic zero is bounded above by 20, and so in our case we must have $r \leq 2$. This gives an upper bound for the rank.

## 8.3 The Case $n = 8$

We start with Theorem 1.7.6, which gives the parametrisation of $Z_{8,1}$.

**Proof.** We start with Theorem 1.7.2 and set $b = a$ as a variable. Also for convenience we take the affine piece with $x_4 = 1$. So we have a surface which is birational to the surface defined by the following equations:

$$\begin{aligned}
f_1' &= -a + 2u_0 + u_1^2 + 2u_2^2,\\
f_2' &= -2au_1 - a + 2u_0u_1 - 2tu_2,\\
f_3' &= -2au_1 + u_0^2 + au_2^2 - t^2.
\end{aligned}$$

by $(a, x_0, x_1, x_2, x_3) \mapsto (a, \frac{-t}{u_2}, \frac{u_0}{u_2}, \frac{u_1}{u_2}, \frac{1}{u_2})$. We use $f_1', f_2'$ to write $a, t$ in terms of $u_0, u_1, u_2$

$$a = 2u_0 + u_1^2 + 2u_2^2, \quad t = \frac{-2au_1 - a + 2u_0u_1}{2u_2}.$$

Then substitute these into $f_3'$ so the equation the surface is given by $f' = 0$ where

$$\begin{aligned}
f' = {} & -u_0^2u_1^2 - 2u_0^2u_1 + u_0^2u_2^2 - u_0^2 - 2u_0u_1^4 - 3u_0u_1^3 - 4u_0u_1^2u_2^2 - u_0u_1^2 - 10u_0u_1u_2^2\\
& + 2u_0u_2^4 - 2u_0u_2^2 - u_1^6 - u_1^5 - 4u_1^4u_2^2 - \frac{1}{4}u_1^4 - 6u_1^3u_2^2 - 3u_1^2u_2^4 - u_1^2u_2^2\\
& - 8u_1u_2^4 + 2u_2^6 - u_2^4.
\end{aligned}$$

This can be viewed as a polynomial in $u_0$ with coefficients in $\mathbb{Q}[u_1,u_2]$. If we complete the square for $u_0$, then we have

$$u_0^2 - u_2^2\frac{u_1^6+3u_1^5+3u_1^4u_2^2+\frac{9}{4}u_1^4+9u_1^3u_2^2+u_1^2u_2^4+9u_1^2u_2^2+2u_1u_2^4-u_2^6+u_2^4}{(u_1-u_2+1)^2(u_1+u_2+1)^2}=0.$$

Now we can replace $u_0$ by $\frac{u_0u_2}{(u_1-u_2+1)(u_1+u_2+1)}$ and so we have the vanishing of

$$u_0^2-(u_1^6+3u_1^5+3u_1^4u_2^2+\frac{9}{4}u_1^4+9u_1^3u_2^2+u_1^2u_2^4+9u_1^2u_2^2+2u_1u_2^4-u_2^6+u_2^4).$$

Finally we replace $a_0$ by $a_0a_2^2$ and $a_1$ by $a_1a_2$, so we conclude the surface has equation $h'=0$ where

$$h'=u_0^2-(u_1^6u_2^2+3u_1^5u_2+3u_1^4u_2^2+\frac{9}{4}u_1^4+9u_1^3u_2+u_1^2u_2^2+9u_1^2+2u_1u_2-u_2^2+1).$$

This equation defines a genus zero curve over $\mathbb{Q}(u_1)$ with a rational point

$$u_0=\frac{3u_1-\frac{3}{2}u_1^2+\frac{1}{2}u_1^3}{u_1-1}, u_2=-\frac{1}{u_1-1}.$$

Therefore we find a parametrization for the surface in $\mathbb{A}^3_{u_0,u_1,u_2}$ defined by $h'=0$

$$u_1=v,\ u_0=-\frac{1}{2}\frac{H_1(u,v)}{H_2(u,v)} \text{ and } u_2=\frac{H_3(u,v)}{H_4(u,v)}$$

where

$$\begin{aligned}H_1(u,v)&=4u^2v^3-12u^2v^2+24u^2v-12uv^5+36uv^4-72uv^3+144uv^2+16u\\&\quad+9v^7-27v^6+90v^5-108v^4+220v^3-12v^2+24v,\\H_2(u,v)&=4u^2v-4u^2-4uv^3+12uv^2-24uv-3v^5-9v^4-36v^2-4v-4\end{aligned}$$

and

$$\begin{aligned}H_3(u,v)&=-4u^2+9v^4+36v^2+4,\\H_4(u,v)&=4u^2v-4u^2-4uv^3+12uv^2-24uv-3v^5-9v^4-36v^2-4v-4.\end{aligned}$$

Now we work backwards through the above isomorphisms. Let $p=u+\frac{3}{2}v^2$ and $q=v$. Then we obtain expressions for $a,x_0,x_1,x_2,x_3$ in terms of $p$ and $q$. Finally, we observe that

$$\begin{aligned}f_1(\lambda^2a,\lambda^3b;\lambda x_0,\lambda x_1,x_2,\lambda^{-1}x_3,x_4)&=f_1(a,b;x_0,x_1,x_2,x_3,x_4),\\g_1(\lambda^2a,\lambda^3b;\lambda x_0,\lambda x_1,x_2,\lambda^{-1}x_3,x_4)&=\lambda g_1(a,b;x_0,x_1,x_2,x_3,x_4),\\h_1(\lambda^2a,\lambda^3b;\lambda x_0,\lambda x_1,x_2,\lambda^{-1}x_3,x_4)&=\lambda^2h_1(a,b;x_0,x_1,x_2,x_3,x_4).\end{aligned}$$

Theorem 1.7.6 follows by setting

$$\lambda = \frac{p(p^2q - p^2 + 2pq^3 - 6pq - 9q^3 - 9q^2 - q - 1)}{-p^2 - 3pq^2 + 9q^2 + 1}$$

and

$$(a^{\{p,q\}}, b^{\{p,q\}}; x_0^{\{p,q\}}, x_1^{\{p,q\}}, x_2^{\{p,q\}}, x_3^{\{p,q\}}) = (\lambda^2 a, \lambda^3 b; \lambda x_0, \lambda x_1, x_2, \lambda^{-1} x_3).$$

□

We now prove Theorem 1.7.7 (the surface $Z_{8,3}$)

**Proof.** Take the equations for $X_E^3(8)$ in Theorem 1.7.3 and take the affine piece with $x_4 = 1$. We make the following substitution

$$x_3 = T,\ a = 2uv - 3w^2,\ b = u^2y - 2uvw - Tuwz + 2w^3,$$
$$x_0 = -3Tuv - (T^2-1)uz + 6Tw^2, x_1 = -3Tw,\ x_2 = u - 3w.$$

A direct computation shows that

$$f_3(\lambda^2 a, \lambda^3 b; \lambda^2 x_0, \lambda x_1, \lambda x_2, x_3, 1) = \lambda^4 f_3(a, b; x_0, x_1, x_2, x_3, 1),$$
$$g_3(\lambda^2 a, \lambda^3 b; \lambda^2 x_0, \lambda x_1, \lambda x_2, x_3, 1) = \lambda^3 g_3(a, b; x_0, x_1, x_2, x_3, 1),$$
$$h_3(\lambda^2 a, \lambda^3 b; \lambda^2 x_0, \lambda x_1, \lambda x_2, x_3, 1) = \lambda^2 h_3(a, b; x_0, x_1, x_2, x_3, 1).$$

Therefore the action

$$(a, b; x_0, x_1, x_2, x_3, 1) \mapsto (\lambda^2 a, \lambda^3 b; \lambda^2 x_0, \lambda x_1, \lambda x_2, x_3, 1)$$

induces the trivial action

$$(u : v : w : y : z) \mapsto (\lambda u : \lambda v : \lambda w : \lambda y : \lambda z) = (u : v : w : y : z).$$

Make the substitution above and replace $h_3$ by $3f_3 - ah_3$. Then $Z_{8,3}$ is birational to the surface in $\mathbb{P}^4_{(u:v:w:y:z)} \times \mathbb{A}^1_T$ defined by $F_3 = G_3 = H_3 = 0$ where

$$F_3 = u^2(-6w^2 + 4uv + 12wv + (27T^2 - 24)v^2 - 18uy + (-54T^2 + 54)wy$$
$$+ 18Twz + (30T^3 - 30T)vz + (3T^4 - 6T^2 + 3)z^2),$$
$$G_3 = u(-12w^2 + 8uv + 12wv + (-9T^2 - 18)uy + (15T^3 + 12T)wz),$$
$$H_3 = u(u - 6w + 6v + (-6T^3 + 6T)z).$$

But when $u = 0$, we have $-4a^3 - 27b^2 = 0$. Therefore $u \neq 0$ and so we can replace $F_3, G_3, H_3$ by $\frac{F_3}{u^2}, \frac{G_3}{u}, \frac{H_3}{u}$ respectively. In particular, $H_3$ is linear now and we can replace $u$ by $6w - 6v + (6T^3 - 6T)z$. Make this substitution in $F_3$ and $G_3$, we conclude that $Z_{8,3}$ is birational to $F_3' = G_3' = 0$ where

$$\begin{aligned} F_3' &= -6w^2 + 36wv + (27T^2 - 48)v^2 + (-54T^2 - 54)wy + 108vy + 18Twz \\ &\quad + (54T^3 - 54T)vz + (-108T^3 + 108T)yz + (3T^4 - 6T^2 + 3)z^2, \\ G_3' &= -12w^2 + 60wv - 48v^2 + (-54T^2 - 108)wy + (54T^2 + 108)vy \\ &\quad + (15T^3 + 12T)wz + (48T^3 - 48T)vz + (-54T^5 - 54T^3 + 108T)yz. \end{aligned}$$

This can be viewed as a genus one curve $C \subset \mathbb{P}^3_{v,w,y,z}$ over $\mathbb{Q}(T)$ defined by $F_3' = G_3' = 0$, with a rational point $(v : w : y : z) = (0 : 0 : 1 : 0)$. Replace $T$ by $1/T$ and put $C$ into Weierstrass form we conclude that $C$ is isomorphic to the one in Theorem 1.7.7

$\square$

We now prove Theorem 1.7.8 (the surface $Z_{8,5}$)

**Proof.** We start with Theorem 1.7.4 and treat both $a$ and $b$ as variables. For convenience we again take the affine piece with $x_4 = 1$. We see that $g_5$ is linear in $b$ and so we can eliminate the variable $b$ by using $g_5 = 0$. In other words, we can replace $g_5$ by

$$g_5' = h_5(u_2^2 - 6) + g_5(6t - 2u_1u_2).$$

Now make the following substitution

$$x_3 = T, a = wx, x_1 = (u + Tx)w, x_0 = v - 6w, x_2 = (T - 3)v - 3w,$$

and further replace $g_5'$ by

$$G_5 = (T^2 - 6T + 12)g_5' + 4((T^2 - 3T - 3)u - (2T + 3)x)(T - 3)wf_5.$$

Since

$$\begin{aligned} f_5(\lambda^2 a, \lambda^3 b; \lambda x_0, \lambda^2 x_1, \lambda x_2, x_3, 1) &= \lambda^2 f_5(a, b; x_0, x_1, x_2, x_3, 1), \\ g_5(\lambda^2 a, \lambda^3 b; \lambda x_0, \lambda^2 x_1, \lambda x_2, x_3, 1) &= \lambda^3 g_5(a, b; x_0, x_1, x_2, x_3, 1), \\ h_5(\lambda^2 a, \lambda^3 b; \lambda x_0, \lambda^2 x_1, \lambda x_2, x_3, 1) &= \lambda^4 h_5(a, b; x_0, x_1, x_2, x_3, 1), \end{aligned}$$

the action

$$(a,b;x_0,x_1,x_2,x_3,1) \mapsto (\lambda^2 a, \lambda^3 b; \lambda^2 x_0, \lambda x_1, \lambda x_2, x_3, 1)$$

induces the trivial action

$$(u:v:w:x) \mapsto (\lambda u : \lambda v : \lambda w : \lambda x) = (u:v:w:x).$$

So $Z_{8,5}$ is birational to the surface defined by $f_5 = G_5 = 0$ and a direct computation shows that $f_5$ and $w^{-2}G_5$ are quadratic in variables $u, v, w, x$.

When $w = 0$, we have $a = 0, x_1 = 0, x_0 = v, x_2 = (T-3)v$ and $x_3 = T$. Using $g_5 = 0$ we conclude that $b = 0$ and so $-4a^3 - 27b^2 = 0$. So we may assume $w \neq 0$. Therefore, setting $H_5 = w^{-2}G_5$, we conclude that $Z_{8,5}$ is a complete intersection of two quadrics in $\mathbb{P}^3_{u,v,w,x}$ defined by $f_5 = H_5 = 0$ over $\mathbb{Q}(T)$, with a rational point

$$(u:v:w:x) = (T^3 - 4T^2 - 4T + 18 : 0 : 0 : -3(T^2 - 4T + 2)).$$

Put this curve into Weierstrass form we see that it is isomorphic to the one stated in Theorem 1.7.8. □

We now prove Theorem 1.7.9 (the surface $Z_{8,7}$)

**Proof.** We start with Theorem 1.7.5 and take the affine piece with $x_4 = 1$. Now make the following substitution

$$\begin{aligned} a &= \frac{-T^2+6}{3}ux - 3uv - 3w^2,\ b = \frac{1}{9}u^2 y + \frac{2T^2-4}{3}uwx + \frac{2}{3}uvw + 2w^3, \\ x_0 &= \frac{Tu}{3} + w,\ x_1 = -\frac{2}{3}Tuv - 2w^2 T,\ x_2 = 2u + wT,\ x_3 = T. \end{aligned}$$

When $u = 0$, we have $a = -3w^2$ and $b = 2w^3$ and so $-4a^3 - 27b^2 = 0$. So $u \neq 0$. Since

$$\begin{aligned} f_7(\lambda^2 a, \lambda^3 b; \lambda x_0, \lambda^2 x_1, \lambda x_2, x_3, 1) &= \lambda^2 f_7(a,b;x_0,x_1,x_2,x_3,1), \\ g_7(\lambda^2 a, \lambda^3 b; \lambda x_0, \lambda^2 x_1, \lambda x_2, x_3, 1) &= \lambda^3 g_7(a,b;x_0,x_1,x_2,x_3,1), \\ h_7(\lambda^2 a, \lambda^3 b; \lambda x_0, \lambda^2 x_1, \lambda x_2, x_3, 1) &= \lambda^4 h_7(a,b;x_0,x_1,x_2,x_3,1), \end{aligned}$$

the action

$$(a,b;x_0,x_1,x_2,x_3,1) \mapsto (\lambda^2 a, \lambda^3 b; \lambda x_0, \lambda^2 x_1, \lambda x_2, x_3, 1)$$

induces the trivial action

$$(u:v:w:x:y) \mapsto (\lambda u : \lambda v : \lambda w : \lambda x : \lambda y) = (u:v:w:x:y).$$

We make the above substitution and so

$$f_7 = uF_7,\ g_7 = u^2G_7, h_7 = uH_7$$

where $F_7, G_7$ are linear and $H_7$ is cubic in $u, v, w, x, y$. Use $F_7, G_7$ to write $w$ and $y$ in terms of the other variables. After some simplification, we conclude that $Z_{8,7}$ is birational to surface defined by $F' = 0$ where

$$\begin{aligned}F' &= (2T^6 + 60T^4 - 360T^2 - 432)u^2v + (-3T^7 + 46T^5 - 36T^3 - 792T)u^2x \\ &\quad + (-4T^5 - 144T^3 + 1008T)uv^2 + (6T^6 - 36T^4 + 264T^2 - 1008)uvx \\ &\quad + (-30T^5 + 568T^3 - 2232T)ux^2 + (2T^4 + 84T^2 - 576)v^3 \\ &\quad + (-3T^5 - 10T^3 - 456T)v^2x + (30T^4 - 338T^2 + 180)vx^2 + (-75T^3 + 394T)x^3.\end{aligned}$$

This is a plane cubic curve defined over $\mathbb{Q}(T)$ with a rational point $(1 : 0 : 0)$. Put this into the Weierstrass form and replace $T$ by $2T$ and so this curve is isomorphic to the one in Theorem 1.5. $\square$

There are some other examples of explicit equations of modular diagonal quotient surfaces. For example, the equations in the case $n = 9$ can be found in [F4, Theorem 1.4].

# 9 Numerical Examples And Further Questions

We focus on the case $K = \mathbb{Q}$ and we only consider the elliptic curves over $\mathbb{Q}$ in this chapter.

## 9.1 Traces of Frobenius

**Definition 9.1.1.** *Let $E/\mathbb{Q}$ be an elliptic curve and $q$ is a prime. The trace of Frobenius of $E$ at $q$ is*

$$a_p = q + 1 - |E(\mathbb{F}_q)|$$

*where $|E(\mathbb{F}_q)|$ is the number of $\mathbb{F}_q$ points of $E$.*

**Theorem 9.1.2.** *Let $E$ be an elliptic curve over $\mathbb{Q}$ and $K_n = \mathbb{Q}(E[n])$ be the field extension of $\mathbb{Q}$ which adjoins the coordinates of the $n$-torsion points of $E$. Each element in $\mathrm{Gal}(K_n/\mathbb{Q})$ acts on $E[n]$ and so we obtain a natural map*

$$\chi_n : \mathrm{Gal}(K_n/\mathbb{Q}) \to Aut(E[n]).$$

*Let $q$ be a prime of good reduction for $E$ and $Frob_q$ be the corresponding Frobenius element in $\mathrm{Gal}(K_n/\mathbb{Q})$. Then we have the following congruence relation for the trace*

$$Tr(\chi_n(Frob_q)) \equiv a_q \ (mod\ n).$$

**Proof.** See [S, Chapter 5]. □

In particular, the above theorem shows that

**Corollary 9.1.3.** *Let $E_1$ and $E_2$ be elliptic curves over $\mathbb{Q}$. Let $q$ be a prime of good reduction for both $E_1$ and $E_2$ and $a_q$ (resp. $b_q$) be the trace of Frobenius of $E_1$ (resp. $E_2$) at $q$. If $E_1$ and $E_2$ are $n$-congruent, then*

$$a_q \equiv b_q (mod\ n).$$

**Proof.** $E_1$ and $E_2$ are $n$-congruent if and only if they have the same mod $n$ representation. The corollary follows from the previous theorem. □

The corollary gives a way to check whether two given elliptic curves are $n$-congruent. We now give some numerical examples.

## 9.2 The Case $n = 6$

**Example 9.2.1.** *Let $E : y^2 = x^3 - 6x + 8$. Then we have a point $(x, y, z) = (1, 864, 24)$ on $X_E^5(6)$ where the equations for $X_E^5(6)$ are given in Theorem 1.7.1. Recall from Section 4.3 that the forgetful map $X_E^5(6) \to X_E^2(3)$ is given by $(x, y, z) \mapsto x/3$. Therefore, we take $F$ to be the curve corresponding to the point $1/3$ on $X_E^2(3)$ and we get*

$$F : y^2 = x^3 - \frac{2187}{2}x + 19683.$$

*We give the traces of Frobenius of these curves at small primes.*

| Prime | 2 | 3 | 5 | 7 | 11 | 13 | 17 | 19 | 23 | 29 | 31 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Traces of Frobenius(E) | 0 | 0 | 3 | 3 | -3 | -6 | -6 | 2 | -6 | 6 | -3 |
| Traces of Frobenius(F) | 0 | 0 | 3 | -3 | 3 | 6 | 6 | 2 | -6 | 6 | 3 |

We see that they have the same traces of Frobenius mod 6.

## 9.3 The Case $n = 8$

We give some triples of 8-congruent elliptic curves. The first example we give is in the case that all three curves are in the Cremona's database.

**Example 9.3.1.** *The elliptic curves $129a1, 645e1, 23349a1$ are 8-congruent to each other. We give the traces of Frobenius of these curves at small primes.*

| Prime | 2 | 3 | 5 | 7 | 11 | 13 | 17 | 19 | 23 | 29 | 31 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Traces of Frobenius(129a1) | 0 | -1 | -2 | -2 | -5 | 3 | -3 | 2 | -1 | 0 | -5 |
| Traces of Frobenius(645e1) | 0 | 1 | 1 | -2 | -5 | -5 | 5 | -6 | -9 | 8 | -5 |
| Traces of Frobenius(23349a1) | 0 | 1 | -2 | -2 | 3 | 3 | -3 | 2 | -1 | 0 | 3 |

We see that apart from $p = 2$ or 3, they have the same traces of Frobenius mod 8.

In principal, one can find all triples of elliptic curves in Cremona's database which are 8-congruent by computing the traces of Frobenius. We now give some triples such that at least one of the curves is not in Cremona's database.

**Example 9.3.2.** *The elliptic curves* $123b1, 7257c1$ *and* $E$ *are* $8$*-congruent to each other where*

$$E : y^2 + y = x^3 - x^2 - 141523922665x + 27678844064358381.$$

*We give the traces of Frobenius of these curves at small primes.*

| Prime | 2 | 3 | 5 | 7 | 11 | 13 | 17 | 19 | 23 | 29 | 31 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Traces of Frobenius(123b1) | 0 | -1 | -2 | -4 | 5 | -4 | -5 | -2 | 4 | 1 | -5 |
| Traces of Frobenius(7257c1) | 0 | -1 | -2 | 4 | 5 | -4 | 3 | -2 | -4 | -7 | 3 |
| Traces of Frobenius(E) | 0 | -1 | 1 | -4 | -3 | -4 | -5 | -2 | -4 | 9 | -5 |

We see that apart from $p = 5$, they have the same traces of Frobenius mod 8.

**Example 9.3.3.** *The elliptic curves* $798i2, E_1$ *and* $E_2$ *are* $8$*-congruent to each other where*

$$E_1 : y^2 + xy = x^3 - 117530731548307x + 235301448542588748065,$$
$$E_2 : y^2 + xy = x^3 - x^2 - 29008860684x - 3143755969310512.$$

The following minimisation method helps to find these triples. We will focus on the curve $X_E(8)$. We define the invariants as follows. The curve $X_E(8)$ is defined by the intersection of three quadrics $f_1, g_1, h_1$ in $\mathbb{P}^4$, and we define the symmetric matrices $M_1, M_2, M_3$ associated to $f_1, g_1, h_1$ respectively. Let $M = xM_1 + yM_2 + zM_3$ and let $F$ be the determinant of $M$, which is a degree 5 polynomial in $x, y, z$. A direct computation shows that $F$ factorises into the product of a quadratic form $F_2$ and a cubic form $F_3$. Let $I_2$ be the determinant of symmetric matrix associated to $F_2$ and $I_3$ be the degree 6 invariant of $F_3$. Then we define $I = I_2^2 I_3$ to be the invariant of $F$.

For each prime $p > 3$, we define the level of $X_E(8)$ at $p$ to be the $p$-adic valuation of the invariant $I$. We aim to minimise the level by a change of coordinates in these quadratic forms. This is a local problem. In practise we use a range of ad hoc tricks to minimise the level.

Replacing $E$ by a quadratic twist does not change the curve $X_E(8)$ so we may assume either $E$ has good reduction, multiplicative reduction, or additive reduction of type II, III and IV.

Explicitly we minimise the level at $p$ by the following steps. If $E$ has good reduction at $p$, then the level of $X_E(8)$ at $p$ is zero. If $E$ has additive reduction of type III, consider the change of coordinate

$$\frac{1}{p}f_1(px_0, px_1, x_2, x_3, x_4), \frac{1}{p^2}g_1(px_0, px_1, x_2, x_3, x_4), \frac{1}{p^2}h_1(px_0, px_1, x_2, x_3, x_4).$$

If $E$ has additive reduction of type IV, consider the change of coordinate

$$f_1(px_0, px_1, x_2, x_3, x_4), \frac{1}{p}g_1(px_0, px_1, x_2, x_3, x_4), \frac{1}{p^2}h_1(px_0, px_1, x_2, x_3, x_4).$$

If $E$ has multiplicative reduction at $p$, then by Tate's algorithm we can find $b_0, b_2, b_4$ such that $E$ is isomorphic to the curve $y^2 = x^3 + b_2x^2 + b_4x + b_6$ where $b_2, b_4, b_6$ depends on the Kodaira's symbol of $E$ at $p$, and

$$a = -\frac{1}{3}b_2^2 + b_4,\ b = \frac{2}{27}b_2^3 - \frac{1}{3}b_2b_4 + b_6.$$

Make the change of coordinate

$$f_1' = f_1(\chi), g_1' = g_1(\chi) - \frac{1}{3}f_1', h_1' = h_1(\chi) + \frac{1}{3}b_2f_2' + \frac{2}{9}b_2^2f_1'$$

where

$$\chi = (x_0 + \frac{1}{9}b_2x_4, x_1 - \frac{2}{9}b_2^2x_3, x_2 + \frac{1}{3}b_2x_3, x_3, x_4).$$

If the level at $p$ is a multiple of 8, say $8k$, consider further the change of coordinate

$$\frac{1}{p^{4k}}f_1'(\pi), \frac{1}{p^{6k}}g_1'(\pi), \frac{1}{p^{8k}}h_1'(\pi)$$

where

$$\pi = (p^{4k}x_0, p^{4k}x_1 - \frac{1}{3}p^{3k}x_2b_2, p^{3k}x_2, x_3, p^{2k}x_4).$$

A direct computation shows that the resulting equation for $X_E(8)$ has level 0 at $p$. Moreover, one can check that the above change of coordinate shows that the minimal level at $p$ we can achieve only depends on the level at $p$ mod 8. Then we can, for example, consider the resulting equation of $X_E(8)$ mod $p$, and move the singular point (if it turns out that the singular subscheme over $\mathbb{Q}$ is a point) to $(0 : 0 : 0 : 0 : 1)$ and apply a diagonal change of coordinate.

The reduction step in our case is simply by using standard method of reducing quadrics. These minimisation and reduction tricks help us to find the triples of directly 8-congruent elliptic curves above.

Recall that in Section 1.5 that if $E$ is $m$-isogenous to $F$ then $F$ is $n$-congruent to $E$ with power $m$ provided that $(m,n)=1$. So in principal we shall be able to find copies of $X_0(m)$ on $Z_{n,m}$. We illustrate an example.

We will compute a copy of $X_0(5)$ on $Z_{8,5}$. Let $E_r : y^2 = x^3 + a_r x + b_r$ be the families of elliptic curves parameterized by $X_0(5)$, where

$$\begin{aligned} a_r &= -27r^4 + 324r^3 - 378r^2 - 324r - 27, \\ b_r &= 54r^6 - 972r^5 + 4050r^4 + 4050r^2 + 972r + 54. \end{aligned}$$

The corresponding 5-isogenous curve $F_r$ has equation

$$y^2 + (1-r)xy - ry = x^3 - rx^2 - 5r(r^2+2r-1)x - r(r^4+10r^3-5r^2+15r-1)$$

and it has $j$-invariant $\frac{(r^4+228r^3+494r^2-228r+1)^3}{r(r^2-11r-1)^5}$. By considering the $j$-map $X_E(4) \to X(1)$ we obtain the value of $t$ which corresponds to $F_r$. Then the point on $X_E^5(8)$ corresponding to $F_r$ is

$$\begin{aligned} t &= r^2+1, \\ x_0 &= -1944r(r^3-11r^2+7r+1)(r^3-7r^2-11r-1), \\ x_1 &= 324r(r^2-12r-1)(r^2+1), \\ x_2 &= 108r(r^2-6r-1), \\ s &= 1. \end{aligned}$$

which can be viewed as a genus 0 curve parametrised by $r$ on $Z_{8,5}$.

## 9.4 The Case $n = 10$

**Example 9.4.1.** *Take the example as in Section 5.2. Recall that $E$ and $F$ are 10-congruent where*

$$E : y^2 = x^3 - 888x - 888$$

*and*

$$F : y^2 = x^3 - 20295349860367278828x + 50177913439407221073308928 48.$$

*We give the traces of Frobenius of these curves at small primes.*

| Prime | 2 | 3 | 5 | 7 | 11 | 13 | 17 | 19 | 23 | 29 | 31 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Traces of Frobenius(E) | 0 | 0 | -1 | 3 | 4 | 0 | -6 | -8 | -4 | 1 | 6 |
| Traces of Frobenius(F) | 0 | 0 | -1 | 3 | 4 | 0 | 4 | 2 | -4 | -9 | 6 |

We see that they have the same traces of Frobenius mod 10.

## 9.5 The Case $n = 12$

**Example 9.5.1.** *Take the example in Section 7.3 with $p = 0$. Then we obtain a pair of 12-congruent curves $E$ and $F$ where*

$$E : y^2 = x^3 + 3100766742402682222362151594025174441938867338885300x$$
$$+ 163539130256807151059647864858281041805880541242727661974214689262398749050000$$

*and*

$$F : y^2 = x^3 - 38015780030065475723459641070700x$$
$$- 97727701703365933429955335721578973399205870000$$

*We give the traces of Frobenius of these curves at small primes.*

| Prime | 2 | 3 | 5 | 7 | 11 | 13 | 17 | 19 | 23 | 29 | 31 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Traces of Frobenius(E) | 0 | 0 | 0 | 4 | -2 | 0 | 0 | -6 | -4 | 9 | 0 |
| Traces of Frobenius(F) | 0 | 0 | 0 | 4 | -2 | 0 | 0 | -6 | -4 | -3 | 0 |

We see that they have the same traces of Frobenius mod 12.

## 9.6 Other Examples

For $n \geq 13$, it is not known whether there are infinitely many pairs of non-isogenous $n$-congruent elliptic curves. Nonetheless, searching in Cremona's table enables us to find examples of $n$-congruent elliptic curves for $n \geq 13$. For example, when $n = 13$, the curves 52a2 and 988b1 are 13-congruent and when $n = 17$, the curves 3675b1 and 47775b1 are 17-congruent. In fact, [KO, Proposition 4], shows that if $p$ is a prime, then to check whether two curves $E_1$ and $E_2$ are $p$-congruent, it suffices to check that the traces of Frobenius of $E_1$ and $E_2$ at $q$ are congruent mod $p$ for all $q < M$ where $M$ is a certain bound.

## 9.7 Further Questions

We briefly discuss further questions in this research topic.

1. In Section 8.1, we did not manage to find an elliptic fibration of the surface $Z_{6,5}$ which admits a rational section. Since for $n = 7$ and $n = 8$, we managed to find elliptic fibrations for the surfaces $Z_{n,r}$ which admit rational sections, we strongly believe that the same conclusion should hold for $Z_{6,5}$.

2. The method we used to compute $X_E(6)$ and $X_E^5(6)$ can be used to compute $X_E(2n)$ where $n$ is an odd number. But this method gives very complicated equations for $X_E(2n)$. It is then not easy to find simple equations for the surface $Z_{2n,1}$. For example, Kani and Schanz shows that the surface $Z_{10,1}$ is an elliptic surface. However, with our equations for $X_E(10)$, we cannot proceed to find an elliptic fibration for $Z_{10,1}$. It would be easier to find an elliptic fibration for $Z_{10,1}$ if one manages to find a simpler equation for $X_E(10)$.

3. The surface $Z_{12,1}$ is an elliptic-K3 surface but we have not managed to find an elliptic fibration.

4. It is not known whether there exist infinitely many pairs of non-isogenous elliptic curves which are $n$-congruent for $n \geq 13$. Further, it is not even known whether there exists any pair of non-isogenous elliptic curves which are $n$-congruent for $n$ large enough.

# 10 Appendix

The coordinates $P_5 = (x_{5,1}, y_{5,1})$ and $Q_5 = (x_{5,2}, y_{5,2})$ in Theorem 2.1.2(iv) are given by

$$
\begin{aligned}
x_{5,1} &= 3u^{10} + 36u^8v^2 + 36u^7v^3 + 72u^6v^4 - 90u^5v^5 + 180u^4v^6 - 108u^3v^7 + 72u^2v^8 \\
&\quad - 36uv^9 + 3v^{10}, \\
y_{5,1} &= 108u^{13}v^2 - 108u^{12}v^3 + 432u^{11}v^4 + 540u^9v^6 - 648u^8v^7 + 2268u^7v^8 \\
&\quad - 3132u^6v^9 + 2700u^5v^{10} - 1620u^4v^{11} + 972u^3v^{12} - 432u^2v^{13} + 108uv^{14}, \\
x_{5,2} &= 3u^{10} + 36\zeta u^8v^2 + (-36\zeta^3 - 36\zeta^2 - 36\zeta - 36)u^7v^3 + 72\zeta^2u^6v^4 - 90u^5v^5 \\
&\quad + 180\zeta^3u^4v^6 - 108\zeta u^3v^7 + (-72\zeta^3 - 72\zeta^2 - 72\zeta - 72)u^2v^8 - 36\zeta^2uv^9 + 3v^{10}, \\
y_{5,2} &= 108\zeta u^{13}v^2 + 108(\zeta^3 + \zeta^2 + \zeta + 1)u^{12}v^3 + 432\zeta^2u^{11}v^4 + 540\zeta^3u^9v^6 \\
&\quad - 648\zeta u^8v^7 - 2268(\zeta^3 + \zeta^2 + \zeta + 1)u^7v^8 - 3132\zeta^2u^6v^9 + 2700u^5v^{10} - 1620\zeta^3u^4v^{11} \\
&\quad + 972\zeta u^3v^{12} + 432(\zeta^3 + \zeta^2 + \zeta + 1)u^2v^{13} + 108\zeta^2uv^{14}
\end{aligned}
$$

where $\zeta$ is a fixed fifth root of unity.

The rational function $g_i$ in Section 7.2 is $g_i = h_i/g$ where

$$
\begin{aligned}
h_i &= ((-12ab\theta_i^2 + 4a^3\theta_i)x^2 + (-48a^2b\theta_i^2 + (-32a^4 - 288ab^2)\theta_i)x + ((384a^3b + 2592b^3)\theta_i^2 \\
&+ (64a^5 + 288a^2b^2)\theta_i + (288a^4b + 1728ab^3)))y + a^2\theta_i^2x^4 + ((8a^3 + 36b^2)\theta_i^2 - 12a^2b\theta_i + 4a^4)x^3 \\
&+ ((-48a^4 - 432ab^2)\theta_i^2 + (144a^3b + 1296b^3)\theta_i + (-48a^5 - 432a^2b^2))x^2 + (-256a^5 - 1728a^2b^2)\theta_i^2x \\
&+ (1024a^6 + 11520a^3b^2 + 31104b^4)\theta_i^2 + (-1536a^5b - 10368a^2b^3)\theta_i + 512a^7 + 3456a^4b^2,
\end{aligned}
$$

and

$$
g = a^4x^2 + a^2(-8a^3 - 72b^2)x + (16a^6 + 288a^3b^2 + 1296b^4).
$$

# Bibliography


[AKM$^3$P] S. An, S. Kim, D. Marshall, S. Marshall, W. McCallum, P. Alexander, *Jacobians of genus one curves.* J. Number Theory 90 (2001), no. 2, 304-315.

[BCP] W. Bosma, J. Cannon and C. Playoust,*The Magma algebra system I: The user language*, J. Symb. Comb. 24 , 235-265 (1997). See also the Magma home page at `http://magma.maths.usyd.edu.au/magma/`

[BD] N. Bruin, K. Doerken, *The Arithmetic of genus two curves with* $(4, 4)$*-split Jacobians*, `http://arxiv.org/pdf/0902.3480.pdf`.

[CM] J.E. Cremona and B. Mazur, *Visualizing elements in the Shafarevich-Tate group, Experimental Mathematics* 9:1, (2000) 13-28.

[F1] T.A. Fisher, *The Hessian of a genus one curve* Proc. Lond. Math. Soc. (3) 104 (2012) 613-648.

[F2] T.A. Fisher, *Invariant theory for the elliptic normal quintic, I. Twists of* $X(5)$ Math. Ann. 356 (2013), no.2, 589-616.

[F3] T.A. Fisher, *On families of 7 and 11-congruent elliptic curves*, LMS J. Comput. Math. 17 (2014), no.1, 536-564.

[F4] T.A. Fisher, *On families of 9-congruent elliptic curves*, to appear in Acta Arithmetica. `http://arxiv.org/abs/1504.07891`.

[HK] E. Halberstadt and A. Kraus, *Sur la courbe modulaire* $X_E(7)$, Experiment. Math. 12 (2003), no.1, 27-40.

[K] F.Klein, *Lectures on the icosahedron and the solution of equations of the fifth degree*, Dover Publications, Inc., New York, N.Y., 1956.

[KO] A. Kraus and J. Oesterle, *Sur une question de B. Mazur*, Math. Ann. 293, 259-275 (1992).

[KS] E.Kani and W.Schanz, *Modular Diagonal Quotient Surfaces*, Math. Z. 227 (1998), no.2, 337-366.

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

[M1] Jean-Yves Merindol, *Proprietes elementaires des surfaces K3*, Asterisque (1985), no. 126, 45-57, Geometry of K3 surfaces: moduli and periods (Palaiseau, 1981/1982). MR 785222.

[MT] M. Schütt and T. Shioda, *Elliptic surfaces*, `http://arxiv.org/pdf/0907.0298.pdf`.

[P] I. Papadopoulos, *Courbes elliptiques ayant meme 6-torsion qu'une courbe elliptique donnee*. Journal of Number Theory 79, 103-114 (1999).

[PSS] B.Poonen, E.F.Schaefer and M.Stoll, *Twists of $X_(7)$ and primitive solutions to $x^2 + y^3 = z^7$*, Duke Math. J. 137 (2007), no. 1, 103-158.

[S] J.H.Silverman, The Arithmetic of Elliptic Curves, Springer-Verlag, GTM 106, 1986. Expanded 2nd Edition, 2009.

[S1] A. Silverberg, *Explicit families of elliptic curves with prescribed mod N representations*, in Modular Forms and Fermat's Last Theorem, eds. Gary Cornell, Joseph H. Silverman, Glenn Stevens, Springer-Verlag, Berlin-Heidelberg-New York (1997), 447-461.

[S2] T.Shioda, *On elliptic modular surfaces*, J. Math. Soc. Japan 24 (1972), 20-59.

[R] D.E.Rohrlich, *Modular Curves, Hecke Correspondences, and L-Functions*. Modular Forms and Fermat's Last Theorem, eds. Gary Cornell, Joseph H. Silverman, Glenn Stevens, Springer-Verlag, Berlin-Heidelberg-New York (1997), 41-100.

[R1] J.P.Roberts, *Explicit families of elliptic curves with prescribed mod 6 representations*. PhD thesis, The Ohio State University, 1999.

[RS1] K.Rubin and A.Silverberg, *Mod* 2 *Representations Of Elliptic Curves*. Proceedings of the American Mathematical Society, Volume 129,Number 1,Pages 53-57.

[RS2] K.Rubin and A.Silverberg, *Mod 6 representations of elliptic curves*. Automorphic forms, automorphic representations, and arithmetic (Fort Worth, TX, 1996), 213-

220, Proceedings of Symposia in Pure Mathematics, 66, Part 1, *Amer.Math.Soc.*, Providence, RI, 1999.

[W] A. Weil, *The field of definition of a variety*. Amer. J. Math. 78 (1956), 509524.

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