SINGULAR MODULI AND SINGULAR VALUES OF THE MODULAR LAMBDA FUNCTION

KEVIN WATMOUGH, Department of Mathematics and Statistics

McGill University, Montreal

AUGUST, 2020

A thesis submitted to McGill University in partial fulfillment of the requirements of the degree of

Masters of Mathematics

Contents

Abstract

Singular moduli are values of the form $j(a + b\sqrt{-d})$, where $a, b \in \mathbb{Q}$, $-d$ is a negative fundamental discriminant, and j is the modular j function. These values are exactly the j-invariants of elliptic curves with complex multiplication. In this thesis, I will discuss two famous results about singular moduli, namely Gross and Zagier's factorization formula and Berwick's congruences, and give generalizations of both to singular values of the modular lambda function λ. I will also give an integral model for the modular curve $Y(2)$.

Résumé

Les modules singuliers sont les valeurs de la forme $j(a+b\sqrt{-d})$, où $a, b \in \mathbb{Q}$, $-d$ est un discriminant fondamental et j est le fonction j de Klein. Ces valeurs sont exactement les invariants modulaires j des courbes elliptiques à multiplication complexe. Dans cette thèse, je vais enquêter deux résultats concernant les modules singuliers: la formule de factorisation de Gross et Zagier, et les congruences de Berwick. Je vais aussi généraliser ces résultats aux valeurs singulier du fonction modulaire λ. Finalement, je vais donner un modèle sur $\mathbb{Z}$ pour la courbe modulaire $Y(2)$.

Acknowledgements

I would like to thank my supervisor, Professor Eyal Goren, for his invaluable advice, patience, and for his financial support. I would also like to thank my parents James and Susan for their constant love and support.

Chapter 1

Introduction

The group $\mathrm{SL}_2(\mathbb{Z})$ of 2×2 matrices with integer coefficients and determinant 1 acts on the upper half plane $\mathcal{H} = \{z \in \mathbb{C} : \mathrm{Im}\,(z) > 0\}$ by fractional linear transformation,

$$\gamma(z) = \frac{az+b}{cz+d}, \quad z \in \mathcal{H},\ \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}). \tag{1.1}$$

The *modular curve* $Y(1)$ over $\mathbb{C}$ is the quotient space $\mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H}$. It is the moduli space of isomorphism classes of elliptic curves over $\mathbb{C}$.

Similarly, if Γ is a *congruence subgroup* of $\mathrm{SL}_2(\mathbb{Z})$, i.e. a subgroup containing the principal congruence subgroup

$$\Gamma(n) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : a \equiv d \equiv 1 \mod n,\ b \equiv c \equiv 0 \mod n \right\} \tag{1.2}$$

for some $n \geq 1$, then one defines the modular curve Y_Γ to be the quotient space $\Gamma\backslash\mathcal{H}$. Of particular interest are the modular curves

$$Y(n) := Y_{\Gamma(n)} \quad Y_0(n) := Y_{\Gamma_0(n)}, \quad Y_1(n) := Y_{\Gamma_1(n)},$$

where

$$\Gamma_0(n) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : c \equiv 0 \mod n \right\}, \tag{1.3}$$

and

$$\Gamma_1(n) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : a \equiv d \equiv 1 \mod n, c \equiv 0 \mod n \right\}. \tag{1.4}$$

These are moduli spaces for elliptic curves plus the following "level n structures" pertaining to the n-torsion points $E[n]$ of an elliptic curve E:

1. The modular curve $Y(n)$ parametrizes elliptic curves E equipped with a symplectic isomorphism $\varphi : (\mathbb{Z}/n\mathbb{Z})^2 \to E[n]$,

2. the modular curve $Y_0(n)$ parametrizes elliptic curves E equipped with a cyclic subgroup $C \subseteq E[n]$ of order n, and

3. the modular curve $Y_1(n)$ parametrizes elliptic curves E equipped with a point $P \in E[n]$ of exact order n.

If Y_Γ is a modular curve, its compactification is the space $X_\Gamma := \Gamma\backslash(\mathcal{H} \cup \mathbb{Q} \cup \{\infty\})$. The compactifications of $Y(n)$, $Y_0(n)$ and $Y_1(n)$ are denoted by $X(n)$, $X_0(n)$ and $X_1(n)$.

Modular curves allow us to translate certain invariants of elliptic curves into modular functions, i.e. meromorphic functions $\mathcal{H} \to \mathbb{C}$ which are invariant under the action of some congruence subgroup Γ. The most famous example is Klein's modular j function $j : \mathcal{H} \to \mathbb{C}$, which corresponds to the j-invariant of elliptic curves, an invariant which determines whether two elliptic curves are isomorphic over $\mathbb{C}$. The j function is $\mathrm{SL}_2(\mathbb{Z})$-invariant, and it is a *hauptmodul* for $X(1)$, that is to say it defines an isomorphism $X(1) \cong \mathbb{P}^1$.

Of particular interest are values of the modular j function at imaginary quadratic arguments, i.e. values $j(a+b\sqrt{-d})$, where $a, b \in \mathbb{Q}$ and $-d$ is a negative fundamental discriminant. These values are called *singular moduli*, and they are exactly the j-invariants of elliptic curves with complex multiplication. A classical result is that all singular moduli are algebraic integers. Moreover, it was recently shown by Bilu, Habegger and Kühne [3]

that no singular modulus is an algebraic unit. I will be interested in two famous results about singular moduli, namely Gross and Zagier's factorization formula and Berwick's congruences.

In 1984, Gross and Zagier [17] proved a factorization formula for the product of differences $j(\tau_1) - \ j(\tau_2)$, where τ_i is an imaginary quadratic number of fundamental discriminant d_i (by this, I mean that $\mathbb{Z} + \tau_i\mathbb{Z}$ is a fractional ideal of the unique quadratic order $\mathcal{O}_i$ of discriminant d_i). Their formula is as follows. Write

$$J(d_1, d_2) := \left(\prod_{\substack{\tau_i \in \mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H} \\ \mathrm{disc}\,(\tau_i) = d_i}} (j(\tau_1) - j(\tau_2)) \right)^{\frac{4}{w_1 w_2}}, \tag{1.5}$$

where w_i is the number of units of the order $\mathcal{O}_i$ of discriminant d_i. Also, for l prime, write

$$\varepsilon(l) := \begin{cases} \left(\frac{d_1}{l}\right), & \text{if } \gcd(d_1, l) = 1, \text{ and} \\ \left(\frac{d_2}{l}\right), & \text{if } \gcd(d_1, l) = 1, \end{cases}$$

where $\left(\frac{d_i}{l}\right)$ is the Kronecker symbol, and extend ε multiplicatively to all positive integers. I will discuss the Kronecker symbol and the function ε extensively in § 3.1. With this notation, Gross and Zagier proved the following theorem.

Theorem 1.6. [17, Theorem 1.3] *If d_1, d_2 are coprime fundamental discriminants, then*

$$J(d_1, d_2)^2 = \pm \prod_{\substack{x,n,n' \in \mathbb{Z} \\ n,n' > 0 \\ x^2 + 4nn' = d_1 d_2}} n^{\varepsilon(n')}.$$

Another result of great interest to the study of singular moduli are Berwick's congruences. In 1928, Berwick [1] conjectured that if j is a singular modulus, then j and $j - 1728$ should satisfy several congruences above certain primes p. Gross and Zagier proved several of these congruences in their above paper [17], but a more general proof would have to wait until 2004, when Berwick's congruences were proven by Bettner [2].

One can consider analogues of singular moduli for other hauptmoduls. If μ is a

hauptmodul for a modular curve X_Γ, namely if μ provides an isomorphism $X_\Gamma \cong \mathbb{P}^1$, then we call the values of μ at imaginary quadratic arguments "singular values" of μ, or "singular μ-values". A natural question to ask is whether results pertaining to singular moduli, such as Gross and Zagier's factorization formula and Berwick's congruences, can be generalized to other hauptmoduls. In the case of Gross and Zagier's formula, this question has recently been answered positively for the following hauptmoduls:

1. Define $x(z) = 2^{12}\frac{\Delta(2z)}{\Delta(z)}$ for $z \in \mathcal{H}$, where Δ is the modular discriminant function. This is a hauptmodul for the modular curve $X_0(2)$. A Gross-Zagier-like factorization formula for x was proven by Yang and Yin [30].

2. Let λ be the modular lambda function, which is a hauptmodul for $X(2)$. It corresponds to the λ-invariant of enhanced elliptic curves for $\Gamma(n)$, defined as follows. Any elliptic curve E over $\mathbb{C}$ has a Weierstrass equation of the form

$$E : y^2 = x(x-1)(x-\lambda).$$

   The choice of λ is not unique (there are six choices of λ if $j(E) \neq 0, 1728$), and each choice of λ corresponds to a symplectic isomorphism $\varphi : (\mathbb{Z}/2\mathbb{Z})^2 \to E[2]$. The number $\lambda \in \mathbb{C}$ corresponding to a given symplectic isomorphism φ is called the λ-*invariant* of the enhanced elliptic curve (E, φ). A Gross-Zagier-like factorization formula for the modular lambda function was proven by Yang, Yin and Yu in [31].

The main focus of this thesis will be finding analogues of Gross and Zagier's formulas and of Berwick's congruences for the modular lambda function. In chapter 2, I will give some necessary background material regarding the modular lambda function λ and modular curves over $\mathbb{C}$. In chapter 3, I will discuss Gross and Zagier's algebraic proof of Theorem 1.6, adding many details which were absent in their paper. In chapter 4, I will prove two results which are consequences of Theorem 1.6. First, in § 4.1, I will give an upper bound on the valuation $v(j)$ of a singular modulus j, where v is a valuation lying above the prime 2. I will provide two proofs of this bound, the first relying on several lemmas of Gross and Zagier [17] and the second using volume estimates for subrings of

a certain quaternion algebra. Both proofs will use a result from [17] which relates the valuation of $j(E)-j(E')$, where E and E' are elliptic curves with complex multiplication, to the number of isomorphisms from E to E'. Second, in § 4.2, I will prove a Gross-Zagier-like formula for the modular lambda function. My formula is weaker than Yang, Yin and Yu's formula, but it is surprisingly simple, and relatively easy to prove. In chapter 5, I will prove an analogue of Berwick's congruences for the modular lambda function, by applying the theory of Newton polygons to Bettner's result. A similar formula for norms of singular lambda values is given in [31].

Finally, one can generalize the idea of modular curves over $\mathbb{C}$ to obtain moduli spaces for elliptic curves over any ring. To do this, one defines more general notions of "level n structures" on elliptic curves, which make sense even when n is not invertible. If $n \geq 3$, then the moduli problems corresponding to these level n structures are representable by some schemes $\mathcal{Y}(n)$, $\mathcal{Y}_0(n)$ and $\mathcal{Y}_1(n)$. We call these schemes *fine moduli schemes* for their corresponding moduli problems. If $n = 1$ or 2, then the moduli problems corresponding to the different level n structures are not representable, so the schemes $\mathcal{Y}(2)$, $\mathcal{Y}_0(2)$ and $\mathcal{Y}_1(2)$ do not exist as fine moduli spaces. Instead, we define "coarse moduli spaces" $\mathcal{Y}(2)$, $\mathcal{Y}_0(2)$ and $\mathcal{Y}_1(2)$, which are the best possible approximation of a fine moduli space for the level n moduli problems.

The modular schemes $\mathcal{Y}(n)$, $\mathcal{Y}_0(n)$ and $\mathcal{Y}_1(n)$ exist as schemes over $\mathbb{Z}$, which motivates the search for integral models for these schemes, i.e. for systems of polynomials which define them as schemes over $\mathbb{Z}$. In 6, I will define such a model for the modular scheme $\mathcal{Y}(2)$. I will do this by constructing a morphism of schemes

$$\mathcal{Y}(2) \to \mathcal{Y}_0(2) \underset{\mathcal{Y}_0(1)}{\times} \mathcal{Y}_0(2),$$

and making use of the integral model $\operatorname{Spec} \mathbb{Z}[x,j]/(\psi_2(x,j))$ for $\mathcal{Y}_0(2)$ given by Mestre [23], where

$$\psi_2(x,j) := (x+16)^3 - xj = 0 \tag{1.7}$$

is the canonical modular polynomial of level 2.

Chapter 2

Modular curves and the modular lambda function

2.1 The cross-ratio and the modular lambda function

Let K be a field not of characteristic 2, and let E be an elliptic curve over K. Then E is given by a Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{2.1.1}$$

over R. Since 2 is invertible, we can make the change of variables

$$y' = \frac{1}{2}(2y + a_1x + a_3),$$

which puts E in the form

$$(y')^2 = x^3 + a_2'x^2 + a_4'x + a_6'. \tag{2.1.2}$$

Over the algebraic closure $\overline{K}$ of K, we factor the right-hand side of Equation (2.1.2) to write E in the form

$$(y')^2 = (x - e_1)(x - e_2)(x - e_3).$$

Now, a straightforward calculation shows that there is a unique projective transformation sending e_1 to 1, e_2 to 0 and fixing ∞. It sends $x \in \mathbb{P}^1$ to the *cross-ratio*[1]

$$(e_2, e_1; x, \infty) := \frac{x - e_2}{e_1 - e_2}$$

of the points e_2, e_1, x and ∞. Let λ be the image of e_3 under this transformation, so

$$\lambda := \frac{e_3 - e_2}{e_1 - e_2}. \tag{2.1.3}$$

Note that $\lambda \neq 0, 1$ since $e_3 \neq e_1, e_2$. So the curve

$$E_\lambda : y^2 = x(x-1)(x-\lambda) \tag{2.1.4}$$

is an elliptic curve over the field $K(e_1, e_2, e_3)$. Also, E is isomorphic to E_λ over $\overline{K}$ via the map

$$(x, y) \mapsto \left(\frac{x - e_2}{e_1 - e_2}, \frac{y}{(e_1 - e_2)^{3/2}} \right). \tag{2.1.5}$$

This map takes $(e_1, 0)$ to $(1, 0)$, $(e_2, 0)$ to $(0, 0)$ and $(e_3, 0)$ to $(\lambda, 0)$.

Moreover, there is a unique value of λ for which such a map exist. Indeed, take $\lambda' \in \overline{K}$ and suppose that E is isomorphic to $E_{\lambda'}$ via an isomorphism taking $(e_1, 0)$ to $(1, 0)$, $(e_2, 0)$ to $(0, 0)$ and $(e_3, 0)$ to $(\lambda', 0)$. Then the x-coordinate of this isomorphism gives a projective transformation taking the ordered tuple (e_2, e_1, e_3, ∞) to $(0, 1, \lambda', \infty)$. Hence both tuples have the same cross ratio, i.e.

$$\lambda' = \frac{\lambda' - 0}{1 - 0} = (0, 1 : \lambda', \infty) = (e_2, e_1 : e_3, \infty) = \frac{e_3 - e_2}{e_1 - e_2} = \lambda,$$

[1]The cross-ratio of four distinct points $z_1, z_2, z_3, z_4 \in \mathbb{A}^1$ is defined to be

$$(z_1, z_2; z_3, z_4) := \frac{(z_3 - z_1)(z_4 - z_2)}{(z_3 - z_2)(z_4 - z_1)}.$$

This can be extended to $\mathbb{P}^1$ by removing the terms containing z_i if $z_i = \infty$. For example, when $z_4 = \infty$, we have

$$(z_1, z_2; z_3, \infty) := \frac{z_3 - z_1}{z_3 - z_2}.$$

Over $\mathbb{R}$, this is the same as taking the limit as $z_4 \to \infty$.

Two ordered sets of points (z_1, z_2, z_3, z_4) and (z_1', z_2', z_3', z_4') have the same cross-ratio if and only if there is a projective transformation taking each z_i to z_i'.

$\sigma \in S_3$	$(e_1', e_2', e_3') = (e_1, e_2, e_3)^\sigma$	$\lambda' = \lambda^\sigma = \frac{e_3'-e_2'}{e_1'-e_2'}$
id	(e_1, e_2, e_3)	λ
(23)	(e_1, e_3, e_2)	$\frac{\lambda}{\lambda-1}$
(12)	(e_2, e_1, e_3)	$1-\lambda$
(123)	(e_2, e_3, e_1)	$\frac{\lambda-1}{\lambda}$
(132)	(e_3, e_1, e_2)	$\frac{1}{1-\lambda}$
(13)	(e_3, e_2, e_1)	$\frac{1}{\lambda}$

Table 2.1: The six values of λ and the action of S_3 on them.

as claimed.

However, note that λ is not an invariant of the elliptic curve E, since it depends on the ordering e_1, e_2, e_3 of the points of exact order 2 of E. Hence for a given elliptic curve, there are six possible values of λ. The symmetric group S_3 acts on these values by permuting the 2-torsion points $(e_1, 0), (e_2, 0)$ and $(e_3, 0)$ of E. The values of λ and the action of S_3 are given in Table 2.1.

Instead, λ is an invariant for *enhanced elliptic curves for* $\Gamma(2)$, i.e. triples (E, P_1, P_2), where E is an elliptic curve over K and P_1, P_2 is an ordered basis for the 2-torsion $E[2]$ of E. The λ-invariant of an enhanced elliptic curve (E, P_1, P_2) is the unique value $\lambda \in \overline{L}$ such that (E, P_1, P_2) is isomorphic over K to the elliptic curve E_λ via an isomorphism taking P_1 to $(1, 0)$ and P_2 to $(0, 0)$.

In § 2.3, we will see how this construction gives a $\Gamma(2)$-invariant function on the upper half plane. But first, we note that one can obtain a true invariant of the elliptic curve E by taking a symmetric polynomial of the values of λ from Table 2.1. The naive choices would be to add or multiply these values,

$$S_{add}(\lambda) = \sum_{\sigma \in S_3} \lambda^\sigma, \quad S_{mult}(\lambda) = \prod_{\sigma \in S_3} \lambda^\sigma,$$

however a quick calculation shows that $S_{add}(\lambda) = 3$ and $S_{mult}(\lambda) = 1$ regardless of the value of λ. Instead, we take the sum of the squares,

$$S(\lambda) = \sum_{\sigma \in S_3} (\lambda^\sigma)^2 = \frac{2 - 6\lambda + 9\lambda^2 - 8\lambda^3 + 9\lambda^4 - 6\lambda^5 + 2\lambda^6}{\lambda^2(1-\lambda)^2}. \tag{2.1.6}$$

This is related to the classical j-invariant $j = j(E)$ by

$$j = 128(S(\lambda) + 3) = 256\frac{(1 - \lambda + \lambda^2)^3}{\lambda^2(1 - \lambda)^2}. \tag{2.1.7}$$

Remark 2.1.8. Let

$$E : y^2 = (x - e_1)(x - e_2)(x - e_3)$$

and

$$E' : y^2 = (x - e_1')(x - e_2')(x - e_3')$$

be two elliptic curves over K whose two-torsion points $(e_i, 0)$ and $(e_i', 0)$ are defined over K. Suppose that $(E, (e_1, 0), (e_2, 0))$ and $(E', (e_1', 0), (e_2', 0))$ have the same λ-invariant λ_0. Then, as a consequence of the above discussion, there is an isomorphism $f : E \to E'$ over $\overline{K}$ taking $(e_i, 0)$ to $(e_i', 0)$. This isomorphism must be of the form

$$(x, y) \mapsto (u^2 x + r, u^3 y)$$

with $u \in \overline{K}^\times$ and $r \in \overline{K}$. The conditions $e_i' = u^2 e_i + r,\ i = 1, 2, 3$, give

$$u^2 = \frac{e_1' - e_2'}{e_1 - e_2}, \quad r = \frac{e_1 e_2' - e_1' e_2}{e_1 - e_2},$$

so f is given by

$$(x, y) \mapsto \left(\left(\frac{e_1' - e_2'}{e_1 - e_2} \right) x + \frac{e_1 e_2' - e_1' e_2}{e_1 - e_2}, \left(\frac{e_1' - e_2'}{e_1 - e_2} \right)^{3/2} y \right). \tag{2.1.9}$$

So E and E' are in fact isomorphic over the quadratic extension $K[\sqrt{(e_1' - e_2')/(e_1 - e_2)}]$ of K.

2.2 Congruence subgroups and modular curves over $\mathbb{C}$

In this section, I will define the modular curves $Y(n)$, $Y_0(n)$ and $Y_1(n)$ as complex manifolds, and explain their connection to "enhanced" elliptic curves.

Fix $n \geq 1$. The *principal congruence subgroup of level* n is the subgroup

$$\Gamma(n) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : a \equiv d \equiv 1 \mod n,\ b \equiv c \equiv 0 \mod n \right\}. \tag{2.2.1}$$

of $\mathrm{SL}_2(\mathbb{Z})$. It is the kernel of the surjective homomorphism

$$\mathrm{SL}_2(\mathbb{Z}) \longrightarrow \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$$

$$\gamma \longmapsto \gamma \mod n,$$

and so is a normal subgroup.

A subgroup $\Gamma < \mathrm{SL}_2(\mathbb{Z})$ is called a *congruence subgroup of level* n if it contains $\Gamma(n)$. Two congruence subgroups of particular interest are

$$\Gamma_0(n) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : c \equiv 0 \mod n \right\} \tag{2.2.2}$$

and

$$\Gamma_1(n) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : a \equiv d \equiv 1 \mod n, c \equiv 0 \mod n \right\}. \tag{2.2.3}$$

Note that

$$\Gamma(n) \subseteq \Gamma_1(n) \subseteq \Gamma_0(n).$$

Now, recall that $\mathrm{SL}_2(\mathbb{Z})$ acts on the upper-half plane $\mathcal{H} = \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$ by linear fractional transformation,

$$\gamma(z) = \frac{az+b}{cz+d} \quad \text{for } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \text{ and } z \in \mathcal{H}. \tag{2.2.4}$$

So if $\Gamma < \mathrm{SL}_2(\mathbb{Z})$ is a congruence subgroup, we can form the quotient space $Y_\Gamma := \Gamma \backslash \mathcal{H}$.

In particular, for $n \geq 1$ we write

$$Y(n) := Y_{\Gamma(n)}, \quad Y_1(n) := Y_{\Gamma_1(n)}, \quad Y_0(n) := Y_{\Gamma_0(n)}. \tag{2.2.5}$$

These spaces are in fact moduli spaces for certain "enhanced" elliptic curves over $\mathbb{C}$. Let us define these enhanced elliptic curves.

Let E be an elliptic curve over $\mathbb{C}$, and fix $n \geq 1$.

A $\Gamma_1(n)$-*structure* on E is a point $P \in E[n]$ of exact order n. We call the pair (E, P) an *enhanced elliptic curve for* $\Gamma_1(n)$. An *isomorphism* $f : (E, P) \to (E', P')$ of enhanced elliptic curves for $\Gamma_1(n)$ is an isomorphism $f : E \to E'$ of elliptic curves such that $f(P) = P'$.

A $\Gamma_0(n)$-*structure* on E is a subgroup $H < E[n]$ of order p. We call the pair (E, H) an *enhanced elliptic curve for* $\Gamma_0(n)$. An isomorphism $f : (E, H) \to (E', H')$ of enhanced elliptic curves for $\Gamma_0(n)$ is an isomorphism of elliptic curves $f : E \to E'$ such that $f(H) = H'$.

To define enhanced elliptic curves for $\Gamma(n)$, we must we must first define the Weil pairing

$$e_n : E[n] \times E[n] \to \mu_n$$

for an elliptic curve E over $\mathbb{C}$, where μ_n is the multiplicative group of n-th roots of unity. To do this, write $E = \mathbb{C}/\Lambda$ for some lattice $\Lambda = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$, with $\omega_1/\omega_2 \in \mathcal{H}$. Then, since $\omega_1/n, \omega_2/n$ form a basis for $E[n]$, we can write

$$\begin{pmatrix} P \\ Q \end{pmatrix} = \gamma \begin{pmatrix} \omega_1/n \\ \omega_2/n \end{pmatrix}$$

for some matrix $\gamma \in M_2(\mathbb{Z}/n\mathbb{Z})$. We then define the *Weil pairing* of P and Q to be

$$e_n(P, Q) := \zeta_n^{\det \gamma},$$

where $\zeta_n = e^{2\pi i/n}$. Since $\zeta_n^n = 1$, $e_n(P,Q)$ is well-defined. One can check that the Weil pairing is bilinear. Similarly, we can define a bilinear pairing

$$d_n : (\mathbb{Z}/n\mathbb{Z})^2 \to \mu_n$$

by

$$d_n((a,b),(c,d)) := \zeta_n^{ad-bc}.$$

Now, a $\Gamma(n)$-*structure* on E is a symplectic isomorphism $\varphi : ((\mathbb{Z}/n\mathbb{Z})^2, d_n) \to (E[n], e_n)$, i.e. an isomorphism $\varphi : (\mathbb{Z}/n\mathbb{Z})^2 \to E[n]$ such that $d_n = e_n \circ \varphi$. An *enhanced elliptic curve for* $\Gamma(n)$ is a pair (E,φ), where E is an elliptic curve over $\mathbb{C}$ and φ is a $\Gamma(n)$-structure on E. An *isomorphism* $f : (E,\varphi) \to (E',\varphi')$ of enhanced elliptic curves for $\Gamma(n)$ is an isomorphism of elliptic curves $f : E \to E'$ such that $f \circ \varphi = \varphi'$.

Proposition 2.2.6. *Fix $n \geq 1$. Then we have well-defined bijections*

1. *between $Y(n)$ and the set of isomorphism classes of enhanced elliptic curves for $\Gamma(n)$, sending $\Gamma(n)\tau$ to the isomorphism class $\left[\mathbb{C}/(\mathbb{Z}+\tau\mathbb{Z}), \frac{1}{n}, \frac{\tau}{n}\right]$,*

2. *between $Y_1(n)$ and the set of isomorphism classes of enhanced elliptic curves for $\Gamma_1(n)$, sending $\Gamma_1(n)\tau$ to the isomorphism class $\left[\mathbb{C}/(\mathbb{Z}+\tau\mathbb{Z}), \frac{1}{n}\right]$, and*

3. *between $Y_0(n)$ and the set of isomorphism classes of enhanced elliptic curves for $\Gamma_0(n)$, sending $\Gamma_0(n)\tau$ to the isomorphism class $\left[\mathbb{C}/(\mathbb{Z}+\tau\mathbb{Z}), \left\langle \frac{1}{n} \right\rangle\right]$.*

Proof. This is [12, Theorem 1.5.1] □

2.3 Lambda as a modular function

In this section, we will see how the lambda invariant constructed in § 2.1 gives rise to a $\Gamma(2)$-invariant function $\lambda : \mathcal{H} \to \mathbb{C}$. This function is called the *modular lambda function.*

Let $\tau \in \Gamma(2)\backslash\mathcal{H}$. In Proposition 2.2.6, we saw that τ corresponds to the isomorphism class $\left[\mathbb{C}/(\mathbb{Z}+\tau\mathbb{Z}), \frac{1}{2}, \frac{\tau}{2}\right]$ of enhanced elliptic curves for $\Gamma(2)$. A Weierstrass equation for

the elliptic curve E is given by

$$y^2 = 4(x - e_1)(x - e_2)(x - e_3), \tag{2.3.1}$$

where

$$e_1 = \wp\left(\frac{1}{2}\right), \quad e_2 = \wp\left(\frac{\tau}{2}\right), \quad e_3 = \wp\left(\frac{\tau+1}{2}\right),$$

and $\wp$ is the Weierstrass $\wp$-function for the lattice $\mathbb{Z} + \tau\mathbb{Z}$ (see [12, §1.4]). The elliptic curve in Equation (2.3.1) is isomorphic via the map $y \mapsto y/2$ to the elliptic curve

$$E : y^2 = (x - e_1)(x - e_2)(x - e_3).$$

Hence the enhanced elliptic curve $\left(\mathbb{C}/(\mathbb{Z} + \tau\mathbb{Z}), \frac{1}{2}, \frac{\tau}{2}\right) \cong (E, (e_1, 0), (e_2, 0))$ has λ-invariant

$$\lambda(\tau) := \lambda\left(\mathbb{C}/(\mathbb{Z} + \tau\mathbb{Z}), \frac{1}{2}, \frac{\tau}{2}\right) = \frac{e_3 - e_2}{e_1 - e_2} = \frac{\wp\left(\frac{\tau+1}{2}\right) - \wp\left(\frac{\tau}{2}\right)}{\wp\left(\frac{1}{2}\right) - \wp\left(\frac{\tau}{2}\right)}. \tag{2.3.2}$$

This is a meromorphic function on $\mathcal{H}$ since $\wp$ is, and it is $\Gamma(2)$-invariant, since if $\tau, \tau' \in \mathcal{H}$ are in the same $\Gamma(2)$-orbit, then the enhanced elliptic curves $\left(\mathbb{C}/(\mathbb{Z} + \tau\mathbb{Z}), \frac{1}{2}, \frac{\tau}{2}\right)$ and $\left(\mathbb{C}/(\mathbb{Z} + \tau'\mathbb{Z}), \frac{1}{2}, \frac{\tau'}{2}\right)$ are isomorphic (by Proposition 2.2.6).

Now, we would like to write down the q-expansion of λ. To do this, we use the fact (see [7, Chapter V, §5, Corollary 1]) that

$$\wp\left(\frac{1}{2}\right) - \wp\left(\frac{\tau}{2}\right) = \pi^2\theta_3(0,\tau)^4, \quad \wp\left(\frac{\tau+1}{2}\right) - \wp\left(\frac{\tau}{2}\right) = \pi^2\theta_1(0,\tau)^4, \tag{2.3.3}$$

where $\theta_1(s,\tau)$ and $\theta_3(s,\tau)$ are the theta-functions

$$\theta_1(s,\tau) = 2\sum_{n\geq 0} q^{\frac{1}{4}(2n+1)^2}\cos\left((2n+1)\pi s\right) \tag{2.3.4}$$

and

$$\theta_3(s,\tau) = 1 + 2\sum_{n\geq 1} q^{n^2}\cos(2n\pi s). \tag{2.3.5}$$

Here, $q = e^{\pi i \tau}$ for $\tau \in \mathcal{H}$. So

$$\lambda(\tau) = \left(\frac{\theta_1(0,\tau)}{\theta_3(0,\tau)}\right)^4. \tag{2.3.6}$$

Moreover, by [5, Corollary 3.1],

$$\theta_1(0,\tau) = 2q^{1/4}\prod_{n\geq 1}(1-q^{2n})(1+q^{2n})^2, \quad \theta_3(0,\tau) = \prod_{n\geq 1}(1-q^{2n})(1+q^{2n-1})^2, \tag{2.3.7}$$

and so

$$\lambda(\tau) = 16q\prod_{n\geq 1}\left(\frac{1+q^{2n}}{1+q^{2n-1}}\right)^8. \tag{2.3.8}$$

This gives the q-expansion

$$\lambda(\tau) = 16q - 128q^2 + 704q^3 - 3072q^4 + O(q^5), \quad q = e^{\pi i\tau}. \tag{2.3.9}$$

The coefficients of this q-expansion are given in OEIS sequence A115977 (see [18]).

Finally, note that this is only one of several possible definitions of the modular lambda function. Indeed, our definition of $\lambda(\tau)$ depends on the choice of correspondence between points of $Y(2)$ and enhanced elliptic curves for $\Gamma(2)$ made in Proposition 2.2.6. In general, if we send $\Gamma(2)\tau \in Y(2)$ to the enhanced elliptic curve $(\mathbb{C}/(\mathbb{Z}+\tau\mathbb{Z}), P_1(\tau), P_2(\tau))$, where $B = (P_1(\tau), P_2(\tau))$ is a choice of basis for the 2-torsion points $\left\{0, \frac{1}{2}, \frac{\tau}{2}, \frac{\tau+1}{2}\right\}$ of $\mathbb{C}/(\mathbb{Z}+\tau\mathbb{Z})$, then the above construction would yield a modular function

$$\lambda_B(\tau) = \frac{\wp(P_1(\tau)+P_2(\tau)) - \wp(P_2(\tau))}{\wp(P_1(\tau)) - \wp(P_2(\tau))}.$$

We can calculate the q-expansion of λ_B using Equation (2.3.3) and Equation (2.3.7), as well as the relations

$$\wp\left(\frac{1}{2}\right) - \wp\left(\frac{\tau+1}{2}\right) = \pi^2\theta_2(0,\tau)^4,$$

where

$$\theta 2(s,\tau) = 1 + 2\sum_{n\geq 1}(-1)^n q^{n^2}\cos(2n\pi s), \tag{2.3.10}$$

$\sigma_B \in S_3$	$B = (P_1(\tau), P_2(\tau))$	τ_B	$\lambda_B(\lambda)$	$\lambda_B(\tau)$	$\lambda_B(q)$
id	$\left(\frac{1}{2}, \frac{\tau}{2}\right)$	τ	λ	$\left(\frac{\theta_1(0,\tau)}{\theta_3(0,\tau)}\right)^4$	$16q\prod_{n\geq 1}\left(\frac{1+q^{2n}}{1+q^{2n-1}}\right)^8$
(23)	$\left(\frac{1}{2}, \frac{\tau+1}{2}\right)$	$\tau+1$	$\frac{\lambda}{\lambda-1}$	$-\left(\frac{\theta_1(0,\tau)}{\theta_2(0,\tau)}\right)^4$	$-16q\prod_{n\geq 1}\left(\frac{1+q^{2n}}{1-q^{2n-1}}\right)^8$
(12)	$\left(\frac{\tau}{2}, \frac{1}{2}\right)$	$\frac{-1}{\tau}$	$1-\lambda$	$\left(\frac{\theta_2(0,\tau)}{\theta_3(0,\tau)}\right)^4$	$\prod_{n\geq 1}\left(\frac{1-q^{2n-1}}{1+q^{2n-1}}\right)^8$
(123)	$\left(\frac{\tau}{2}, \frac{\tau+1}{2}\right)$	$\frac{\tau-1}{\tau}$	$\frac{\lambda-1}{\lambda}$	$-\left(\frac{\theta_2(0,\tau)}{\theta_1(0,\tau)}\right)^4$	$-\frac{1}{16q}\prod_{n\geq 1}\left(\frac{1-q^{2n-1}}{1+q^{2n}}\right)^8$
(132)	$\left(\frac{\tau+1}{2}, \frac{1}{2}\right)$	$\frac{1}{1-\tau}$	$\frac{1}{1-\lambda}$	$\left(\frac{\theta_3(0,\tau)}{\theta_2(0,\tau)}\right)^4$	$\prod_{n\geq 1}\left(\frac{1+q^{2n-1}}{1-q^{2n-1}}\right)^8$
(13)	$\left(\frac{\tau+1}{2}, \frac{\tau}{2}\right)$	$\frac{\tau}{\tau+1}$	$\frac{1}{\lambda}$	$\left(\frac{\theta_3(0,\tau)}{\theta_1(0,\tau)}\right)^4$	$\frac{1}{16q}\prod_{n\geq 1}\left(\frac{1+q^{2n-1}}{1+q^{2n}}\right)^8$

Table 2.2: The six possible definitions $\lambda_B(\tau)$ of the modular lambda function, corresponding to the six bases B of $E_\tau[2]$. The first column shows how $S_3 \cong \Gamma(2)\backslash \mathrm{SL}_2(\mathbb{Z})$ acts on these functions, by specifying the element $\sigma_B \in S_3$ taking the basis $\left(\frac{1}{2}, \frac{\tau}{2}\right)$ to B. The third column gives the element $\tau_B \in Y(2)$ such that $\lambda_B(\tau) = \lambda(\tau_B)$, i.e. the element such that the enhanced elliptic curve (E_τ, B) is isomorphic to $\left(E_{\tau_B}, \frac{1}{2}, \frac{\tau_B}{2}\right)$. The fourth column gives λ_B as a function of λ. The fifth column gives λ_B in terms of the theta functions $\theta_i(0,\tau), i = 1,2,3$. Finally, the last column gives the q-expansion of λ_B.

which satisfies

$$\theta_2(0,\tau) = \prod_{n\geq 1}(1-q^{2n})(1-q^{2n-1})^2 \tag{2.3.11}$$

(again, these come from [7, Chapter V, §5, Corollary 1] and [5, Corollary 3.1]). The results of these calculations are given in Table 2.2.

In particular, note that one of the choices of λ_B is $\frac{1}{\lambda(\tau)}$. So, unlike the modular j-function, which has a zero at $\tau = \frac{-1+\sqrt{-3}}{2}$, λ has no zeros or poles on $\mathcal{H}$. Modular functions with this property are called *modular units*.

Chapter 3

Gross-Zagier's factorization formula

3.1 Introduction

Singular moduli, that is complex numbers of the form $j(a+b\sqrt{-d})$, where $a, b \in \mathbb{Q}$ and d is a positive integer, have been studied as far back as the works of Klein, Hilbert and Weber. They are exactly the j-invariants of elliptic curves over $\mathbb{C}$ with complex multiplication, i.e. elliptic curves whose endomorphism rings are orders in quadratic imaginary fields. In 1984, Gross and Zagier discovered a remarkable factorization formula for norms of differences of singular moduli (see Theorem 3.1.5 below). In [17], they provide two proofs of this formula. In this chapter, I will discuss their first (algebraic) proof, adding some details which were not present in the cited paper.

3.1.1 The Kronecker symbol

Recall that if p is an odd prime and $a \in \mathbb{Z}$, the *Legendre symbol* $\left(\frac{a}{p}\right)$ is given by

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{if } a \text{ is a square mod } p \text{ and } a \not\equiv 0 \mod p, \\ -1, & \text{if } a \text{ is not a square mod } p, \\ 0, & \text{if } a \equiv 0 \mod p. \end{cases} \tag{3.1.1}$$

The Legendre symbol is multiplicative in its top argument, i.e.

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

Also, if p and q are distinct odd primes, then the law of quadratic reciprocity states that

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

The Kronecker symbol generalizes the Legendre symbol to any pair of non-zero integers. It uses the same notation as the Legendre symbol, and is defined as follows:

1. If p is an odd prime then $\left(\frac{m}{p}\right)$ is just the Legendre symbol, as defined above.
2. $\left(\frac{m}{2}\right) = \begin{cases} 0, & \text{if } 2|m, \\ 1, & \text{if } a \equiv \pm 1 \mod 8, \\ -1, & \text{if } a \equiv \pm 3 \mod 8. \end{cases}$
3. $\left(\frac{m}{1}\right) = 1$.
4. $\left(\frac{m}{-1}\right) = \begin{cases} 1, & \text{if } m \geq 0, \\ -1, & \text{if } m < 0. \end{cases}$
5. If $n = up_1^{a_1} \cdots p_r^{a_r}$, where $p_1, \ldots, p_r$ are distinct primes and $u = \pm 1$, then

$$\left(\frac{m}{n}\right) = \left(\frac{m}{u}\right)\left(\frac{m}{p_1}\right)^{a_1} \cdots \left(\frac{m}{p_r}\right)^{a_r}.$$

Lemma 3.1.2. *The Kronecker symbol has the following properties:*

1. $\left(\frac{mm'}{n}\right) = \left(\frac{m}{n}\right)\left(\frac{m'}{n}\right)$ *and* $\left(\frac{m}{nn'}\right) = \left(\frac{m}{n}\right)\left(\frac{m}{n'}\right)$, *for all* $m, m', n, n' \in \mathbb{Z}$ *with* $n, n' \neq 0$.
2. *(Quadratic reciprocity, limited version) If* $m \equiv 1 \mod 4$, $n \equiv 0$ *or* $1 \mod 4$ *and* m, n *are relatively prime, then*

$$\left(\frac{m}{n}\right) = \left(\frac{n}{|m|}\right).$$

If in addition to these properties we have $\operatorname{sgn}(m) = -\operatorname{sgn}(n)$*, then*

$$\left(\frac{m}{n}\right) = \left(\frac{n}{m}\right).$$

3. $\left(\frac{m}{n}\right)$ *depends only on* $n \mod m$*.*

Proof. Property (1) follows immediately from the multiplicativity of the Legendre symbol. For properties (2) and (3), see [9, Exercise 13.15(a)-(b)]. □

For more on the Kronecker symbol, see [9].

3.1.2 Gross-Zagier's main theorem

Let $d_1, d_2 < 0$ be two negative fundamental discriminants with $\gcd(d_1, d_2) = 1$, and let $D = d_1 d_2 > 0$. For $i = 1, 2$ let $\mathcal{O}_i$ be the imaginary quadratic order of discriminant d_i, let $w_i = \mathcal{O}_i^\times$ be the number of units in $\mathcal{O}_i$, and let $h_i = h(\mathcal{O}_i)$ be the class number of $\mathcal{O}_i$. We say that an imaginary quadratic number $\tau_i \in \mathcal{H}$ has discriminant d_i, and write $\operatorname{disc}(\tau_i) = d_i$, if $\mathbb{Z} + \tau_i\mathbb{Z}$ is a fractional ideal of $\mathcal{O}_i$. The singular moduli $j(\tau_i)$ with $\operatorname{disc}(\tau_i) = d_i$ are exactly the j-invariants of the elliptic curves over $\mathbb{C}$ with complex multiplication by $\mathcal{O}_i$. In [17], Gross and Zagier consider the following product:

$$J(d_1, d_2) := \left(\prod_{\substack{\tau_i \in \Gamma\backslash\mathcal{H} \\ \operatorname{disc}(\tau_i) = d_i}} (j(\tau_1) - j(\tau_2)) \right)^{\frac{4}{w_1 w_2}} \tag{3.1.3}$$

Their main result is a formula for $J(d_1, d_2)$, given in Theorem 3.1.5 below.

If l is prime and $\left(\frac{D}{l}\right) \neq -1$, define

$$\varepsilon(l) = \begin{cases} \left(\frac{d_1}{l}\right) \text{ if } \gcd(l, d_1) = 1 \\ \left(\frac{d_2}{l}\right) \text{ if } \gcd(l, d_2) = 1, \end{cases} \tag{3.1.4}$$

where $\left(\frac{d_i}{l}\right)$ is the Kronecker symbol. Note that since $\gcd(d_1, d_2) = 1$, we must have either $\gcd(l, d_1) = 1$ or $\gcd(l, d_2) = 1$. Also, if $\gcd(l, d_1) = \gcd(l, d_2) = 1$, then $1 = \left(\frac{D}{l}\right) =$

$\left(\frac{d_1}{l}\right)\left(\frac{d_2}{l}\right)$ and so $\left(\frac{d_1}{l}\right) = \left(\frac{d_2}{l}\right)$. So $\varepsilon(l)$ is well-defined. We extend ε multiplicatively: if $n = l_1^{a_1} \cdots l_r^{a_r}$, where each l_i satisfies $\left(\frac{D}{l_i}\right) \neq -1$, then

$$\varepsilon(n) = \varepsilon(l_1)^{a_1} \cdots \varepsilon(l_r)^{a_r}.$$

The main interest of this chapter is the following theorem of Gross-Zagier:

Theorem 3.1.5. *Let d_1, d_2 be as above. Then*

$$J(d_1, d_2)^2 = \pm \prod_{\substack{x,n,n' \in \mathbb{Z} \\ n,n'>0 \\ x^2+4nn'=D}} n^{\varepsilon(n')}.$$

This is [17, Theorem 1.3]. As stated earlier, in this chapter I will discuss their algebraic proof of this result, adding many details which were omitted in their paper.

If m is a positive integer and every prime factor l of m satisfies $\left(\frac{D}{l}\right) \neq -1$, we can define

$$F(m) := \prod_{nn'=m} n^{\varepsilon(n')},$$

where the product runs over positive integers. Note that the definition of F depends on d_1 and d_2 through ε. We can rewrite the formula of Theorem 3.1.5 as

$$J(d_1, d_2)^2 = \pm \prod_{\substack{x^2<D \\ x^2 \equiv D \mod 4}} F\left(\frac{D-x^2}{4}\right).$$

Proposition 3.1.6. *Fix d_1 and d_2 as above. The function F has the following properties:*

1. *If there is a unique prime number l with $\varepsilon(l) = -1$ and dividing m to an odd power, then $F(m)$ is a power of l. Furthermore, if*

$$m = l^{2a+1} p_1^{2a_1} \cdots p_s^{2a_s} q_1^{b_1} \cdots q_t^{b_t}$$

with $\varepsilon(l) = \varepsilon(p_1) = \ldots = \varepsilon(p_s) = -1$ and $\varepsilon(q_1) = \ldots = \varepsilon(q_t) = 1$, then

$$F(m) = l^{(a+1)(b_1+1)\cdots(b_t+1)}.$$

2. *If there are at least two distinct primes l_1, l_2 with $\varepsilon(l_i) = -1$ and dividing m to an odd power, then $F(m) = 1$.*

3. *If there are no such primes, then $F(m)$ is a power of $\sqrt{m}$.*

Proof. Write $m = l_1^{e_1} \cdots l_r^{e_r}$. Then

$$\begin{aligned}
F(m) &= \prod_{nn'=m} n^{\varepsilon(n')} \\
&= \prod_{i_1=0}^{e_1} \cdots \prod_{i_r=0}^{e_r} \left(l_1^{i_1} \cdots l_r^{i_r}\right)^{\varepsilon(l_1)^{e_1-i_1}\cdots\varepsilon(l_r)^{e_r-i_r}} \\
&= \prod_{k=1}^{r} \left(\prod_{i_1=0}^{e_1} \cdots \prod_{i_r=0}^{e_r} l_k^{\varepsilon(l_1)^{e_1-i_1}\cdots\varepsilon(l_r)^{e_r-i_r}\cdot i_k} \right) \\
&= \prod_{k=1}^{r} l_k^{\sum_{i_1=0}^{e_1} \cdots \sum_{i_r=0}^{e_r} \varepsilon(l_1)^{e_1-i_1} \cdots \varepsilon(l_r)^{e_r-i_r} \cdot i_k} \\
&= \prod_{k=1}^{r} l_k^{\prod_{j\neq k} \left(\sum_{i_j=0}^{e_j} \varepsilon(l_j)^{e_j-i_j} \right) \cdot \left(\sum_{i_k=0}^{e_k} \varepsilon(l_k)^{e_k-i_k} \cdot i_k \right)} \\
&= \prod_{k=1}^{r} l_k^{B_k \prod_{j\neq k} A_j},
\end{aligned}$$

where

$$A_k = \sum_{i=0}^{e_k} \varepsilon(l_k)^{e_k-i}, \quad B_k = \sum_{i=0}^{e_k} \varepsilon(l_k)^{e_k-i} \cdot i.$$

So we need to calculate A_k and B_k for each prime factor l_k of m.

Case 1: $\varepsilon(l_k) = 1$. Then

$$A_k = \sum_{i=0}^{e_k} 1 = e_k + 1$$

and

$$B_k = \sum_{i=0}^{e_k} i = \frac{e_k(e_k+1)}{2}.$$

Case 2: $\varepsilon(l_k) = -1$ and $e_k = 2a_k$ is even. Then

$$A_k = \sum_{i=0}^{2a_k} (-1)^{2a_k-i} = \sum_{i=0}^{2a_k} (-1)^i = 1$$

and

$$B_k = \sum_{i=0}^{2a_k} (-1)^{2a_k - i} i = \sum_{i=0}^{2a_k} (-1)^i i = -1 + 2 - 3 + 4 - \ldots - (2a_k - 1) + 2a_k = a_k.$$

Case 3: $\varepsilon(l_k) = -1$ and $e_k = 2b_k + 1$ is odd. Then

$$A_k = \sum_{i=0}^{2a_k+1} (-1)^{2a_k+1-i} = \sum_{i=0}^{2a_k+1} (-1)^{i-1} = 0$$

and

$$B_k = \sum_{i=0}^{2a_k+1} (-1)^{2a_k+1-i} i = \sum_{i=0}^{2a_k+1} (-1)^{i-1} i = 1 - 2 + 3 - 4 + \cdots + (2a_k + 1) = a_k + 1.$$

The fact that $A_k = 0$ in case 3 gives part 2 of the proposition. The formula for $F(m)$ in part 1 is also clear by looking at the formulae of A_k and B_k in each case.

For part 3, note that in cases 1 and 2 we have $B_k = \frac{e_k}{2} A_k$, and so if m is as in part 3 then

$$F(m) = \prod_{k=1}^{r} l_k^{\frac{e_k}{2} \prod_j A_j} = m^{\frac{1}{2} \prod_k A_j}.$$

□

Proposition 3.1.7. *If $m = \frac{D - x^2}{4}$ for some $x \in \mathbb{Z}$ satisfying $x^2 < D$ and $x^2 \equiv D \mod 4$, then $\varepsilon(m) = -1$.*

Proof. See also [9, Exercise 13.15]. We first fix some notation. By swapping d_1 and d_2 if necessary, we can assume that $d_1 \equiv 1 \mod 4$. Let

$$a = \pm \gcd(d_1, m),$$

with the sign chosen so that $a \equiv 1 \mod 4$. Write

$$d_1 = ad, \quad m = ab.$$

Claim 3.1.8. *We have*

$$\varepsilon(m) = \left(\frac{d_1}{b}\right)\left(\frac{d_2}{a}\right), \tag{3.1.9}$$

and

$$\left(\frac{d_1}{b}\right) = \left(\frac{a}{d_2}\right)\left(\frac{d}{-1}\right). \tag{3.1.10}$$

Before proving the claim, note that if $\gcd(n, n') = 1$ then $\left(\frac{n'}{n}\right) = \pm 1$ and so $\left(\frac{n'}{n}\right)^{-1} = \left(\frac{n'}{n}\right)$. Here we will only be taking the Kronecker symbol of coprime integers, so we will use this property without stating so.

Proof. (of Claim) For Equation (3.1.9), we first note that $\gcd(d_1, b) = 1$. For this, note that since $m = \frac{D-x^2}{4}$, $d_1|D$, $\gcd(d_1, 4) = 1$ and d_1 is squarefree, we have $a = \pm\gcd(d_1, m) = \pm\gcd(d_1, x^2) = \pm\gcd(d_1, x)$. Also, $\gcd(d_2, a) = 1$ since $a|d_2$.

Second, note that if $n \in \mathbb{Z}$ with $\gcd(d_i, n) = 0$ for $i = 1$ or 2, then $\varepsilon(n) = \left(\frac{d_1}{n}\right)$. Hence

$$\varepsilon(m) = \varepsilon(a)\varepsilon(b) = \left(\frac{d_2}{a}\right)\left(\frac{d_1}{b}\right).$$

For Equation (3.1.10), we start with some observations. First,

$$\left(\frac{d_1}{b}\right) = \left(\frac{d_1}{4b}\right) = \left(\frac{a}{4b}\right)\left(\frac{d}{4b}\right). \tag{3.1.11}$$

Second, dividing $4m = d_1d_2 - x^2$ by a gives $4b = dd_1 - a(x/a)^2$, and so

$$4b \equiv dd_2 \mod a. \tag{3.1.12}$$

Hence

$$\begin{aligned}
\left(\frac{a}{d}\right) &= \left(\frac{a}{d_2}\right)\left(\frac{a}{dd_2}\right) && \text{by multiplicativity} \\
&= \left(\frac{a}{d_2}\right)\left(\frac{a}{4b}\right) && \text{by Equation (3.1.12) and Lemma 3.1.2} \\
&= \left(\frac{a}{d_2}\right)\left(\frac{d_1}{b}\right)\left(\frac{d}{4b}\right) && \text{by Equation (3.1.11),}
\end{aligned}$$

and so

$$\begin{aligned}
\left(\frac{d_1}{b}\right) &= \left(\frac{a}{d_2}\right)\left(\frac{a}{d}\right)\left(\frac{d}{4b}\right) \\
&= \left(\frac{d}{a}\right)\left(\frac{d}{4b}\right) && \text{by quadratic reciprocity} \\
&= \left(\frac{a}{d_2}\right)\left(\frac{d}{4ab}\right) && \text{by multiplicativity} \\
&= \left(\frac{a}{d_2}\right)\left(\frac{d}{D-x^2}\right) && \text{since } 4ab = 4m = D - x^2 \\
&= \left(\frac{a}{d_2}\right)\left(\frac{d}{-x^2}\right) && \text{since } d|D \text{ and by Lemma 3.1.2} \\
&= \left(\frac{a}{d_2}\right)\left(\frac{d}{-1}\right) && \text{by multiplicativity and since } \left(\frac{d}{x}\right)^2 = (\pm 1)^2 = 1,
\end{aligned}$$

as desired. □

Now, we have

$$\begin{aligned}
\varepsilon(m) &= \left(\frac{d_1}{b}\right)\left(\frac{d_2}{a}\right) && \text{by Equation (3.1.9)} \\
&= \left(\frac{d_2}{a}\right)\left(\frac{a}{d_2}\right)\left(\frac{d}{-1}\right) && \text{by Equation (3.1.10)} \\
&= \left(\frac{d_2}{\operatorname{sgn}(a)}\right)\left(\frac{d_2}{|a|}\right)\left(\frac{a}{d_2}\right)\left(\frac{d}{-1}\right) && \text{by multiplicativity} \\
&= \left(\frac{d_2}{\operatorname{sgn}(a)}\right)\left(\frac{a}{d_2}\right)^2\left(\frac{d}{-1}\right) && \text{by quadratic reciprocity} \\
&= \left(\frac{d_2}{\operatorname{sgn}(a)}\right)\left(\frac{d}{-1}\right) && \text{since } \left(\frac{a}{d_2}\right)^2 = (\pm 1)^2 = 1.
\end{aligned}$$

Finally, note that since a and d have opposite signs

$$\left(\frac{d}{-1}\right) = \begin{cases} -1 \text{ if } a > 0 \\ \\ 1 \text{ if } a < 0 \end{cases}$$

and, since $d_2 < 0$,

$$\left(\frac{d_2}{\operatorname{sgn}(a)}\right) = \begin{cases} 1 \text{ if } a > 0 \\ -1 \text{ if } a < 0, \end{cases}$$

Hence $\varepsilon(m) = -1$ by considering the cases $a > 0$ and $a < 0$ separately. □

It follows that if $m = \frac{D-x^2}{4}$, then there must be at least one prime l dividing m to an odd power with $\varepsilon(l) = -1$. Hence $F(m)$ is a power of l if there is only one such l, and $F(m) = 1$ if there are two or more such primes l. So we can conclude the following about $J(d_1, d_2)$:

Corollary 3.1.13. *If l is a prime dividing $J(d_1, d_2)$ then*

1. *$\varepsilon(l) = -1$,*
2. *l divides an integer of the form $\frac{D-x^2}{4}$, and*
3. *$l \leq \frac{D}{4}$.*

3.2 Preliminary results

In this section, I present two results from [17] which will play key roles in the algebraic proof of Theorem 3.1.5. The first calculates the valuation of $j(\tau_1) - j(\tau_2)$. The second is a refinement of Deuring's lifting theorem which will allow us to transition from counting isomorphisms of elliptic curves to counting elements of an order in a quaternion algebra.

3.2.1 Calculating $v(j - j')$

For the rest of this section, W will denote a complete, discrete valuation ring, with uniformizer π and corresponding valuation v, such that

1. its field of fractions has characteristic 0,
2. its residue field $k = W/\pi$ is algebraically closed of characteristic $l > 0$, and
3. v is normalized so that $v(\pi) = 1$.

For example, we could take W to be (a finite extension of) the Witt vectors $W\left(\overline{\mathbb{F}}_l\right)$. Also, to simplify things, we assume that $l > 3$. However, the main result of this section, Proposition 3.2.8, is still true if $l = 2, 3$. See [17, Proposition 2.3] for these cases.

Let E, E' be elliptic curves over W with good reduction mod π. Then, by [11], E and E' have Weierstrass equations over W,

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{3.2.1}$$

and

$$E' : y^2 + a'_1xy + a'_3y = x^3 + a'_2x^2 + a'_4x + a'_6. \tag{3.2.2}$$

Let Δ, Δ' be the discriminants of E, E'. Since E, E' have good reduction mod π, we can choose the equations above so that $\Delta, \Delta' \not\equiv 0 \mod \pi$, and then $\Delta, \Delta' \in W^\times$. The change of variables

$$(x, y) \mapsto \left(\frac{x - 3a_1^2 - 12a_2}{36}, \frac{y - a_1x - a_3}{216}\right),$$

which is defined over W since $2, 3 \in W^\times$, puts E in the form

$$E : y^2 = x^3 + Ax + B. \tag{3.2.3}$$

The discriminant of this Weierstrass equation is 6^{-12} times the discriminant of Equation (3.2.1), so is a unit in W. A calculation gives that that the discriminant and j-invariant of E are

$$\Delta = -16(4A^3 + 27B^2), \quad j = -1728\frac{(4A)^3}{\Delta}. \tag{3.2.4}$$

A similar change of variables gives E' the Weierstrass equation

$$E' : y^2 = x^3 + A'x + B', \tag{3.2.5}$$

and then its discriminant and j-invariant are

$$\Delta' = -16(4(A')^3 + 27(B')^2) \in W^\times, \quad j' = -1728\frac{(4A)^3}{\Delta'}. \tag{3.2.6}$$

For $n \geq 1$, let $\mathrm{Iso}_n(E, E')$ denote the set of isomorphisms from $E \mod \pi^n$ to $E' \mod \pi^n$, and let

$$i(n) := \frac{1}{2}\#\mathrm{Iso}_n(E, E'). \tag{3.2.7}$$

The following result , which is [17, Proposition 2.3], relates the number of isomorphisms $E \to E' \mod \pi^n$ to the valuation of $j - j'$.

Proposition 3.2.8. $v(j - j') = \sum_{n \geq 1} i(n)$.

Proof. Since $l > 3$, we have $v(2) = v(3) = 0$. Also, since $\Delta \in W^\times$ and $1728\Delta = -16(4A^3 + 27B^2)$,

$$0 \geq \min\{v(A^3), v(B^2)\},$$

so $v(A) = 0$ or $v(B) = 0$ since $A, B \in W$. Hence $A \in W^\times$ or $B \in W^\times$.

Relative to the Weierstrass equations Equation (3.2.3) and Equation (3.2.5), any isomorphism from E' to E over k is of the form

$$(x, y) \mapsto (u^2 x + r, u^3 y + s u^2 x t) \tag{3.2.9}$$

with $r, s, t, u \in k$ and $u \neq 0$. Looking at the relations this gives between A, B and A', B', we see that we must have $r = s = t = 0$ and that u must satisfy

$$\begin{cases} A \equiv u^4 A' \mod \pi \\ B \equiv u^6 B' \mod \pi. \end{cases} \tag{3.2.10}$$

Conversely, any such $u \in k$ gives an isomorphism $E' \to E, (x, y) \mapsto (u^2 x, u^3 y)$. So giving an isomorphism from E to E' over k is equivalent to finding a solution u to Equation (3.2.10).

Similarly, by [11], we know that any isomorphism $E' \mod \pi^n \xrightarrow{\sim} E \mod \pi^n$ is of the form Equation (3.2.9) with $r, s, t \in W/\pi^n$ and $u \in (W/\pi^n)^\times$. So finding such an

isomorphism is equivalent to finding a solution u of

$$\begin{cases} A \equiv u^4 A' \mod \pi^n \\ B \equiv u^6 B' \mod \pi^n. \end{cases} \tag{3.2.11}$$

Now suppose that $i(1) \geq 1$. Since k is algebraically closed, this is equivalent to saying that $j - j' \equiv 0 \mod \pi$, i.e. that $v(j - j') \geq 1$. By the above discussion, it is also equivalent to saying that there exists $u_0 \in k^\times$ satisfying Equation (3.2.10). We consider separately the cases $A \in W^\times$ and $B \in W^\times$.

Case 1: A is a unit. Note that since W is a discrete valuation ring, $x \in W$ is a unit if and only if $x \mod \pi$ is a unit in k. Then $A \mod \pi$ is a unit, so $A' \mod \pi$ is a unit since $A \equiv u_0^4 A' \mod \pi$, so A' is a unit in W. So by making appropriate changes of coordinates on E and E' we can get $A = A' = 1$. Subject to these constraints, we can modify B and B' only by ± 1, so choose B, B' so that $v(B - B')$ is maximal. In particular, note that this means that $v(B - B') \geq v(B + B')$.

Now, for $n \geq 1$, the number of isomorphisms $\mod \pi^n$ is the number of solutions $u \in (W/\pi^n)^\times$ to

$$\begin{cases} u^4 \equiv 1 \mod \pi^n \\ B \equiv u^6 B' \mod \pi^n. \end{cases} \tag{3.2.12}$$

Under the assumption that $v(B - B')$ is maximal, the number of such solutions is

$$2i(n) = \begin{cases} 4 & \text{if } B \equiv B' \equiv 0 \mod \pi^n, \\ 2 & \text{if } B \equiv B' \mod \pi^n \text{ and } B, B' \not\equiv 0 \mod \pi^n, \\ 0 & \text{otherwise,} \end{cases}$$

or equivalently

$$2i(n) = \begin{cases} 4 & \text{if } B - B' \equiv 0 \mod \pi^n \text{ and } B + B' \equiv 0 \mod \pi^n, \\ 2 & \text{if } B - B' \equiv 0 \mod \pi^n \text{ and } B + B' \not\equiv 0 \mod \pi^n, \\ 0 & \text{if } B - B' \not\equiv 0 \mod \pi^n. \end{cases}$$

Indeed, if there is such a solution, then $B \cong \pm B' \mod \pi^n$, and then since $v(B - B') \geq v(B + B')$ we must have $B \equiv B' \mod \pi^n$. Then there are two solutions if $B \not\equiv 0 \mod \pi^n$ and four solutions if $B \equiv B' \equiv 0 \mod \pi^n$.

So we have

$$\sum_{n \geq 1} i(n) = v(B + B') + v(B - B').$$

On the other hand, since $A = A' = 1$,

$$\begin{aligned} j - j' &= -1728 \left(\frac{(4A)^3}{\Delta} - \frac{(4A')^3}{\Delta'} \right) \\ &= -1728 \cdot 4^3 \left(\frac{\Delta' - \Delta}{\Delta \Delta'} \right) \\ &= 1728 \cdot 4^3 \left(\frac{16 \cdot 27 B'^2 - 16 \cdot 27 B^2}{\Delta \Delta'} \right) \\ &= -\frac{2^{16} 3^5}{\Delta \Delta'} \left(B^2 - B'^2 \right), \end{aligned} \tag{3.2.13}$$

and so

$$v(j - j') = v(B^2 - B'^2) = v(B + B') + v(B - B')$$

since $-\dfrac{2^{16} 3^5}{\Delta \Delta'} \in W^\times$.

Case 2: B is a unit. Then by the same argument as in Case 1, we have $B' \in W^\times$ as well. Choose Weierstrass equations so that $B = B'$. Subject to this constraint we can modify A and A' only by a cube root of 1, so choose A, A' so that $v(A - A')$ is maximal.

For $n \geq 1$, the number of isomorphisms mod π^n is the number of solutions $u \in$

$(W/\pi^n)^\times$ to

$$\begin{cases} u^6 \equiv 1 \mod \pi^n \\ A \equiv u^4 A' \mod \pi^n, \end{cases} \tag{3.2.14}$$

which is

$$2i(n) = \begin{cases} 6 & \text{if } A \equiv A' \equiv 0 \mod \pi^n \\ 2 & \text{if } A \equiv \omega A' \text{ or } \omega^2 A' \mod \pi^n, \text{ and } A, A' \not\equiv 0 \mod \pi^n, \end{cases}$$

where $\omega = e^{2\pi i/3}$ is a primitive third root of unity. So we have

$$\sum_{n \geq 1} i(n) = v(A - A') + v(A - \omega A') + v(A - \omega^2 A') = v(A^3 - A'^3) = v(j - j'),$$

the last equality coming from a calculation similar to Equation (3.2.13). □

Corollary 3.2.15. *Suppose that $(l-1)|12$ and that E, E' have supersingular reduction mod π. Then*

$$v(j - j') \geq \frac{12}{l-1}.$$

Proof. We know that when $(l-1)|12$, there is a unique supersingular j-invariant in $\overline{\mathbb{F}}_l$, and its automorphism group has order $\frac{24}{l-1}$. So we must have $E \cong E' \mod \pi$, and then $v(j - j') \geq i(1) = \frac{12}{l-1}$. □

Corollary 3.2.16. *Let d be a negative fundamental discriminant, and suppose that E has complex multiplication by the order $\mathcal{O}$ of discriminant d. If $d < -4$ and $\left(\frac{d}{l}\right) = 1$, then*

$$\mathrm{Nm}\,(j)\mathrm{Nm}\,(j - 1728) \not\equiv 0 \mod l.$$

Proof. Let $K = \mathrm{Frac}\,(\mathcal{O})$ be the imaginary quadratic field of discriminant d. Since $\left(\frac{d}{l}\right) = 1$, E has ordinary reduction mod π for any prime π of $K(j)$ dividing l. Then $\mathrm{End}_{W/\pi}(E) = \mathrm{End}_W(E) = \mathcal{O}$. If $d < -4$, then $\mathcal{O}^\times = \{\pm 1\}$ and so $j \neq 0, 1728 \mod \pi$ since the elliptic curves with these j-invariants have more than 2 automorphisms mod π. □

Corollary 3.2.17. *Suppose that* $\left(\frac{d}{l}\right) = -1$. *Then*

$$\begin{cases} j \equiv 0 \mod 2^{12} & \text{if } l = 2, \\ j \equiv 1728 \mod 3^6 & \text{if } l = 3, \\ j \equiv 0 \mod 5^3 & \text{if } l = 5, \\ j \equiv 1728 \mod 7^2 & \text{if } l = 7, \\ j^{1/3}(j-1728)^{1/2} \equiv 0 \mod 11 & \text{if } l = 11, \\ j \equiv 5 \mod 13 & \text{if } l = 13. \end{cases}$$

Proof. Since $\left(\frac{d}{l}\right) = -1$, E has supersingular reduction modulo π for any prime π of $K(j)$ dividing l. If $l = 2, 3, 5, 7, 13$, then there is a unique supersingular j-invariant in characteristic l. It is 0 if $l = 2, 5$, 1728 if $l = 3, 7$ and 5 if $l = 13$.[1] Applying Corollary Corollary 3.2.15 gives the result for $l = 2, 3, 5, 7, 13$.

If $l = 11$, then the only supersingular j-invariants are $0, 1728$. So $E \cong E' \mod \pi$, for some elliptic curve E' with $j(E') = 0$ or $j(E') = 1728$. If $j(E') = 0$, then

$$v(j) \geq i(1) = \frac{1}{2}\#\mathrm{Aut}_{W/\pi}(E') = 3,$$

and if $j(E') = 1728$ then

$$v(j - 1728) \geq i(1) = 2. \qquad \square$$

3.2.2 A refinement of Deuring's lifting theorem

As before, let W be a discrete valuation ring with uniformizer π such that W/π is algebraically closed of characteristic $l > 0$. Let E_0 be an elliptic curve over W/π^n, and let $\alpha_0 \in \mathrm{End}_{W/\pi^n}(E)$ be such that $\mathbb{Z}[\alpha_0]$ is the ring of integers of an imaginary quadratic field K, i.e. such that $d := \mathrm{Tr}(\alpha_0) - 4\mathrm{Nm}(\alpha_0)$ is a negative fundamental discriminant,

[1] For the case $l = 13$, we can check that 5 is supersingular by checking that the equations $H_{13}(\lambda) = 0$ and $5 = \frac{(1-\lambda+\lambda^2)^3}{\lambda^2(1-\lambda)^2}$ are the same mod 13. This means that any of the λ values lying above $j = 5$ are solutions to $H_{14}(x) = 0 \mod l$, and so correspond to supersingular elliptic curves by [26, §V, Theorem 4.1].

where $\mathrm{Tr}\,(\alpha_0) = \alpha + \alpha^\wedge \in \mathbb{Z}$ is the trace of α_0 and $\mathrm{Nm}\,(\alpha_0) = \alpha \circ \alpha^\wedge \in \mathbb{Z}$ is the norm of α_0.

Note that α_0 satisfies the quadratic equation $x^2 - tx + n = 0$, where $t = \mathrm{Tr}\,(\alpha_0)$ and $n = \mathrm{Nm}\,(\alpha_0)$. On $\mathrm{Lie}\,(E_0)$, α_0 induces multiplication by some $w_0 \in W/\pi^n$ satisfying this same equation.

If (E, α) is a lift of (E_0, α_0) to W, i.e. E is an elliptic curve over W and $\alpha \in \mathrm{End}_W(E)$ with $(E, \alpha) \mod \pi^n = (E_0, \alpha_0)$, then α acts on $\mathrm{Lie}\,(E)$ by an element $w \in W$ satisfying

$$\begin{cases} w \equiv w_0 \mod \pi^n \\ w^2 - tw + n = 0. \end{cases} \tag{3.2.18}$$

So the existence of such a w is a necessary condition for the existence of a lifting of (E_0, α_0) to W. The following proposition says that it is also a sufficient condition.

Proposition 3.2.19. *Suppose that $w \in W$ satisfies*

$$\begin{cases} w \equiv w_0 \mod \pi^n \\ w^2 - tw + n = 0. \end{cases}$$

Then there exists an elliptic curve E over W and $\alpha \in \mathrm{End}_W(E)$ such that $(E, \alpha) \equiv (E_0, \alpha_0) \mod \pi^n$ and α induces multiplication by w on $\mathrm{Lie}\,(E)$.

Moreover, if (E', α') is another such lifting, then $E \cong E'$ and the diagram

$$\begin{array}{ccc} E & \xrightarrow{\alpha} & E \\ \wr\downarrow & & \wr\downarrow \\ E' & \xrightarrow{\alpha'} & E' \end{array}$$

commutes.

Before the proof, we give a brief introduction to Serre-Tate's deformation theory. Let W, π be as above and let $k = W/\pi$ be the residue field of W. Recall that we had $\mathrm{char}\,(k) = l > 0$.

Definition 3.2.20. Let A be an abelian variety over k. The *l-divisible group* of A,

denoted $A(l)$ or $A[l^\infty]$, is

$$\varinjlim_{n\to\infty} A[l^n] = \bigcup_{n>0} A[l^n],$$

where $A[l^n]$ is the group scheme of l^n-torsion points of A.

More generally, an *l-divisible group (of height h)* $\{G_n\}$ over a scheme S is a system of finite flat commutative group schemes

$$G_1 \xrightarrow{i_1} G_2 \to \ldots \to G_n \xrightarrow{i_n} G_{n+1} \to \ldots$$

over S such that for each $n \in \mathbb{N}$, G_n is locally free of rank l^{nh} over S, and the sequence

$$0 \to G_n \xrightarrow{i_n} G_{n+1} \xrightarrow{\times l^n} G_{n+1}.$$

is exact.

This means that i_n identifies G_n with the l^n-torsion of G_{n+1}.

A *morphism* of l-divisible groups $\{G_n\} \to \{H_n\}$ is a collection of homomorphisms of group schemes $f_n : G_n \to H_n, n \in \mathbb{N}$ such that for each n, the following diagram commutes:

$$\begin{array}{ccc} G_n & \xrightarrow{f_n} & H_n \\ \uparrow & & \uparrow \\ G_{n-1} & \xrightarrow{f_{n-1}} & H_{n-1}. \end{array}$$

The l-divisible group of A can be viewed as an l-divisible group in the general sense by taking $G_n = A[l^n]$.

Definition 3.2.21. Let R be a local, Noetherian, complete ring with residue field k, and let A be an abelian variety over k. A *deformation* of A to R is an abelian scheme $\mathcal{A}$ over R together with an isomorphism of abelian varieties $i : \mathcal{A} \otimes_R k \xrightarrow{\sim} A$.

We can define deformations in other categories similarly. For example, if $G = \{G_n\}$ is an l-divisible group over k, a deformation of G to R is an l-divisible group $\mathcal{G} = \{\mathcal{G}_n\}$ over R together with an isomorphism of l-divisible groups $f : \mathcal{G} \otimes_R k \xrightarrow{\sim} G$, that is to say a morphism $f = \{f_n\}$ such that each $f_n : \mathcal{G}_n \otimes_R k \to G_n$ is an isomorphism.

Another example is the following: if $\Phi(x,y) \in k[[x,y]]$ is a (commutative, 1-dimensional) formal group law over k (see, for example, [26, Chapter IV] for an introduction to formal group laws), then a deformation of Φ to R is a formal group law $F(x,y)$ over R such that $F \mod \mathfrak{m} = \Phi$, where $\mathfrak{m}$ is the maximal ideal of R.

If $\mathcal{A}$ is a deformation of an abelian variety A to R, then we get a deformation of the l-divisible group G of A,

$$\mathcal{G} = \mathcal{A}(l) = \varinjlim_{n \in \mathbb{N}} \mathcal{A}[l^n].$$

The theory of Serre-Tate says that the converse is true, i.e. that given a deformation $\mathcal{G}$ of G, we can get a deformation $\mathcal{A}$ of A such that $\mathcal{G} = \mathcal{A}(l)$, provided that $\mathrm{char}\,(k) = l$. So deforming an abelian variety A is equivalent to deforming its l-divisible group G.

Also, if A_1, A_2 are abelian varieties, then a homomorphism $f : A_1 \to A_2$ gives a homomorphism of the l-divisible groups, $\tilde{f} : A_1(l) \to A_2(l)$. If $\mathcal{A}_1, \mathcal{A}_2$ are deformations of A_1, A_2 respectively, then f lifts to $\mathrm{Hom}\,(\mathcal{A}_1, \mathcal{A}_2)$ if and only if $\tilde{f}$ lifts to $\mathrm{Hom}\,(\mathcal{A}_1(l), \mathcal{A}_2(l))$.

We also introduce the "canonical lift" of an abelian variety. Let R be a local, Noetherian, complete ring with maximal ideal $\mathfrak{m}$ and residue field $R/\mathfrak{m} \cong k$, and let A be an abelian variety of dimension g over k. We say that A is *ordinary* if $A[l^n](k) \cong (\mathbb{Z}/l^n\mathbb{Z})^g, \forall n \geq 1$. In this case, there is a unique lift $\mathcal{A}$ of A to R with the property $\mathrm{End}_R(\mathcal{A}) = \mathrm{End}_k(A)$ (via $(f : \mathcal{A} \to \mathcal{A}) \mapsto (f \mod \mathfrak{m} : A \to A)$). We call this $\mathcal{A}$ the *canonical lift* of A to R.

Proof. (of Proposition 3.2.19) Let $(\overline{E}, \overline{\alpha})$ be the reduction of (E_0, α_0) to $k = W/\pi$.

Case 1: $\overline{E}$ is ordinary. So $\mathbb{Z}[\overline{\alpha}] = \mathrm{End}\,(\overline{E})$. Then there are unique (canonical) lifts

1. (E, α) of $(\overline{E}, \overline{\alpha})$ to W, and
2. $(\widetilde{E}, \widetilde{\alpha})$ of $(\overline{E}, \overline{\alpha})$ to W/π^n.

Then (E_0, α_0) and $(E, \alpha) \mod \pi^n$ are both lifts of $(\overline{E}, \overline{\alpha})$ to W/π^n, and so by uniqueness they must be isomorphic. So (E, α) is a lift of (E_0, α_0), and it is clearly unique since any other lift would also be a lift of $(\overline{E}, \overline{\alpha})$.

Case 2: $\overline{E}$ is supersingular. Then the formal group $f(x,y)$ of $\overline{E}$ over k has dimension 1 and height 2, and deforming $(\overline{E}, \overline{\alpha})$ is the same as deforming $f(x,y)$ considered as an

$\hat{\mathcal{O}}$-module, where $\hat{\mathcal{O}}$ is the completion of $\mathcal{O} = \mathbb{Z}[\alpha_0]$ relative to l. Note that we can indeed consider f as an $\hat{\mathcal{O}}$-module, since there is a $w \in W$ lifting w_0 and satisfying $w^2 - tw + n = 0$, so $\mathcal{O} \subseteq W$, so $\hat{\mathcal{O}} \subseteq W$ as well.

Now, I claim that f has height 1 as a formal $\hat{\mathcal{O}}$-module. To see this, note that since it has height 2 as a $\mathbb{Z}_l$-module, we can write the homomorphism l_f of f corresponding to multiplication by l as a power series in x^{l^2}. Since $\overline{E}$ is supersingular, l is either inert or ramified in $\mathcal{O}$. We consider each case separately.

Case 2 a: l is inert in $\mathcal{O}$. Then $\mathcal{O}/l\mathcal{O}$ has $q = l^2$ elements, and l is a uniformizer for $\hat{\mathcal{O}}$. We can write l_f as a power series in $x^{l^2} = x^q$, so f has height 1 over $\mathcal{O}$.

Case 2 b: l is ramified in $\mathcal{O}$. Then $\mathcal{O}/l\mathcal{O}$ has l elements, and $\hat{\mathcal{O}}$ has uniformizer π satisfying $\pi^2 = ul$, for some $u \in \mathcal{O}^\times$. If h is the height of f as a formal $\mathcal{O}$-module, then we can write π_f as a power series in x^{l^h}, say

$$\pi_f = a(x^{l^h}) = a_1 x^{l^h} + \dots$$

Then

$$\pi_f^2 = a \circ a(x) = a_1^2 x^{l^2 h} + \dots$$

is a power series in $x^{l^2 h}$. So $l_f = u_f \circ \pi_f^2$ is too, since u is a unit, so

$$u_f = u_1 x + \dots$$

But we know that l_f is a power series in x^{l^2}, so $h = 1$.

So f has height 1 as a formal $\hat{\mathcal{O}}$-module, and, by [16], its universal deformation space is $\mathrm{Spf}(\hat{\mathcal{O}})$, and there is a unique deformation F of f as an $\hat{\mathcal{O}}$-module, or equivalently as an $\mathcal{O}$-module, to any local, Noetherian, complete ring R with residue field k. Hence there is also a unique deformation of $(\overline{E}, \overline{\alpha})$ to any such ring. Now, the same argument as in Case 1 shows that there is a unique lift of (E_0, α_0) to W. $\square$

3.3 The algebraic proof of Gross-Zagier's formula

3.3.1 Counting isomorphisms modulo π^n

As in [17], we assume that $d_1 = -p$, $p > 0$ prime, to simplify some computations. The general case is handled in [13].

We use the following notation:

1. $\tau = \frac{1+\sqrt{-p}}{2}$,
2. $K = \mathbb{Q}(\sqrt{-p})$, and $\mathcal{O} = \mathbb{Z}[\tau]$ is the ring of integers of K,
3. $j = j(\tau)$, and $H = K(j)$ is the Hilbert class field of K,
4. $w \in \mathbb{C}$ is a fixed imaginary quadratic number of discriminant d_2, $K_2 = \mathbb{Q}(w)$ is the quadratic field of discriminant d_2, $\mathcal{O}_2 = \mathbb{Z}[w]$ is the ring of integers of K_2, and H_2 is the Hilbert class field of K_2, and
5. $\tilde{H} = H \cdot H_2$.

We define the algebraic integer

$$\alpha := \prod_{\substack{\tau_2 \in \Gamma\backslash\mathcal{H} \\ \operatorname{disc}(\tau_2) = d_2}} (j - j(\tau_2))^{\frac{4}{w_1 w_2}} \in \tilde{H} \subseteq \mathbb{C}, \tag{3.3.1}$$

where as before w_i is the size of the unit group of the imaginary quadratic order $\mathcal{O}_i$ with discriminant d_i. Note that $J(d_1, d_2) = \operatorname{Nm}_{H/K}(\alpha)$. Our goal is to calculate the valuation of α at every non-archimedean valuation of $\tilde{H}$.

So let v be a finite place of $\tilde{H}$ corresponding to a prime ideal $\mathfrak{p} = \mathfrak{p}_v$, and let l be the rational prime lying above $\mathfrak{p}$. For the rest of this chapter, fix an embedding $i : \overline{\mathbb{Q}} \to \overline{\mathbb{Q}}_p$ such that $\mathfrak{p} = i^{-1}(\mathfrak{m}_{\overline{\mathbb{Q}}_p}) \cap \mathcal{O}_K$, where $\mathfrak{m}_{\overline{\mathbb{Q}}_p}$ is the unique maximal ideal of $\overline{\mathbb{Q}}_p$.

Let $W(\overline{\mathbb{F}}_l)$ denote the Witt vectors of the field $\overline{\mathbb{F}}_l$. This is a complete discrete valuation ring with uniformizer l and residue field $\overline{\mathbb{F}}_l$. Let $W = W(\overline{\mathbb{F}}_l) \cdot \mathcal{O}_{\tilde{H}}$. Let π be a uniformizer for W, and $e = e(W/W(\overline{\mathbb{F}}_l))$ be the residue degree of W over $W(\overline{\mathbb{F}}_l)$. One can check that $e = 1$ if $l \not| pq$ and $e = 2$ if $l|p$ or $l|q$.

Now, there exists an elliptic curve over $H \subseteq \mathrm{Frac}\,(W)$ with j-invariant j and with complex multiplication by $\mathcal{O}$ over H (i.e. with $\mathrm{End}_H(E) = \mathcal{O}$). So by [25, Theorem 9], there exists an elliptic curve E over W with j-invariant $j(E) = j$, complex multiplication by $\mathcal{O}$ over W, and with good reduction modulo π. Similarly, for each imaginary quadratic $\tau_2 \in \mathbb{C}$ of discriminant d_2, there exists an elliptic curve E_{τ_2} over W with j-invariant $j\left(E_{\tau_2}\right) = j(\tau_2)$, complex multiplication by $\mathcal{O}_2$ over W, and good reduction modulo π. Write

$$\mathcal{J}(d_2) = \{E_{\tau_2} : \tau_2 \in \mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H}, \mathrm{disc}\,(\tau_2) = d_2\}.$$

By Proposition 3.2.8, we can write

$$\begin{aligned}
\mathrm{ord}_v(\alpha) &= \frac{4}{ew_1w_2} \sum_{\substack{\tau_2 \in \mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H} \\ \mathrm{disc}\,(\tau_2) = d_2}} \mathrm{ord}_v(j - j(\tau_2)) \\
&= \frac{4}{ew_1w_2} \sum_{E' \in \mathcal{J}(d_2)} \mathrm{ord}_v(j - j(E')) \\
&= \frac{2}{ew_1w_2} \sum_{n \geq 1} \sum_{E' \in \mathcal{J}(d_1)} \#\mathrm{Iso}_{W/\pi^n}(E, E').
\end{aligned}$$

Now, define

$$S_n := \{\alpha_0 \in \mathrm{End}_{W/\pi^n}(E) : \mathrm{Tr}\,(\alpha_0) = \mathrm{Tr}\,(w), \mathrm{Nm}\,(\alpha_0) = \mathrm{Nm}\,(w), \alpha_0 = w \text{ on } \mathrm{Lie}\,(E)\},$$

where w is the imaginary quadratic number of discriminant d_2 fixed above.

Proposition 3.3.2. *We have*

$$\#S_n = \frac{1}{w_2} \sum_{E'} \#\mathrm{Iso}_{W/\pi^n}(E, E'),$$

where the sum is over a set of representatives for the isomorphism classes of elliptic curves with complex multiplication by $\mathbb{Z}[w]$. Hence we can write

$$\mathrm{ord}_v(\alpha) = \frac{2}{ew_1} \sum_{n \geq 1} \#S_n$$

Proof. Given an isomorphism $f : E \xrightarrow{\sim} E' \mod \pi^n$, we get an element $w_f = f^{-1} \circ w \circ f$ of S_n.

Conversely, let $\alpha_0 \in S_n$. Then w satisfies the conditions of Proposition 3.2.19 for the pair $(E \mod \pi^n, \alpha_0)$, and so there exists an elliptic curve F over W and $\alpha \in \mathrm{End}_W(F)$ such that

1. $(F, \alpha) \equiv (E, \alpha_0) \mod \pi^n$
2. α induces multiplication by w on $\mathrm{Lie}(F)$.

Then F has complex multiplication by $\mathbb{Z}[\alpha] = \mathbb{Z}[w]$, and hence is isomorphic to one of the elliptic curves E', by some map $f : F \to E'$ with $\alpha = f^{-1} \circ w \circ f$. Hence

$$f \mod \pi^n \in \mathrm{End}_{W/\pi^n}(E, E').$$

Moreover, Proposition 3.2.19 says that if (F', α') is another lifting of $(E \mod \pi^n, \alpha_0)$, then $F' \cong F$ over W and we have a commutative diagram

$$\begin{array}{ccc} F & \xrightarrow{\alpha} & F \\ \wr\downarrow & & \wr\downarrow \\ F' & \xrightarrow{\alpha'} & F', \end{array}$$

hence E' is unique and f is unique up to an automorphism of E' over W, i.e. up to multiplication by $\mathcal{O}_2^\times$.

This shows that the map

$$\bigcup_{E'} \#\mathrm{Iso}_{W/\pi^n}(E, E') \longrightarrow S_n$$

$$f \longmapsto w_f = f^{-1} \circ w \circ f$$

is w_2-to-1, which gives the first claim.

The second claim follows from the first part of the proposition and the fact that for each τ_2 of discriminant d_2, there is, up to isomorphism, a unique elliptic curve over W with complex multiplication by $\mathbb{Z}[w]$ and j-invariant $j(\tau)$, and so $\{E_{\tau_2} : \tau_2 \in \mathcal{F}, \mathrm{disc}(\tau_2) = d_2\}$

is a set of representatives for the isomorphism classes of elliptic curves with complex multiplication by $\mathbb{Z}[w]$. $\square$

So we need to determine the size of the set $\#S_n$ for all $n \geq 1$.

3.3.2 Computing $\mathrm{End}_{W/\pi^n}(E)$

Recall that we had

$$\alpha = \prod_{\substack{\tau_2 \in \mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H} \\ \mathrm{disc}\,(\tau_2)=d_2}} (j - j(\tau_2))^{\frac{4}{w_1 w_2}}. \tag{3.3.3}$$

We want to find $\mathrm{ord}_v(\alpha)$, where v is a finite place of $\tilde{H}$ lying above a prime l. By Proposition 3.3.2, it's enough to find $\#S_n$ for all $n \geq 1$. To this end, we will find a formula for the order $\mathrm{End}_{W/\pi^n}(E)$ for $n \geq 1$.

Proposition 3.3.4. *If* $\left(\frac{l}{p}\right) = 1$ *then* $\mathrm{ord}_v(\alpha) = 0$.

Proof. Since $\left(\frac{l}{p}\right) = 1$, E has ordinary reduction $\mod \pi$. So $\mathrm{End}_{W/\pi^n}(E) = \mathcal{O}$ for all $n \geq 1$. Since $\mathcal{O}$ has no elements of discriminant d_2, $S_n = \varnothing, \forall n \geq 1$. Hence $\mathrm{ord}_v(\alpha) = 0$. $\square$

So assume that $\left(\frac{l}{p}\right) \neq 1$, i.e. that E has supersingular reduction $\mod \pi$. Also, let $d_2 = -q, q > 0$. Since E has supersingular reduction $\mod \pi$, $\mathrm{End}_{W/\pi}(E)$ is isomorphic to a maximal order in the quaternion algebra B ramified at l and ∞, which we can write as

$$B = \left\{ [\alpha, \beta] := \begin{pmatrix} \alpha & \beta \\ -l\overline{\beta} & \overline{\alpha} \end{pmatrix} : \alpha, \beta \in K \right\} \subseteq M_2(K) \tag{3.3.5}$$

by Proposition A.2. For $n > 1$, $\mathrm{End}_{W/\pi^n}(E)$ is isomorphic to a subring of the maximal order $\mathrm{End}_{W/\pi}(E)$.

Since $p \equiv 3 \mod 4$, the class number h of K is odd, and $j(\mathcal{O})$ is the unique real j-invariant of discriminant $-p$. So there is a unique embedding $\mathbb{Q}(j) \to \mathbb{R} \cap \overline{\mathbb{Q}}$, sending j to $j(\mathcal{O})$. Since we've fixed an embedding $\overline{\mathbb{Q}} \to \overline{\mathbb{Q}}_l$, this gives an embedding $\mathbb{Q}(j) \to \overline{\mathbb{Q}}_l$, which can be extended to one of two embeddings $i_1 : H \to \overline{\mathbb{Q}}_l$. Let $p_1 = i_1^{-1}(\mathfrak{m}_{\overline{\mathbb{Q}}_l}) \cap \mathcal{O}_H$ and v_1 be the valuation of H corresponding to p_1. On the other hand, let v_0 be the

valuation on H obtained by restricting v. Then, for example by [4, Corollary 1.3.5], there is a unique $\sigma \in \mathrm{Gal}\,(H/K)$ such that $\mathrm{ord}_{v_0}(x) = \mathrm{ord}_{v_1}(\sigma(x))$ for all $x \in H^\times$. Let $\mathfrak{a} = \mathfrak{a}_\sigma$ be a fractional ideal of K such that $([\mathfrak{a}], H/K) = \sigma$, i.e. such that the ideal class $[\mathfrak{a}] \in \mathrm{Cl}\,(\mathcal{O})$ corresponds to σ under the Artin isomorphism.

Also, let $D^{-1} = \{x \in K : \mathrm{Tr}\,(xy) \in \mathbb{Z}, \forall y \in \mathcal{O}\}$ be the inverse different of $\mathcal{O}$, and fix $\lambda \in \mathcal{O}$ such that $\lambda^2 = -l \mod D$. Recall for later use that$D^{-1} = \frac{1}{\sqrt{-p}}\mathcal{O}$ and $D = \sqrt{-p}\mathcal{O}$.

For $x \in \mathbb{Z}$, define

$$\delta(x) := \begin{cases} 2 \text{ if } p|x \\ \\ 1 \text{ otherwise,} \end{cases} \tag{3.3.6}$$

and define the set

$$T_n = \left\{(x, \mathfrak{b}) \in \mathbb{Z} \times [\mathfrak{a}^2] : \mathfrak{b} \subseteq \mathcal{O}, x^2 + 4l^{2n-1}\mathrm{Nm}\,(\mathfrak{b}) = pq\right\}, \tag{3.3.7}$$

where $[\mathfrak{a}^2]$ is the class of $\mathfrak{a}^2$ in $\mathrm{Cl}\,(\mathcal{O})$. In particular, we have

$$T_1 = \left\{(x, \mathfrak{b}) \in \mathbb{Z} \times [\mathfrak{a}^2] : \mathfrak{b} \subseteq \mathcal{O}, x^2 + 4l\mathrm{Nm}\,(\mathfrak{b}) = pq\right\}. \tag{3.3.8}$$

Proposition 3.3.9. *If $l \nmid pq$, then $e = 1$ and for all $n \geq 1$, we have*

$$\mathrm{End}_{W/\pi^n}(E) = \left\{[\alpha, \beta] \in B : \alpha \in D^{-1}, \beta \in D^{-1}l^{n-1}\overline{\mathfrak{a}}/\mathfrak{a}, \alpha \equiv \lambda\beta \mod \mathcal{O}\right\}$$

and

$$\#S_n = \frac{w_1}{4} \sum_{(x,\mathfrak{b}) \in T_n} \delta(x).$$

The sum in the proposition counts the number of elements in R_n, i.e. the number of $(x, \mathfrak{b}) \in \mathbb{Z} \times [\mathfrak{a}^2]$ satisfying $x^2 + 4l\mathrm{Nm}\,(\mathfrak{b}) = pq$, counting a pair $(x, \mathfrak{b})$ twice if $p|x$.

Before we prove this lemma, we give a result from [8] which will be useful. Let A be a ring, M, M' be finitely generated projective left A-modules, and let $\mathcal{M}, \mathcal{M}'$ be left A-module schemes over a base scheme S. Write $M'^\vee := \mathrm{Hom}_A(M, A)$.

Lemma 3.3.10. ([8, Lemma 7.14]) *The map*

$$\xi_{M,M'} : M'^{\vee} \otimes_A \mathrm{Hom}_S(\mathcal{M}, \mathcal{M}') \otimes_A M \longrightarrow \mathrm{Hom}_S(\mathrm{Hom}_A(M, \mathcal{M}), \mathrm{Hom}_A(M', \mathcal{M}'))$$

$$l' \otimes \varphi \otimes m \longmapsto (f \mapsto (m' \mapsto l'(m')\varphi(f(m))))$$

is a well-defined isomorphism.

Proof. To see that $\xi_{M,M'}$ is well-defined, note that the map

$$\xi_{M,M'} : M'^{\vee} \times \mathrm{Hom}_S(\mathcal{M}, \mathcal{M}') \times M \longrightarrow \mathrm{Hom}_S(\mathrm{Hom}_A(M, \mathcal{M}), \mathrm{Hom}_A(M', \mathcal{M}'))$$

$$(l', \varphi, m) \longmapsto (f \mapsto (m' \mapsto l'(m')\varphi(f(m))))$$

is A-multilinear, and so it induces a group homomorphism

$$M'^{\vee} \otimes_A \mathrm{Hom}_S(\mathcal{M}, \mathcal{M}') \otimes_A M \to \mathrm{Hom}_S(\mathrm{Hom}_A(M, \mathcal{M}).$$

To check that it is an isomorphism, first note that if N, N' are another pair of finitely generated projective left A-modules, then $\xi_{M\oplus N,M'} = \xi_{M,M'} \oplus \xi_{N,M'}$ and $\xi_{M,M'\oplus N'} = \xi_{M,M'} \oplus \xi_{M,N'}$. This requires checking that the diagrams in Figure 3.1 commute.

Now, since M, M' are projective and finitely generated, there are A-modules N, N' and $r, r' > 0$ such that $M \oplus N \cong A^{\oplus r}$ and $M' \oplus N' \cong A^{\oplus r'}$. Then by the above observation, we have $\xi_{M\oplus N,M'\oplus N'} = \xi_{M,M'} \oplus \xi_{N,M'} \oplus \xi_{M,N'} \oplus \xi_{N,N'}$ and $\xi_{M\oplus N} = \xi_{A,A}^{\otimes rr'}$. So $\xi_{M\oplus N,M'\oplus N'}$ is an isomorphism if and only if $\xi_{M,M'}, \xi_{N,M'}, \xi_{M,N'}$, and $\xi_{N,N'}$ are, or if and only if $\xi_{A,A}$ is. So it's enough to check that $\xi_{A,A}$ is an isomorphism. This is easy to check. □

Corollary 3.3.11. *The map*

$$M^{\vee} \otimes_A \mathrm{End}_S(\mathcal{M}) \otimes_A M \longrightarrow \mathrm{End}_S(\mathrm{Hom}_A(M, \mathcal{M}),)$$

$$l' \otimes \varphi \otimes m \longmapsto (f \mapsto (m' \mapsto l'(m')\varphi(f(m))))$$

is a well-defined isomorphism of rings.

Proof. It follows from Lemma 3.3.10 with $M' = M$ and $\mathcal{M}' = \mathcal{M}$ that it is a well-defined isomorphism of groups. The ring structure on the left-hand side is given by

$$(l'_1 \otimes \varphi_1 \otimes m_1) \cdot (l'_2 \otimes \varphi_2 \otimes m_2) = l'_1 \otimes \varphi_1 l'_2(m_1)\varphi_2 \otimes m_2.$$ □

$$
\begin{array}{ccc}
M'^{\vee} \otimes_A \operatorname{Hom}_S(\mathcal{M}, \mathcal{M}') \otimes_A (M \oplus N) & \xrightarrow{\sim} & (M'^{\vee} \otimes_A \operatorname{Hom}_S(\mathcal{M}, \mathcal{M}') \otimes_A M) \oplus (M'^{\vee} \otimes_A \operatorname{Hom}_S(\mathcal{M}, \mathcal{M}') \otimes_A N) \\
\downarrow{\scriptstyle \xi_{M\oplus N, M'}} & & \downarrow{\scriptstyle \xi_{M,M'} \oplus \xi_{N,M'}} \\
\operatorname{Hom}_S(\operatorname{Hom}_A(M \oplus N, \mathcal{M}), \operatorname{Hom}_A(M', \mathcal{M}')) & \xrightarrow{\sim} & \operatorname{Hom}_S(\operatorname{Hom}_A(M, \mathcal{M}), \operatorname{Hom}_A(M', \mathcal{M}')) \oplus \operatorname{Hom}_S(\operatorname{Hom}_A(N, \mathcal{M}), \operatorname{Hom}_A(M', \mathcal{M}'))
\end{array}
$$

$$
\begin{array}{ccc}
(M' \oplus N')^{\vee} \otimes_A \operatorname{Hom}_S(\mathcal{M}, \mathcal{M}') \otimes_A M & \xrightarrow{\sim} & (M'^{\vee} \otimes_A \operatorname{Hom}_S(\mathcal{M}, \mathcal{M}') \otimes_A M) \oplus (N'^{\vee} \otimes_A \operatorname{Hom}_S(\mathcal{M}, \mathcal{M}') \otimes_A M) \\
\downarrow{\scriptstyle \xi_{M,M'\oplus N'}} & & \downarrow{\scriptstyle \xi_{M,M'} \oplus \xi_{M,N'}} \\
\operatorname{Hom}_S(\operatorname{Hom}_A(MN, \mathcal{M}), \operatorname{Hom}_A(M' \oplus N', \mathcal{M}')) & \xrightarrow{\sim} & \operatorname{Hom}_S(\operatorname{Hom}_A(M, \mathcal{M}), \operatorname{Hom}_A(M', \mathcal{M}')) \oplus \operatorname{Hom}_S(\operatorname{Hom}_A(M, \mathcal{M}), \operatorname{Hom}_A(N', \mathcal{M}'))
\end{array}
$$

Figure 3.1: The commutative diagrams showing that $\xi_{M\oplus N,M'} = \xi_{M.M'}$ and $\xi_{M,M'\oplus N'} = \xi_{M,M'} \oplus \xi_{M,N'}$ The vertical isomorphisms come from the natural isomorphisms $(X \oplus Y) \otimes Z \cong (X \otimes Z) \oplus (Y \otimes Z)$ and $\operatorname{Hom}(X \oplus Y, Z) \cong \operatorname{Hom}(X, Z) \oplus \operatorname{Hom}(Y, Z)$.

Corollary 3.3.12. *Let $E, \sigma, \mathfrak{a}$ be as above. Then for any W-scheme S, we have*

$$\mathrm{End}_S(E^\sigma) \cong \mathfrak{a}^{-1} \otimes_{\mathcal{O}} \mathrm{End}_S(E) \otimes_{\mathcal{O}} \mathfrak{a}.$$

Proof. Applying Corollary 3.3.11 to $M = \mathfrak{a},\ \mathcal{M} = E$ and $A = \mathcal{O}$, we get

$$\mathrm{End}_S(\mathrm{Hom}_{\mathcal{O}}(\mathfrak{a}, E)) = \mathrm{Hom}_{\mathcal{O}}(\mathfrak{a}, \mathcal{O}) \otimes_{\mathcal{O}} \mathrm{End}_S(E) \otimes_{\mathcal{O}} \mathfrak{a}.$$

So we need to show that $\mathrm{Hom}_{\mathcal{O}}(\mathfrak{a}, \mathcal{O}) \cong \mathfrak{a}^{-1}$ as $\mathcal{O}$-modules and that $\mathrm{Hom}_{\mathcal{O}}(\mathfrak{a}, E) \cong E^\sigma$ as S-schemes.

Write $\mathfrak{a} = \frac{1}{\gamma}\langle \omega_1, \omega_2 \rangle$ with $\gamma, \omega_1, \omega_2 \in \mathcal{O}$. If $f \in \mathrm{Hom}_{\mathcal{O}}(\mathfrak{a}, \mathcal{O})$, then $\omega_1 f\left(\frac{\omega_2}{\gamma}\right) = \omega_2 f\left(\frac{\omega_1}{\gamma}\right)$, and so for $a = \frac{a_1\omega_1}{a_2\omega_2} \in \gamma$ we have $f\left(\frac{a_1\omega_1 + a_2\omega_2}{\gamma}\right) = \frac{a_1\omega_1}{\omega_1} f\left(\frac{\omega_1}{\gamma}\right) + \frac{a_2\omega_2}{\omega_2} f\left(\frac{\omega_2}{\gamma}\right) = ax$, where $x := \frac{\gamma}{\omega_1} f\left(\frac{\omega_1}{\gamma}\right) = \frac{\gamma}{\omega_2} f\left(\frac{\omega_2}{\gamma}\right)$ So we get mutually inverse bijections

$$\mathrm{Hom}_{\mathcal{O}}(\mathfrak{a}, \mathcal{O}) \longrightarrow \{x \in K : x\omega_1, x\omega_2 \in \mathcal{O}\} = \mathfrak{a}^{-1}$$

$$f \longmapsto \frac{\gamma}{\omega_1} f\left(\frac{\omega_1}{\gamma}\right) = \frac{\gamma}{\omega_2} f\left(\frac{\omega_2}{\gamma}\right)$$

$$(a \mapsto ax) \longmapsfrom x$$

Also, these bijections clearly respect the A-module structures, so $\mathrm{Hom}_{\mathcal{O}}(\mathfrak{a}, \mathcal{O}) \cong \mathfrak{a}^{-1}$.

For a proof that $\mathrm{Hom}_{\mathcal{O}}(\mathfrak{a}, E) \cong E^\sigma$, see [8, Corollary 7.11]. □

We also note that the right-hand in the lemma is a maximal order when $n = 1$ and $\mathfrak{a} = \mathcal{O}$:

Lemma 3.3.13. *The ring*

$$R_\lambda := \{[\alpha, \beta] \in B : \alpha, \beta \in D^{-1}, \alpha \equiv \lambda\beta \mod \mathcal{O}\}$$

is a maximal order in the quaternion algebra B. The only maximal orders of B containing the order

$$R := \{[\alpha, \beta] \in B : \alpha, \beta \in \mathcal{O}\}$$

are R_λ *and* $R_{-\lambda}$.

Proof. The elements $[1,0]$, $\left[\frac{1+\sqrt{-p}}{2},0\right]$, $[0,1]$, $\left[0,\frac{1+\sqrt{-p}}{2}\right]$ form a basis for R, and a quick calculation shows that $\mathrm{disc}\,(R)=p^2l^2$.

Moreover, we have a short exact sequence

$$0\to R\to R_\lambda \xrightarrow{\varphi} D^{-1}/\mathcal{O}\to 0,$$

where $R\to R_\lambda$ is inclusion and $\varphi([\alpha,\beta])=\beta+\mathcal{O}$. Indeed, φ is surjective since $\forall\beta\in D^{-1}$, $[\lambda\beta,\beta]\in R_\lambda$, $\mathrm{Ker}\,(\varphi)\supseteq R$, and $\mathrm{Ker}\,(\varphi)\subseteq\tilde{R}$, since if $[\alpha,\beta]\in\mathrm{Ker}\,(\varphi)$ then $\beta\in\mathcal{O}$ and so $\alpha\in\mathcal{O}$ as well since $\alpha\in\lambda\beta+\mathcal{O}$.

So $[R_\lambda:R]=\#D^{-1}/\mathcal{O}=p$, where the last equality is obtained by noting that $\frac{1}{\sqrt{-p}}\frac{1+\sqrt{-p}}{2}\equiv\frac{1}{\sqrt{-p}}\frac{p-1}{2} \mod\mathcal{O}$. Then $\mathrm{disc}\,(R_\lambda)=l^2$ since $\mathrm{disc}\,(R=[R_\lambda:R]^2\mathrm{disc}\,(R_\lambda)$, and so R_λ is a maximal order. The same argument shows that $R_{-\lambda}$ is a maximal order.

Now, note that $R_\lambda\neq R_{-\lambda}$, since otherwise we would have $\alpha\equiv\lambda\beta \mod\mathcal{O}\Leftrightarrow\alpha\equiv-\lambda\beta \mod\mathcal{O}$ and so $2\lambda\in\mathcal{O}$ for all $\beta\in D^{-1}$, but if we take $\beta=\frac{1}{\sqrt{-p}}$ then $2\lambda\beta=\frac{2\lambda}{\sqrt{-p}}\notin\mathcal{O}$ since $\lambda\not\equiv 0 \mod p$. Since $\frac{1}{\sqrt{-p}}\notin\mathbb{Z}_p$, we can use the same argument to show that $R_\lambda\otimes_{\mathbb{Z}}\mathbb{Z}_p\neq R_{-\lambda}\otimes_{\mathbb{Z}}\mathbb{Z}_p$. So $R_\lambda\otimes_{\mathbb{Z}}\mathbb{Z}_p$ and $R_{-\lambda}\otimes_{\mathbb{Z}}\mathbb{Z}_p$ are two maximal orders containing the order $R\otimes_{\mathbb{Z}}\mathbb{Z}_p$ of $B\otimes_{\mathbb{Q}}\mathbb{Q}_p$. Also, $R_\lambda\cap R_{-\lambda}=R$, since $[\alpha,\beta]\in R_\lambda\cap R_{-\lambda}$ if and only if $\alpha,\beta\in D^{-1}$ and $\alpha\equiv\lambda\beta\equiv-\lambda\beta \mod\mathcal{O}$, if and only if $\alpha\in\lambda\beta+\mathcal{O}$, $\beta\in D^{-1}$ and $2\lambda\beta\in\mathcal{O}$, if and only if $\alpha\in\lambda\beta+\mathcal{O}$ and $\beta\in\frac{1}{2\lambda}\mathcal{O}\cap D^{-1}=\mathcal{O}$. So $(R_\lambda\otimes_{\mathbb{Z}}\mathbb{Z}_p)\cap(R_{-\lambda}\otimes_{\mathbb{Z}}\mathbb{Z}_p)=(R_\lambda\cap R_{-\lambda})\otimes_{\mathbb{Z}}\mathbb{Z}_p=R\otimes_{\mathbb{Z}}\mathbb{Z}_p$.

Also, if $q\neq p$ is prime, then since p is invertible in $\mathbb{Z}_q$, we have $\mathrm{disc}\,(R_\lambda\otimes_{\mathbb{Z}}\mathbb{Z}_q)=\mathrm{disc}\,(R\otimes_{\mathbb{Z}}\mathbb{Z}_q)=(l^2)$ as ideals in $\mathbb{Z}_q$, and so $R_\lambda\otimes_{\mathbb{Z}}\mathbb{Z}_q=R\otimes_{\mathbb{Z}}\mathbb{Z}_q$. Similarly, $R_{-\lambda}\otimes_{\mathbb{Z}}\mathbb{Z}_q=R\otimes_{\mathbb{Z}}\mathbb{Z}_q$, and if Q is any maximal order of B containing R then $Q\otimes_{\mathbb{Z}}\mathbb{Z}_q=R\otimes_{\mathbb{Z}}\mathbb{Z}_q$.

Now, let Q be any maximal of B containing R. We just said that $Q\otimes_{\mathbb{Z}}\mathbb{Z}_q=R\otimes_{\mathbb{Z}}\mathbb{Z}_q=R_\lambda\otimes_{\mathbb{Z}}\mathbb{Z}_q=R\otimes_{\mathbb{Z}}\mathbb{Z}_q=R_{-\lambda}\otimes_{\mathbb{Z}}\mathbb{Z}_q=R\otimes_{\mathbb{Z}}\mathbb{Z}_q$ for any prime $q\neq p$. Also, we have $R\otimes_{\mathbb{Z}}\mathbb{Z}_p\subseteq(Q\otimes_{\mathbb{Z}}\mathbb{Z}_p)\cap(R_\lambda\otimes_{\mathbb{Z}}\mathbb{Z}_q)\subseteq R_\lambda\otimes_{\mathbb{Z}}\mathbb{Z}_p$, so either $(Q\otimes_{\mathbb{Z}}\mathbb{Z}_p)\cap(R_\lambda\otimes_{\mathbb{Z}}\mathbb{Z}_q)=R\otimes_{\mathbb{Z}}\mathbb{Z}_p$ or $(Q\otimes_{\mathbb{Z}}\mathbb{Z}_p)\cap(R_\lambda\otimes_{\mathbb{Z}}\mathbb{Z}_q)=(R_\lambda\otimes_{\mathbb{Z}}\mathbb{Z}_p)$ since $[R_\lambda\otimes_{\mathbb{Z}}\mathbb{Z}_p:R\otimes_{\mathbb{Z}}\mathbb{Z}_p]=p$ is prime. In the first case, since $R\otimes_{\mathbb{Z}}\mathbb{Z}_p$ is an Eichler order and $B\otimes_{\mathbb{Q}}\mathbb{Q}_p\cong M_2(\mathbb{Q})$, [28, Lemma 2.4] gives that

$Q \otimes_{\mathbb{Z}} \mathbb{Z}_p = R_{-\lambda} \otimes_{\mathbb{Z}} \mathbb{Z}_p$. Hence either $Q \otimes_{\mathbb{Z}} \mathbb{Z}_q = R_\lambda \otimes_{\mathbb{Z}} \mathbb{Z}_q, \forall q$ or $Q \otimes_{\mathbb{Z}} \mathbb{Z}_q = R_{-\lambda} \otimes_{\mathbb{Z}} \mathbb{Z}_q, \forall q$, and so either $Q = R_\lambda$ or $Q = R_{-\lambda}$. □

Also, note that $R_\lambda \cong R_{-\lambda}$ via the map $[\alpha, \beta] \mapsto [\alpha, -\beta]$. Indeed, this is clearly a bijection from R_λ to $R_{-\lambda}$, and $[\alpha, \beta] \cdot [\alpha', \beta'] = [\alpha\alpha' - l\beta\overline{\beta'}, \alpha\beta' + \beta\alpha']$ while $[\alpha, -\beta] \cdot [\alpha', -\beta'] = [\alpha\alpha' - l\beta\overline{\beta'}, -\alpha\beta' - \beta\alpha']$. Hence any maximal order of B containing R is isomorphic to R_λ.

Proof. (of Proposition 3.3.9) First, suppose that $[\mathfrak{a}] = [\mathcal{O}]$. Then $\mathrm{End}_{W/\pi}(E)$ contains $\mathrm{End}_W(E) = \mathcal{O}$, and by Skolem-Noether we can choose our inclusion $\mathrm{End}_{W/\pi}(E) \subseteq B$ so that $\mathcal{O}$ is sent to $\{[\alpha, 0] : \alpha \in \mathcal{O}\}$.

Since $l \neq p$, l must be inert in K, i.e. $l\mathcal{O}_K$ is prime. Hence l splits completely in H/K, and so if $v|l$ is a finite place of H then $H_v = K_l \cong \mathbb{Q}_{l^2}$, where $\mathbb{Q}_{l^2} = \mathbb{Q}_l[x]/(x^{p^2-1} - 1)$ is the unique unramified degree 2 extension of $\mathbb{Q}_l$. From general field theory, there is an automorphism $\sigma = \sigma(l\mathcal{O}_K/l\mathbb{Z}) \in \mathrm{Gal}(K/\mathbb{Q})$ such that σ induces the Frobenius automorphism $\varphi : x \to x^l$ on $\mathcal{O}_K/l\mathcal{O}_K = \mathbb{F}_{l^2}$ over $\mathbb{Z}/l\mathbb{Z}$. Since σ is nontrivial and $\mathrm{Gal}(K/\mathbb{Q}) = \{\pm\}$, σ must be complex conjugation. Also, σ extends to an automorphism $\tau : K_l \to K_l$, which must again induce φ on $\mathcal{O}_{K,l}/l\mathcal{O}_{K,l} = \mathcal{O}_K/l\mathcal{O}_K$.

Since $\overline{j(\mathcal{O})} = j(\overline{\mathcal{O}}) = j(\mathcal{O})$, also $j(\mathcal{O})^\tau = j(\mathcal{O})$ and so $E^\tau = E$ since there is a unique elliptic curve over W with j-invariant $j(\mathcal{O})$ and good reduction $\mod \pi$. Reducing $\mod \pi$, we have $E \mod \pi \cong E^{(l)} \mod \pi$, so $E \mod \pi$ is defined over $\mathbb{F}_l$ and $\mathrm{End}_{W/\pi}(E)$ contains the Frobenius endomorphism $\mathrm{Fr} : (x, y) \mapsto (x^l, y^l)$.

Also, if $\alpha \in \mathcal{O}$, we have $[\alpha]^\sigma = [\alpha^\sigma] = [\overline{\alpha}]$, since $[\alpha]^\sigma$ acts on $\mathrm{Lie}(E)$ by α^σ. Hence $\mathrm{Fr} \circ [\alpha] = [\overline{\alpha}] \circ \mathrm{Fr}$, since if $[\alpha]$ is given by $(x, y) \mapsto (f(x, y), g(x, y))$, then

$$\begin{aligned}
\mathrm{Fr}([\alpha](x, y)) &\equiv (f(x, y)^l, g(x, y)^l) \mod \pi \\
&\equiv (f^l(x^l, y^l), g^l(x^l, y^l)) \mod \pi \\
&\equiv (f^\sigma(x^l, y^l), g^\sigma(x^l, y^l) \mod \pi \\
&\equiv [\alpha]^\sigma(\mathrm{Fr}(x, y)) \mod \pi \\
&\equiv [\overline{\alpha}](\mathrm{Fr}(x, y)) \mod \pi.
\end{aligned}$$

Now, write $\mathrm{Fr} = [x, y]$ in $\mathrm{End}_{W/\pi}(E) \subseteq B$. The condition $\mathrm{Fr} \circ [\alpha] = [\overline{\alpha}] \circ \mathrm{Fr}$ becomes $[x\alpha, y\overline{\alpha}] = [x\overline{\alpha}, y\overline{\alpha}]$. So $x\alpha = x\overline{\alpha}, \forall \alpha \in \mathcal{O}$, and so $x = 0$. Then since E has supersingular reduction $\mod \pi$, Fr has trace 0 and so satisfies $\mathrm{Fr}^2 + l = 0$, i.e. $\mathrm{Nm}\,(y) = 1$, so y is a unit in $\mathcal{O}_K$. Since $K = \mathbb{Q}(\sqrt{-p})$ with $p \geq 2$, we have $\mathcal{O}_K \subseteq \{\pm 1, \pm\omega\}$ where ω is a third root of unity. If $y = \pm\omega$, then $K = \mathbb{Q}(\sqrt{-3})$ contains all the sixth roots of unity, and conjugation by $[x, 0]$ for some sixth root of unity x gives an automorphism of B fixing $\mathcal{O}$ and sending $[0, y]$ to $[0, 1]$. If $y = -1$, then $[\alpha, \beta] \mapsto [\alpha, -\beta]$ gives such an automorphism.

So we can choose the inclusion $\mathrm{End}_{W/\pi}(E) \subseteq B$ so that $\mathcal{O}$ is sent to $\{[\alpha, 0] : \alpha \in \mathcal{O}\} \subseteq B$ and Fr is sent to $[0, 1] \in B$. Then $\mathrm{End}_{W/\pi}(E)$ contains the order $R = \{[\alpha, \beta] : \alpha, \beta \in \mathcal{O}\}$, and so by Lemma 3.3.13 it is isomorphic to

$$R_\lambda := \{[\alpha, \beta] \in B : \alpha, \beta \in D^{-1}, \alpha \equiv \lambda\beta \mod \mathcal{O}\}.$$

For $n > 1$, [15, Proposition 3.3] gives

$$\begin{aligned}\mathrm{End}_{W/\pi^n}(E) &= \mathcal{O} + l^n \mathrm{End}_{W/\pi}(E) \\ &= \left\{[\alpha, \beta] : \alpha \in D^{-1}, \beta \in D^{-1}l^{n-1}, \alpha \equiv \lambda\beta \mod \mathcal{O}\right\}.\end{aligned}$$

Now, let $\mathfrak{a}$ be arbitrary. Since $j(E^\sigma) = \sigma(j(E)) = \sigma(j)$, the unique embedding $\mathbb{Q}(j(E^\sigma)) \hookrightarrow \mathbb{Q}_l$ is $\iota' = \iota \circ \sigma^{-1}$. So if v_2 is the place on H corresponding to one of the (equivalent) extensions of this embedding, we have $v_2(x) = v_1(\sigma^{-1}(x)) = v(x), \forall x \in H^\times$, so E^σ corresponds to the identity element in $\mathrm{Gal}\,(H/K)$ and hence to the ideal class $[\mathcal{O}] \in \mathrm{Cl}\,(\mathcal{O})$. So by the case $[\mathfrak{a}] = [\mathcal{O}]$, we have

$$\mathrm{End}_{W/\pi^n}(E^\sigma) = \left\{[\alpha, \beta] \in B : \alpha \in D^{-1}, \beta \in D^{-1}l^{n-1}, \alpha \equiv \lambda\beta \mod \mathcal{O}\right\}.$$

Applying Corollary 3.3.12 with $S = \mathrm{Spec}\,(W/\pi^n)$, we get that

$$\begin{aligned}
\mathrm{End}_{W/\pi^n}(E) &= \mathfrak{a}^{-1} \cdot \mathrm{End}_{W/\pi^n}(E^\sigma) \cdot \mathfrak{a} \\
&= \left\{[x,0] : x \in \mathfrak{a}^{-1}\right\} \cdot \left\{[\alpha,\beta] : \alpha \in D^{-1}, \beta \in D^{-1}l^{n-1}, \alpha \equiv \lambda\beta \mod \mathcal{O}\right\} \cdot \{[y,0] : y \in \mathfrak{a}\} \\
&= \left\{[xy\alpha, x\overline{y}\beta] : \alpha \in D^{-1}, \beta \in D^{-1}l^{n-1}, \alpha \equiv \lambda\beta \mod \mathcal{O}, x \in \mathfrak{a}^{-1}, y \in \mathfrak{a}\right\} \\
&= \left\{[\alpha,\beta] : \alpha \in D^{-1}, \beta \in D^{-1}l^{n-1}\overline{\mathfrak{a}}/\mathfrak{a}, \alpha \equiv \lambda\beta \mod \mathcal{O}\right\}.
\end{aligned}$$

Now we count the elements of S_n. We start by counting the number of elements with trace $\mathrm{Tr}\,(w)$ and norm $\mathrm{Nm}\,(w)$.

First, suppose $[\alpha,\beta] \in S_n$. Since $D^{-1} = \frac{1}{\sqrt{-p}}\mathcal{O}$ and $D^{-1}\overline{\mathfrak{a}}/\mathfrak{a} = \frac{1}{\sqrt{-p}}\overline{\mathfrak{a}}/\mathfrak{a}$, we can write

$$\alpha = \frac{x + t\sqrt{-p}}{2\sqrt{-p}}, \quad \beta = \frac{\gamma l^{n-1}}{\sqrt{-p}},$$

with $x, t \in \mathbb{Z}$ and $\gamma \in \overline{\mathfrak{a}}/\mathfrak{a}$. Then $\mathrm{Tr}\,([\alpha,\beta]) = \alpha + \overline{\alpha} = \mathrm{Tr}\,(\alpha) = t$, and so $t = \mathrm{Tr}\,(w)$. Also, note that $\mathrm{Nm}\,(\alpha) + l\mathrm{Nm}\,(\beta) = \mathrm{Nm}\,([\alpha,\beta]) = \mathrm{Nm}\,(w)$. Define $\mathfrak{b} := (\gamma)\mathfrak{a}/\overline{\mathfrak{a}}$, We want to check that $(x,\mathfrak{b}) \in T_n$.

Note that $[\overline{\mathfrak{a}}] = [\mathfrak{a}^{-1}]$ in $\mathrm{Cl}\,(\mathcal{O})$, since $\mathfrak{a}\overline{\mathfrak{a}} = (\mathrm{Nm}\,(\mathfrak{a})) \in [\mathcal{O}]$. Hence $\mathfrak{a}/\overline{\mathfrak{a}} \in [\mathfrak{a}^2]$, so also $\mathfrak{b} \in [\mathfrak{a}^2]$.

Also, we have $\mathrm{Nm}\,(\mathfrak{a}) = \mathrm{Nm}\,(\overline{\mathfrak{a}})$, and so

$$\begin{aligned}
\mathrm{Nm}\,(\mathfrak{b}) = \mathrm{Nm}\,((\gamma)) = \mathrm{Nm}\,(\gamma) = \mathrm{Nm}\left(\frac{\beta\sqrt{-p}}{l^{n-1}}\right) &= \frac{\mathrm{Nm}\,(\beta)p}{l^{2n-2}} = \frac{p(\mathrm{Nm}\,(w) - \mathrm{Nm}\,(\alpha))}{l^{2n-1}} \\
&= \frac{p}{l^{2n-1}}\left(\mathrm{Nm}\,(w) - \frac{\mathrm{Tr}\,(w)^2 + x^2}{4} - \frac{x^2}{4p}\right) = \frac{1}{4l^{2n-1}}\left(-p\mathrm{disc}\,(w) - x^2\right) \\
&= \frac{1}{4l^{2n-1}}\left(pq - x^2\right),
\end{aligned}$$

i.e. $x^2 + 4l^{2n-1}\mathrm{Nm}\,(\mathfrak{b}) = pq$.

Conversely, let $(x,\mathfrak{b}) \in T_n$. Note that since $[\mathfrak{b}] = [\mathfrak{a}^2]$ and $[\overline{\mathfrak{a}}] = [\mathfrak{a}^{-1}]$, we have $[\mathfrak{b}\overline{\mathfrak{a}}/\mathfrak{a}] = [\mathcal{O}]$, so $\mathfrak{b}\overline{\mathfrak{a}}/\mathfrak{a}$ is a principal ideal. If $\gamma \in K$ is a generator for $\mathfrak{b}\overline{\mathfrak{a}}/\mathfrak{a}$, we get an

element $[\alpha, \beta] \in B$ by taking

$$\alpha = \frac{x + \mathrm{Tr}(w)\sqrt{-p}}{2\sqrt{-p}} \text{ and } \beta = \frac{\gamma l^{n-1}}{\sqrt{-p}}.$$

Then $\mathrm{Tr}([\alpha, \beta]) = \mathrm{Tr}(w)$ and $\mathrm{Nm}([\alpha, \beta]) = \mathrm{Nm}(w)$. We have $w_1 = \#\mathcal{O}^\times$ choice of generator γ, so we want to determine for which γ we have $[\alpha, \beta] \in S_n$, i.e. $[\alpha, \beta] \in \mathrm{End}([\alpha, \beta])$ and $[\alpha, \beta] = w$ on $\mathrm{Lie}(E)$.

To check whether $[\alpha, \beta] \in \mathrm{End}_{W/\pi^n}(E)$, we need to check that $\alpha \equiv \lambda\beta \mod \mathcal{O}$. Note that

$$\begin{aligned} \gamma^2 &\equiv \gamma\overline{\gamma} \mod \mathcal{O} \\ &= \mathrm{Nm}(\gamma) = \mathrm{Nm}(\mathfrak{b}), \end{aligned}$$

and so

$$x^2 = pq - 4l^{2n-1}\mathrm{Nm}(\mathfrak{b}) \equiv -4l^{2n-1}\gamma^2 \mod \mathcal{O}.$$

Hence

$$\begin{aligned} l\beta^2 = -\frac{\gamma^2 l^{2n-1}}{p} &\equiv \frac{x^2}{4p} \mod \mathcal{O} \\ &\equiv -\alpha^2 \mod \mathcal{O}. \end{aligned}$$

So $\alpha \equiv \pm\lambda\beta \mod \mathcal{O}$. And if $\alpha \equiv \lambda\beta \mod \mathcal{O}$, then replacing γ by $-\gamma$ gives $\alpha \equiv -\lambda\beta \mod \mathcal{O}$. If $x \equiv 0 \mod p$, then we get $l\beta^2 \equiv -\alpha^2 \equiv 0 \mod \sqrt{-p}$, and so we get $\alpha \equiv \lambda\beta \equiv -\lambda\beta \equiv 0$, so any generator γ gives an an element of $\mathrm{End}_{W/\pi^n}(E)$. And if $x \neq 0 \mod p$, exactly half of the generators γ give such an element. So the number of $[\alpha, \beta] \in \mathrm{End}_{W/\pi^n}(E)$ corresponding to a pair $(x, \mathfrak{b}) \in T_n$ is

$$\begin{cases} w_1 \text{ if } p|x \\ \frac{w_1}{2} \text{ if } p \not| x. \end{cases}$$

Hence

$$\#\{[\alpha,\beta] \in \mathrm{End}_{W/\pi^n}(E) : \mathrm{Tr}([\alpha,\beta]) = \mathrm{Tr}(w), \mathrm{Nm}([\alpha,\beta]) = \mathrm{Nm}(w)\} = \frac{w_1}{2} \sum_{(x,\mathfrak{b})\in T_n} \delta(x).$$

Finally, since $\mathrm{Tr}([\alpha,\beta]) = \mathrm{Tr}(w)$ and $\mathrm{Nm}([\alpha,\beta]) = \mathrm{Nm}(w)$, $[\alpha,\beta]$ must act on $\mathrm{Lie}(E)$ by either w or $\overline{w}$. And if $[\alpha,\beta]$ acts by w, then its dual $[\alpha,\beta]^\wedge = [\overline{\alpha},-\beta]$ acts by $\overline{w}$ (to see that $[\overline{\alpha},-\beta$ is the dual endomorphism of $[\alpha,\beta]$, note that $[\alpha,\beta]\cdot[\overline{\alpha},-\beta] = [\alpha\overline{\alpha} + l\beta\overline{\beta}, 0]$ is the multiplication by $\mathrm{Nm}([\alpha,\beta])$ map). Since $\overline{w} \neq w \mod \pi^n$ by Hensel's lemma, and $[\overline{\alpha},-\beta]$ corresponds to the pair $(-x,\mathfrak{b})$ and the generator $-\gamma$ of $\mathfrak{b}\overline{\mathfrak{a}}/\mathfrak{a}$ (if $[\alpha,\beta]$ corresponds to $(x,\mathfrak{b})$ and the generator γ), exactly half of the endomorphisms found above give multiplication by w on $\mathrm{Lie}(E)$. Hence

$$\#S_n = \frac{w_1}{4} \sum_{(x,\mathfrak{b})\in T_n} \delta(x),$$

as desired. □

Proposition 3.3.14. *If $l|q$, then $e = 2$, and for $n \geq 1$ we have*

$$\mathrm{End}_{W/\pi^n}(E) = \{[\alpha,\beta] \in B : \alpha \in D^{-1}, \beta \in l^{m-1}\overline{\mathfrak{a}}/\mathfrak{a}, \alpha \equiv \beta \mod \mathcal{O}\},$$

where $m = \left\lfloor \frac{n+1}{2} \right\rfloor$, and

$$\#S_n = \begin{cases} \dfrac{w_1}{2} \displaystyle\sum_{(x,\mathfrak{b})\in T_1} \delta(x), & \text{if } n = 1 \\ 0, & \text{if } n > 1. \end{cases}$$

Proof. Since l is inert in $A_v/\mathbb{Q}_l$, the calculation in Proposition 3.3.9 gives

$$\mathrm{End}_{A_v/l^nA_v}(E) = \left\{[\alpha,\beta] \in B : \alpha \in D^{-1}, \beta \in D^{-1}l^{n-1}\overline{\mathfrak{a}}/\mathfrak{a}, \alpha \equiv \lambda\beta \mod \mathcal{O}\right\}.$$

Using the fact that W is a quadratic ramified extension of A_v, we calculate

$$\mathrm{End}_{W/\pi^n}(E) = \{[\alpha, \beta] \in B : \alpha \in D^{-1}, \beta \in l^{m-1}\overline{\mathfrak{a}}/\mathfrak{a}, \alpha \equiv \beta \mod \mathcal{O}\},$$

with $m = \left\lfloor \frac{n+1}{2} \right\rfloor$.

Now, as in the proof of Proposition 3.3.9, the elements of this ring with trace $\mathrm{Tr}(w)$ and norm $\mathrm{Nm}(w)$ give solutions to $x^2 + 4l^{2m-1}\mathrm{Nm}(\mathfrak{b}) = pq$, where $x \in \mathbb{Z}$ and $\mathfrak{b} \subseteq \mathcal{O}$ is an ideal in the same class as $[\mathfrak{a}]$, and this correspondence is $\frac{w_1}{2}\delta(x)$-to-1.

For $n > 2$, i.e. $m > 1$, we consider separately the cases $l \neq 2$ and $l = 2$:

Case 1: $l \neq 2$. Suppose that we had a solution $(x, \mathfrak{b})$ to $x^2 + 4l^{2m-1}\mathrm{Nm}(\mathfrak{b}) = pq$. Then since $l|q$, we must have $l|x$, hence $l^2|q$, which contradicts the fact that q is a fundamental discriminant.

Case 2: $l = 2$. Then since q is a fundamental discriminant and $2|q$, we can write $q = 4q'$ where q' is square-free and $q' \equiv 2, 3 \mod 4$. Suppose that we had a solution $(x, \mathfrak{b})$ to $x^2 + 2^{2m+1}\mathrm{Nm}(\mathfrak{b}) = pq = 4pq'$. Then $2|x$, say $x = 2x'$, and then $(x')^2 + 2^{2m-1}\mathrm{Nm}(\mathfrak{b}) = pq'$. We again divide into cases.

Case 2a: 2 divides q'. Then we must have $2|x$, and then $4|q'$, which contradicts the fact that q' is square-free.

Case 2a: 2 does not divide q'. Then $q' \equiv 3 \mod 4$. On the other hand, $(x')^2 + 2^{2m-1}\mathrm{Nm}(\mathfrak{b}) \equiv 0, 1 \mod 4$ since $m > 1$ and $(x')^2$ is a square. This is again a contradiction.

This shows that $S_n = \varnothing$ for $n > 2$. For $n = 2$, note that $\alpha_0 \in \mathrm{End}_{W/\pi^2}(E)$ acts on $\mathrm{Lie}(E)$ by an element of W/π, but $w \mod \pi^2$ does not lie in W/π, so we must have $S_2 = \varnothing$. Hence $S_n = \varnothing$ for all $n \geq 2$.

Finally, for $n = 1$, note that since $w \equiv \overline{w} \mod \pi$, any $\alpha_0 \in \mathrm{End}_{W/\pi}(E)$ with $\mathrm{Tr}(\alpha_0) = \mathrm{Tr}(w)$ and $\mathrm{Nm}(\alpha_0) = \mathrm{Nm}$) automatically acts by w on $\mathrm{Lie}(E)$. So

$$\#S_1 = \frac{w_1}{2} \sum_{(x,\mathfrak{b}) \in T_1} \delta(x),$$

as desired. □

Proposition 3.3.15. *If $l = p$, then $e = 1$, and for $n \geq 1$ we have*

$$\mathrm{End}_{W/\pi^n}(E) = \{[\alpha, \beta] \in B : \alpha \in \mathcal{O}, \beta \in D^{n-2}\overline{\mathfrak{a}}/\mathfrak{a}\},$$

and

$$\#S_n = \begin{cases} \frac{w_1}{2}\#T_1 = \frac{w_1}{2}\#\left\{(x, \mathfrak{b}) \in \mathbb{Z} \times [\mathfrak{a}^2] : x^2 + 4l\mathrm{Nm}(\mathfrak{b}) = pq \text{ and } p|x\right\}, & \text{if } n = 1 \\ 0, \text{ if } n > 1. \end{cases}$$

Proof. The formula for $\mathrm{End}_{W/\pi^n}(E)$ is obtained from a similar computation as was done in Proposition 3.3.9.

Suppose that $\alpha_0 = [\alpha, \beta] \in \mathrm{End}_{W/\pi^n}(E)$ with $\mathrm{Tr}(\alpha_0) = \mathrm{Tr}(w)$ and $\mathrm{Nm}(\alpha_0) = \mathrm{Nm}(w)$. Since $\mathrm{Tr}(\alpha) = \mathrm{Tr}(\alpha_0) = \mathrm{Tr}(w)$ and $\beta \in D^{n-2}\overline{\mathfrak{a}}/\mathfrak{a} = (\sqrt{-p})^{n-2}\mathfrak{a}/\overline{\mathfrak{a}}$, we can write $\alpha = \frac{\mathrm{Tr}(w)+z\sqrt{-p}}{2}$ and $\beta = \frac{\gamma(\sqrt{-p})^{n-1}}{\sqrt{-p}}$ with $z \in \mathbb{Z}$ and $\gamma \in \overline{\mathfrak{a}}/\mathfrak{a}$. Taking $x = pz$ and $\mathfrak{b} = (\gamma)\overline{\mathfrak{a}}/\mathfrak{a}$ gives a solution to $x^2 + 4p^n\mathrm{Nm}(\mathfrak{b}) = pq$. Conversely, any solution $(x, \mathfrak{b})$ gives w_1 choices of generator γ of $\mathfrak{b}$, and half of those generators will give an element of S_n since $w \not\equiv \overline{w}$ mod π. So

$$\#S_n = \frac{w_1}{2}\#T_n = \frac{w_1}{2}\#\left\{(x, \mathfrak{b}) \in \mathbb{Z} \times [\mathfrak{a}^2] : x^2 + 4p^n\mathrm{Nm}(\mathfrak{b}) = pq \text{ and } p|x\right\}.$$

If $n > 1$ then there are no solutions to $x^2 + 4p^n\mathrm{Nm}(\mathfrak{b}) = pq$ since $p \nmid q$. □

3.3.3 Completing the proof

As in § 3.3.2, let $d_1 = -p$, where p is prime, and $d_2 = -q$ be negative fundamental discriminants. Note that $p \equiv 3 \mod 4$, so by quadratic reciprocity we have

$$\varepsilon(p) = \left(\frac{-q}{p}\right) = \left(\frac{-p}{-q}\right) = \left(\frac{-p}{-1}\right)\left(\frac{-p}{q}\right) = -\varepsilon(q).$$

So we can assume without loss of generality that $\varepsilon(p) = 1$.

Now, for $m \geq 1$ and $\mathfrak{c}$ a fractional ideal of $\mathcal{O}$, define

$$r_{\mathfrak{c}}(m) := \#\{\mathfrak{b} \in [\mathfrak{c}] : \mathfrak{b} \in \mathcal{O}, \mathrm{Nm}\,(\mathfrak{b}) = m\} \tag{3.3.16}$$

and

$$R(m) := \#\{\mathfrak{c} \text{ an ideal of } \mathcal{O} : \mathrm{Nm}\,(\mathfrak{c}) = m\}. \tag{3.3.17}$$

Note that since $\#\mathrm{Cl}\,(\mathcal{O})$ is odd, the map $[\mathfrak{c}] \mapsto [\mathfrak{c}^2]$ is a bijection, so

$$\sum_{[\mathfrak{c}] \in \mathrm{Cl}\,(\mathcal{O})} r_{\mathfrak{c}^2}(m) = \sum_{[\mathfrak{c}] \in \mathrm{Cl}\,(\mathcal{O})} r_{\mathfrak{c}}(m) = R(m).$$

We combine Proposition 3.3.9, Proposition 3.3.14 and Proposition 3.3.15 to get the formula

$$\mathrm{ord}_v(\alpha) = \frac{1}{2} \sum_{x \in \mathbb{Z}} \sum_{n \geq 1} \delta(x) r_{\mathfrak{a}^2} \left(\frac{pq - x^2}{4l^n} \right).$$

Using the fact that $J(-p,-q) = \mathrm{Nm}_{H/K}(\alpha)$, we get

$$\begin{aligned}
\mathrm{ord}_v(J(-p,-q)) &= \sum_{\sigma \in \mathrm{Gal}\,(H/K)} \mathrm{ord}_v(\sigma(\alpha)) \\
&= \frac{1}{2} \sum_{\sigma \in \mathrm{Gal}\,(H/K)} \sum_{x \in \mathbb{Z}} \sum_{n \geq 1} \delta(x) r_{\mathfrak{a}^2_{\sigma(j(E))}} \left(\frac{pq - x^2}{4l^n} \right) \\
&= \frac{1}{2} \sum_{\sigma \in \mathrm{Gal}\,(H/K)} \sum_{x \in \mathbb{Z}} \sum_{n \geq 1} \delta(x) r_{(\mathfrak{a}^\sigma)^2} \left(\frac{pq - x^2}{4l^n} \right) \\
&= \frac{1}{2} \sum_{\mathfrak{c} \in \mathrm{Cl}\,(\mathcal{O})} \sum_{x \in \mathbb{Z}} \sum_{n \geq 1} \delta(x) r_{\mathfrak{c}^2} \left(\frac{pq - x^2}{4l^n} \right) \\
&= \frac{1}{2} \sum_{x \in \mathbb{Z}} \sum_{n \geq 1} \delta(x) R \left(\frac{pq - x^2}{4l^n} \right).
\end{aligned}$$

To complete the proof, we use the fact that

$$R(m) = \sum_{\substack{n \mid m \\ n > 0}} \left(\frac{n}{p} \right).$$

This gives

$$\mathrm{ord}_v J(-p,-q) = \frac{1}{2}\sum_{x\in\mathbb{Z}}\sum_{n\geq 1}\delta(x)\sum_{\substack{n'|\frac{pq-x^2}{4l^n}\\ n'>0}}\left(\frac{n'}{p}\right),$$

so

$$\mathrm{ord}_v J(-p,-q)^2 = \sum_{x\in\mathbb{Z}}\sum_{n\geq 1}\delta(x)\sum_{\substack{n'|\frac{pq-x^2}{4l^n}\\ n'>0}}\left(\frac{n'}{p}\right),$$

On the other hand, let

$$P := \prod_{\substack{x,n,n'\in\mathbb{Z}\\ n,n'>0\\ x^2+4nn'=pq}} n^{\varepsilon(n')}.$$

Then we have

$$\begin{aligned}
\mathrm{ord}_v P &= \sum_{\substack{x,n,n'\in\mathbb{Z}\\ n,n'>0\\ x^2+4nn'=pq}} \varepsilon(n')\mathrm{ord}_v n \\
&= \sum_{\substack{x,n,n'\in\mathbb{Z}\\ n,n'>0\\ x^2+4nn'=pq}} \sum_{\substack{N>0\\ l^N|n}} \varepsilon(n') \\
&= \sum_{x\in\mathbb{Z}} \sum_{\substack{n,n'>0\\ x^2+4nn'=pq}} \sum_{\substack{m,N>0\\ n=l^N m}} \varepsilon(n') \\
&= \sum_{x\in\mathbb{Z}} \sum_{m,N>0} \sum_{\substack{n'>0\\ x^2+4l^N mn'=pq}} \varepsilon(n') \\
&= \sum_{x\in\mathbb{Z}}\sum_{n>0}\sum_{\substack{n'>0\\ n'|\frac{pq-x^2}{4l^n}}} \varepsilon(n').
\end{aligned}$$

To complete the proof, I'll show that for every $x\in\mathbb{Z}$ and $n\geq 1$ such that $4l^n|(pq-x^2)$,

we have

$$\sum_{\substack{n'>0 \\ n'|\frac{pq-x^2}{4l^n}}} \varepsilon(n') = \mathfrak{d}(x) \sum_{\substack{n'|\frac{pq-x^2}{4l^n} \\ n'>0}} \left(\frac{n'}{p}\right). \tag{3.3.18}$$

I'll handle the cases $p|x$ and $p \not| x$ separately.

Case 1: p does not divide x. Then also p does not divide $\frac{pq-x^2}{4l^n}$. So for each n' dividing $\frac{pq-x^2}{4l^n}$, we have $\gcd(-p, n') = 1$, and so (by quadratic reciprocity)

$$\varepsilon(n') = \left(\frac{-p}{n'}\right) = \left(\frac{n'}{p}\right).$$

Summing over all such n' and using the fact that $\mathfrak{d}(x) = 1$ gives Equation (3.3.18).

Case 2: p divides x. Then p^2 divides x^2, and so p divides $\frac{pq-x^2}{4l^n}$ with multiplicity one. So we can write

$$\begin{aligned}
\sum_{\substack{n'>0 \\ n'|\frac{pq-x^2}{4l^n}}} \varepsilon(n') &= \sum_{\substack{n'>0 \\ n'|\frac{pq-x^2}{4l^n} \\ \gcd(p,n')=1}} (\varepsilon(n') + \varepsilon(pn')) \\
&= \sum_{\substack{n'>0 \\ n'|\frac{pq-x^2}{4l^n} \\ \gcd(p,n')=1}} 2\varepsilon(n') && \text{by multiplicativity of } \varepsilon \text{ and since } \varepsilon(p) = 1, \\
&= \sum_{\substack{n'>0 \\ n'|\frac{pq-x^2}{4l^n} \\ \gcd(p,n')=1}} \delta(x) \left(\frac{-p}{n'}\right) \\
&= \sum_{\substack{n'>0 \\ n'|\frac{pq-x^2}{4l^n} \\ \gcd(p,n')=1}} \delta(x) \left(\frac{n'}{p}\right) && \text{by quadratic reciprocity} \\
&= \sum_{\substack{n'>0 \\ n'|\frac{pq-x^2}{4l^n}}} \delta(x) \left(\frac{n'}{p}\right) && \text{since } \left(\frac{n'}{p}\right) = 0 \text{ if } p|n'.
\end{aligned}$$

This shows that $\operatorname{ord}_v J(-p,-q)^2 = \operatorname{ord}_v P$ for every finite place v of H, and so $J(-p,-q)^2 = \pm P$, as desired.

Chapter 4

Two applications of Gross and Zagier's formula

In this chapter, I will give two consequences of Gross and Zagier's factorization formula (Theorem 3.1.5). First, in § 4.1, I will give a bound on $v(j)$, where j is a singular modulus, in terms of the discriminant of j, and v is a valuation above 2. Second, in § 4.2, I will give a factorization formula for norms of differences of singular lambda values, similar to Gross and Zagier's formula for singular moduli.

4.1 Bounding the valuation of singular moduli

We start by establishing some notation. Let

1. K be a quadratic imaginary field of discriminant $d_K < 0$,
2. $\mathcal{O}_K = \mathbb{Z}[t]$ be the ring of integers of K,
3. h be the class number of K,
4. H be the Hilbert class field of K,
5. v be a non-archimedean valuation of H dividing 2,
6. A_v be the completion of the maximal unramified extension of the ring of v-integers of H,

7. $W = A_v[\omega]$, where $\omega = \frac{-1+\sqrt{-3}}{2}$,

8. π be a uniformizer for W,

9. E be an elliptic curve over W with complex multiplication by $\mathcal{O}_K$, and

10. $j = j(E) \in H$ be the j-invariant of E.

A natural question to ask is how large the valuation $v(j)$ of j can be. Moreover, how does $v(j)$ compare to the class number h of K?

Berwick's congruences (see Theorem 5.1.2) tell us that $v(j) \leq 6$ unless 2 is inert in K, i.e. unless $d_K \equiv 5 \mod 8$, in which case $v(j) \geq 15$.

Assume that 2 *is inert in* K. Also assume that $d_K < -4$, since if $d_K = -3$ then $j = 0$, and that d_K is prime, so that we may use results form § 3.3.2.

Now, let E_0 be an elliptic curve over W with complex multiplication by $\mathbb{Z}[\omega]$, where $\omega = \frac{-1+\sqrt{-3}}{2}$. Note that $j(E_0) = 0$. So by Proposition 3.2.8, we have

$$v(j) = v\left(j - j(E_0)\right) = \frac{1}{2}\sum_{n\geq 1} \#\mathrm{Iso}_{W/\pi^n}(E, E_0).$$

Also, note that if $E \cong E_0 \mod \pi^n$, then (see, for example, [26, §III, Theorem 10.1])

$$2 \leq \#\mathrm{Iso}_{W/\pi^n}(E, E_0) \leq 24,$$

and so

$$N \leq v(j) \leq 12N, \tag{4.1.1}$$

where

$$N := \max\{n : E \cong E_0 \mod \pi^n\}. \tag{4.1.2}$$

From here, I will bound N using two methods. First, in § 4.1.1, I will use results from [17] to reduce the problem of finding isomorphisms $E \cong E_0 \mod \pi^n$ to finding pairs $(x, \mathfrak{b})$, where $x \in \mathbb{Z}$ and $\mathfrak{b}$ is an ideal of $\mathcal{O}_K$ in a fixed ideal class, such that

$$x^2 + 2^{2n+1}\mathrm{Nm}\,(\mathfrak{b}) = -3d_K.$$

From there, it will be easy to bound n in terms of d_K, since $x^2 \geq 0$ and $\mathrm{Nm}(\mathfrak{b}) \geq 1$. Second, in § 4.1.2, I will bound N using volume estimates for orders in quaternion algebras, proven in [14].

Both methods give remarkably similar upper bounds. The bound of § 4.1.1, which is somewhat better, is given in the following theorem.

Theorem 4.1.3. *Let K be a quadratic imaginary field of prime fundamental discriminant d_K. Let $j = j(E)$, where E is an elliptic curve over W with complex multiplication by $\mathcal{O}_K$. Then*

$$v(j) \leq 6 \log_2 |d_K| + 6(\log_2 3 - 1).$$

Note that we can drop the condition that 2 is inert in K, since if 2 is split or ramified in K then

$$v(j) \leq 6 \leq 6 \log_2 |d_K| + 6(\log_2 3 - 1).$$

Finally, we can use this result, along with known bounds on the class number h of K to answer the second question asked at the beginning of this section, namely how $v(j)$ compares to h. Let χ_{d_K} be the Dirichlet character $\chi_{d_K}(n) = \left(\frac{d_K}{n}\right)$. Recall that the L-function of χ_{d_K} is

$$L(s, \chi_{d_K}) = \sum_{n \geq 1} \frac{\chi_{d_K}(n)}{n^s}. \tag{4.1.4}$$

Corollary 4.1.5. *Let K be a quadratic imaginary field of prime fundamental discriminant d_K and class number h, and let $j = j(E)$, where E is an elliptic curve over W with complex multiplication by $\mathcal{O}_K$. Suppose that the Riemann Hypothesis for $L(s, \chi_{d_K})$ holds, i.e. that all the zeroes of $L(s, \chi_{d_K})$ satisfy $\mathrm{Re}(s) = \frac{1}{2}$. Then there is a constant $c > 0$, which does not depend on d_K, such that*

$$\frac{v(j)}{h} < c.$$

Proof. By a result of Dirichlet, we can write the class number of K as

$$h = \frac{w(d_K)\sqrt{|d_K|} L(1, \chi_{d_K})}{2},$$

where

$$w(d_K) = \begin{cases} 2, & \text{if } d_K < -4, \\ 4, & \text{if } d_K = -4, \text{ and} \\ 6, & \text{if } d_K = -3. \end{cases}$$

Moreover, by [22, Theorem 1], assuming that the Riemann Hypothesis for $L(s, \chi_{d_K})$ holds, we have

$$L(1, \chi_{d_K}) > \frac{c_0}{\log\log|d_K|}$$

for some constant $c_0 > 0$ not depending on d_K. Hence

$$h \geq \frac{c_0 w(d_K)\sqrt{|d_K|}}{2\log\log|d_K|},$$

and so

$$\frac{v(j)}{h} \leq \frac{12\left(\log_2|d_K| + \log_2 3 - 1\right)\log\log|d_K|}{c_0 w(d_K)\sqrt{|d_K|}}.$$

The right-hand side goes to zero as $d_K \to \infty$, hence is bounded. □

4.1.1 An upper bound using lemmas of Gross and Zagier

Fix $n \geq 1$, and suppose that $E \cong E_0 \mod \pi^n$. Since $\mathrm{Tr}(\omega) = -1$ and $\mathrm{Nm}(\omega) = 1$, we define

$$S_n := \{\alpha_0 \in \mathrm{End}_{W/\pi^n}(E) : \mathrm{Tr}(\alpha_0) = \mathrm{Tr}(\omega) = -1, \mathrm{Nm}(\alpha_0) = \mathrm{Nm}(\omega) = 1, \alpha_0 = \omega \text{ on } \mathrm{Lie}(E)\},$$

as in § 3.3.1. By Proposition 3.3.2 with $d_2 = -3$, we have

$$\#S_n = \frac{1}{6}\#\mathrm{Iso}_{W/\pi^n}(E, E_0).$$

In particular, this means that $E \cong E_0 \mod \pi^n$ if and only if S_n is non-empty.

Moreover, since 2 is inert in K, we have $\left(\frac{d_K}{2}\right) = -1$, so by Proposition 3.3.9,

$$\#S_n = \frac{\#\mathcal{O}_K^\times}{2} \sum_{(x,\mathfrak{b})\in T_n} \delta(x),$$

where

$$T_n = \{(x,\mathfrak{b}) \in \mathbb{Z} \times [\mathfrak{a}^2] : \mathfrak{b} \subseteq \mathcal{O}_K, x^2 + 2^{2n+1}\mathrm{Nm}\,(\mathfrak{b}) = -3d_K\}$$

and

$$\delta(x) = \begin{cases} 2 & \text{if } d_K | x, \text{ and} \\ 1 & \text{otherwise.} \end{cases}$$

Here, $\mathfrak{a}$ is the fractional ideal defined in § 3.3.2. Hence S_n is non-empty if and only T_n is.

So if $E \cong E_0 \mod \pi^n$, then T_n is non-empty, and so there exists $x \in \mathbb{Z}$ and an ideal $\mathfrak{b}$ of $\mathcal{O}_K$ (in the same class as $[\mathfrak{a}^2]$) such that

$$x^2 + 2^{2n+1}\mathrm{Nm}\,(\mathfrak{b}) = -3d_K.$$

Note that $x^2 \geq 0$, and $\mathrm{Nm}\,(\mathfrak{b}) \geq 1$, so we get

$$2^{2n+1} \leq -3d_K = 3|d_K|,$$

i.e.

$$n \leq \frac{1}{2}\left(\log_2 |d_K| + \log_2 3 - 1\right).$$

Hence also

$$N \leq \frac{1}{2}\left(\log_2 |d_K| + \log_2 3 - 1\right),$$

and so

$$v(j) \leq 12N \leq 6\left(\log_2 |d_K| + \log_2 3 - 1\right).$$

This proves Theorem 4.1.3.

4.1.2 An upper bound using volume estimates

Fix $n \geq 1$, and suppose that $E \cong E_0 \mod \pi^n$. Write

$$R = \mathrm{End}_{W/\pi}(E_0)$$

and

$$R_n = \mathrm{End}_{W/\pi^n}(E_0).$$

Since E_0 has supersingular reduction mod π, R is a maximal order in the quaternion algebra $B = B_{2,\infty}$ ramified at 2 and ∞. Also, by [15],

$$R_n = \mathbb{Z}[\omega] + 2^{n-1}R,$$

and so $\mathbb{Z}[\omega] \subseteq R_n$. Moreover, since $E \cong E_0 \mod \pi^n$, we have $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{d_K}}{2}\right] \subseteq R_n$, so

$$\mathbb{Z}\left[\frac{1+\sqrt{d_K}}{2}, \omega\right] = \mathbb{Z} + \mathbb{Z}\frac{1+\sqrt{d_K}}{2} + \mathbb{Z}\omega + \mathbb{Z}\frac{1+\sqrt{d_K}}{2} \cdot \omega \subseteq R_n.$$

Hence

$$\mathrm{covol}\,(R_n) \leq \mathrm{covol}\left(\mathbb{Z}\left[\frac{1+\sqrt{-d_K}}{2}, \omega\right]\right).$$

On the one hand, by [14, Lemma 2.1.1], we have

$$\mathrm{covol}\left(\mathbb{Z}\left[\frac{1+\sqrt{d_K}}{2}, \omega\right]\right) \leq 4\mathrm{Nm}\left(\frac{1+\sqrt{d_K}}{2}\right)\mathrm{Nm}\,(\omega) = 1 + |d_K|.$$

On the other hand, we can write

$$B = \left\{ [\alpha, \beta] = \begin{pmatrix} \alpha & \beta \\ -2\overline{\beta} & \overline{\alpha} \end{pmatrix} \right\} \subseteq M_2(K),$$

and, by Proposition 3.3.9,

$$\begin{aligned} R_n &= \{[\alpha,\beta] \in B : \alpha \in \frac{1}{\sqrt{-3}}\mathbb{Z}[\omega], \beta \in \frac{2^{n-1}}{\sqrt{-3}}\mathbb{Z}[\omega], \alpha \equiv \beta \mod \mathbb{Z}[\omega]\} \\ &= \mathbb{Z}[1,0] + \mathbb{Z}[\omega,0] + \mathbb{Z}\left[2^{n-1}, 2^{n-1}\right] + \mathbb{Z}\left[\frac{2^{n-1}\omega}{\sqrt{-3}}, \frac{2^{n-1}\omega}{\sqrt{-3}}\right]. \end{aligned}$$

By [29, Ch. 17, Exercise 7] and a calculation using the fact that $\mathrm{Tr}\,[\alpha,\beta] = \mathrm{Tr}\,(\alpha)$, we get

$$\mathrm{covol}\,(R_n) = 4 \cdot \mathrm{discrd}\,(R_n) = 2^{2n-1}.$$

Hence

$$2^{2n-1} \leq 1 + |d_K|,$$

i.e.

$$n \leq \frac{1}{2}\left(1 + \log_2\left(|d_K| + 1\right)\right).$$

Applying this to $N = \max\{n : E \cong E_0 \mod \pi^n\}$ and using Equation (4.1.1), we obtain

$$v(j) \leq 6 + 6\log_2(|d_K| + 1). \tag{4.1.6}$$

4.2 An analogue of Gross-Zagier's factorization formula for the modular lambda function

4.2.1 Introduction

In this section, I will study an analogue of Gross-Zagier's product $J(d_1, d_2)$ for the modular lambda function λ. Let d_1, d_2 be coprime negative fundamental discriminants. For $i = 1, 2$, let K_i be the quadratic imaginary field with discriminant d_i, and let $w_i = \#\mathcal{O}_{K_i}^{\times}$. Define

$$\Lambda(d_1, d_2) := \prod_{\substack{\tau_i \in \Gamma(2)\backslash\mathcal{H} \\ \mathrm{disc}\,\tau_i = d_i}} (\lambda(\tau_1) - \lambda(\tau_2)). \tag{4.2.1}$$

A priori, $\Lambda(d_1, d_2)$ lies in the field

$$L = \mathbb{Q}(\sqrt{d_i}, \lambda(\tau_i) : \operatorname{disc} \tau_i = d_i, i = 1, 2),$$

but in fact we have:

Lemma 4.2.2. $\Lambda(d_1, d_2) \in \mathbb{Q}$.

Proof. Let

$$F_{d_2}(X) = \prod_{\substack{\tau_2 \in \Gamma(2)\backslash\mathcal{H} \\ \operatorname{disc}(\tau_2) = d_2}} (X - \lambda(\tau_2)) \in L[X].$$

Note that if $\tau_2 \in \Gamma(2)\backslash\mathcal{H}$ is imaginary quadratic of discriminant d_2, then $\lambda(\tau_2)$ is an algebraic number, and it's Galois conjugates over $\mathbb{Q}$ are all of the form $\lambda(\tau_2')$, with $\tau_2' \in \Gamma(2)\backslash\mathcal{H}$ imaginary quadratic of discriminant d_2. So $F_{d_2}(X)$ is a product of minimal polynomials over $\mathbb{Q}$ of algebraic numbers of the form $\lambda(\tau_2)$, hence $F_{d_2}(X) \in \mathbb{Q}[X]$.

Now, we can write

$$\Lambda(d_1, d_2) = \prod_{\substack{\tau_1 \in \Gamma(2)\backslash\mathcal{H} \\ \operatorname{disc}(\tau_1) = d_1}} F_{d_2}(\lambda(\tau_1)).$$

If $\tau_1 \in \Gamma(2)\backslash\mathcal{H}$ is imaginary quadratic of discriminant d_1, then the Galois conjugates of $\lambda(\tau_1)$ over $\mathbb{Q}$ are of the form $\lambda(\tau_1')$, with $\tau_1' \in \Gamma(2)\backslash\mathcal{H}$ imaginary quadratic of discriminant d_1. So the Galois conjugates of $F_{d_2}(\lambda(\tau_1))$ are of the form $F_{d_2}(\lambda(\tau_1'))$. Hence $\Lambda(d_1, d_2)$ is a product of norms over $\mathbb{Q}$ of algebraic numbers of the form $F_{d_2}(\lambda(\tau_1))$. So $\Lambda(d_1, d_2) \in \mathbb{Q}$, as desired. □

It is natural to ask whether we can find a formula for $\Lambda(d_1, d_2)$ similar to Gross-Zagier's formula for $J(d_1, d_2)$. In this section, I will do so, by proving the following Theorem:

Theorem 4.2.3. $\Lambda(d_1, d_2) = 2^m J(d_1, d_2)^6$ *for some* $m \in \mathbb{Z}$.

4.2.2 Calculating $v(\lambda - \lambda')$

In order to prove Theorem 4.2.3, I will begin by giving an analogue of Proposition 3.2.8 for the modular lambda function.

Let W be a complete discrete valuation ring with with uniformizer π such that

1. its field of fractions K has characteristic 0, and

2. its residue field $k = W/\pi$ is algebraically closed of characteristic $l > 2$.

For example, we could take W to be the ring of integers of of $\widehat{\mathbb{Q}}_l^{\mathrm{ur}} \cdot \mathcal{L}$, where $\widehat{\mathbb{Q}}_l^{\mathrm{ur}}$ is the completion of the maximal unramified extension of $\mathbb{Q}_l$ and $\mathcal{L}$ is the completion of any number field at a prime $\mathfrak{p}$ dividing l. Let v be the valuation corresponding to π, normalized so that $v(\pi) = W$.

Let (E, P_1, P_2) and (E', P_1', P_2') be enhanced elliptic curves for $\Gamma(2)$ over W which have good reduction modulo π. Let $\lambda = \lambda(E, P_1, P_2)$ and $\lambda' = \lambda(E', P_1', P_2')$. Since 2 is invertible in W, we can find a Weierstrass equation for E of the form

$$E : y^2 = x^3 + a_2x^2 + a_4x + a_6. \tag{4.2.4}$$

Since E has good reduction modulo π and k is algebraically closed, $x^3 + a_2x + a_4x + a_6$ factors into distinct roots over k, and hence over W by Hensel's lemma. So we can write the Weierstrass equation in Equation (4.2.4) as

$$E : y^2 = (x - e_1)(x - e_2)(x - e_3),$$

where $e_1, e_2, e_3 \in W$ are distinct. Since E has good reduction modulo π, we must have $x_i - x_j \not\equiv 0 \mod \pi$. Note that $(e_i, 0)$, $i = 1, 2, 3$, are the points of order 2 of E, and we can assume, by reordering the x_i's, that $P_1 = (e_1, 0)$ and $P_2 = (e_2, 0)$. Then, as in § 2.1, (E, P_1, P_2) is isomorphic over $\overline{K}$ to the enhanced elliptic curve $(E_\lambda, (1, 0), (0, 0))$ via the map

$$(x, y) \mapsto \left(\frac{x - e_2}{e_1 - e_2}, \frac{y}{(e_1 - e_2)^{3/2}} \right),$$

where E_λ is the elliptic curve over W given by the Weierstrass equation

$$E_\lambda : y^2 = x(x - 1)(x - \lambda).$$

Moreover, Hensel's lemma gives that $(e_1 - e_2)^{1/2} \in W$, and so (E, P_1, P_2) is in fact isomorphic to $(E_\lambda, (1,0), (0,0))$.

A similar argument show that (E', P_1', P_2') is isomorphic to the enhanced elliptic curve $(E_{\lambda'}, (1,0), (0,0))$ over W. We are now ready to prove the following result.

Proposition 4.2.5. *Using the notation introduced above, we have*

$$v(\lambda - \lambda') = \frac{1}{2} \sum_{n \geq 1} \#\mathrm{Iso}_{W/\pi^n}((E, P_1, P_2), (E', P_1', P_2')),$$

where for $n \geq 1$, $\mathrm{Iso}_{W/\pi^n}((E, P_1, P_2), (E', P_1', P_2'))$ *denotes the set of isomorphisms of enhanced elliptic curves for* $\Gamma(2)$ *from* $(E, P_1, P_2) \mod \pi^n$ *to* $(E', P_1', P_2') \mod \pi^n$.

Proof. By our above discussion, we can assume that $(E, P_1, P_2) = (E_\lambda, (1,0), (0,0))$ and $(E', P_1', P_2') = (E_{\lambda'}, (1,0), (0,0))$. So write $\overline{E}_\lambda = E_\lambda \mod \pi^n$ and $\overline{E}_{\lambda'} = E_{\lambda'} \mod \pi^n$. By Remark 2.1.8, any isomorphism $f : \big(\overline{E}_\lambda, (1,0), (0,0)\big) \xrightarrow{\sim} \big(\overline{E}_{\lambda'}, (1,0), (0,0)\big)$ of enhanced elliptic curves is of the form

$$(x, y) \to (x, \pm y).$$

If $\lambda \equiv \lambda' \mod \pi^n$, then both of these maps define isomorphisms from $\big(\overline{E}_\lambda, (1,0), (0,0)\big)$ to $\big(\overline{E}_{\lambda'}, (1,0), (0,0)\big)$. On the other hand, if $\lambda \not\equiv \lambda' \mod \pi^n$, then we cannot have $\big(\overline{E}_\lambda, (1,0), (0,0)\big) \cong \big(\overline{E}_{\lambda'}, (1,0), (0,0)\big)$. So

$$\#\mathrm{Iso}_{W/\pi^n}((E, P_1, P_2), (E', P_1', P_2')) = \begin{cases} 0, & \text{if } \lambda \not\equiv \lambda' \mod \pi^n, \\ 2, & \text{if } \lambda \equiv \lambda' \mod \pi^n. \end{cases}$$

Proposition 4.2.5 follows from this and the fact that

$$v(\lambda - \lambda') = \sum_{\substack{n \geq 1 \\ \pi^n | (\lambda - \lambda')}} 1. \qquad \square$$

4.2.3 Proving Theorem 4.2.3

As before, let d_1, d_2 be coprime negative fundamental discriminants. Recall that our goal is to prove the identity

$$\Lambda(d_1, d_2) = 2^m J(d_1, d_2)^6,$$

for some $m \in \mathbb{Z}$. Since $\Lambda(d_1, d_2), J(d_1, d_2) \in \mathbb{Q}$, and any 2-unit of $\mathbb{Q}$ is of the form 2^m with $m \in \mathbb{Z}$, we need to show that

$$v(\Lambda(d_1, d_2)) = 6v(J(d_1, d_2))$$

for any non-archimedean valuation v of

$$L = \mathbb{Q}(\sqrt{-d_i}, \lambda(\tau_i) : \mathrm{disc}\,(\tau_i) = d_i, i = 1, 2)$$

not dividing 2.

For $i = 1, 2$, let $K_i = \mathbb{Q}(\sqrt{d_i})$, and let $w_i = \#\mathcal{O}_{K_i}^\times$. Fix a finite place v of L not dividing 2. We need to show that

$$\sum_{\substack{\tau_i \in \Gamma(2)\backslash\mathcal{H} \\ \mathrm{disc}\,(\tau_i) = d_i}} v(\lambda(\tau_1) - \lambda(\tau_2)) = \frac{24}{w_1 w_2} \sum_{\substack{\tau_i \in \mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H} \\ \mathrm{disc}\,(\tau_i) = d_i}} v(j(\tau_1) - j(\tau_2)). \tag{4.2.6}$$

Let W be the completion of the maximal unramified extension of the ring of v-integers of L. Let

1. π be a uniformizer of W, chosen so that $v(\pi) = 1$,
2. K be the field of fractions of W, and
3. $k = W/(\pi)$ be the residue field of W.

Fix $\tau_1 \in \Gamma(2)\backslash\mathcal{H}$ of discriminant d_1. Write $j = j(\tau_1)$ and $\lambda = \lambda(\tau_1)$. By the same argument as in § 3.3.1, there exists an elliptic curve E over W with j-invariant $j(E) = j$, complex multiplication by $\mathcal{O}_{K_1}$ and good reduction modulo π. Then, by the same

argument as in § 4.2.2, E has a Weierstrass equation of the form

$$E : y^2 = (x - e_1)(x - e_2)(x - e_3)$$

with $e_1, e_2, e_3 \in W$. Note that $\lambda = \lambda(E, P_1, P_2)$ for some choice of $\Gamma(2)$-structure (P_1, P_2) on E. So, by reordering the e_i's, we can assume that $\lambda = \lambda(E, (e_1, 0), (e_2, 0))$. Then, again by the same argument as in § 4.2.2, the enhanced elliptic curves (E, P_1, P_2) and $(E_\lambda, (1, 0), (0, 0))$, where E_λ is given by the Weierstrass equation

$$E_\lambda : y^2 = x(x - 1)(x - \lambda),$$

are isomorphic over W. In particular, this means that $E \cong E_\lambda$ over W, and so E_λ has complex multiplication by $\mathcal{O}_{K_1}$ over W and good reduction modulo π.

Define

$$\mathcal{L}(d_1) := \left\{ \left(E_{\lambda(\tau_1)}, (1, 0), (0, 0) \right) : \tau_1 \in \Gamma(2)\backslash\mathcal{H}, \operatorname{disc}(\tau_1) = d_1 \right\}. \tag{4.2.7}$$

This is a set of representatives for isomorphism classes over $\overline{\mathbb{Q}}_p$ of enhanced elliptic curves for $\Gamma(2)$ with complex multiplication by $\mathcal{O}_{K_1}$.

Now, we saw in § 3.3.1 that for each $\tau_1 \in \mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H}$ of discriminant d_1, there is an elliptic curve E_{τ_1} over W with good reduction mod π, complex multiplication by $\mathcal{O}_{K_1}$ and j-invariant $j(\tau_1)$. By our above discussion, we can take E_{τ_1} to be $E_{\lambda(\tau_1'}$ for some $\tau_1'\Gamma(2)\backslash \in \mathcal{H}$ lying above τ_1 for some τ. Write

$$\mathcal{J}(d_1) = \{E_{\tau_1} : \tau_1 \in \mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H}, \operatorname{disc}(\tau_1) = d_1\}. \tag{4.2.8}$$

This is a set of representatives for the isomorphism classes over $\overline{\mathbb{Q}}_p$ of elliptic curves with complex multiplication by $\mathcal{O}_{K_1}$. We get a surjective map from $\mathcal{L}(d_1)$ to $\mathcal{J}(d_1)$ by forgetting the $\Gamma(2)$-structure $((1, 0), (0, 0))$ on E_λ, i.e. by sending an enhanced elliptic curve $(E, P, Q) \in \mathcal{L}(d_1)$ to the elliptic curve E_{τ_1} representing the isomorphism class of E over $\overline{\mathbb{Q}}_p$.

Note that the above discussion also works if we replace d_1 with d_2 and K_1 with K_2. Also, note that the map $\mathcal{L}(d_i) \to \mathcal{J}(d_i)$ is 2-to-1 if $d_i = -3$ and 3-to-1 if $d_i = -4$, since[1] the quotient map $\Gamma(2)\backslash\mathcal{H} \to \mathrm{SL}_2(\mathbb{Z})$ is 2-to-1 above ω and 3-to-1 above i.

We are now ready to prove Theorem 4.2.3. We start by considering the case $d_1, d_2 < -4$.

Lemma 4.2.9. *Suppose that $d_1, d_2 < -4$. Fix $\tau_1 \in \Gamma(2)\backslash\mathcal{H}$ of discriminant d_1, and write $j = j(\tau_1)$ and $\lambda = \lambda(\tau_1)$. Then*

$$\sum_{\substack{\tau_2 \in \Gamma(2)\backslash\mathcal{H} \\ \mathrm{disc}\,(\tau_2) = d_2}} v(\lambda - \lambda(\tau_2)) = \sum_{\substack{\tau_2 \in \mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H} \\ \mathrm{disc}\,(\tau_2) = d_2}} v(j - j(\tau_2)).$$

Proof. Let $(E, P_1, P_2) = (E_\lambda, (1,0), (0,0))$. By our above discussion and Propositions 3.2.8 and 4.2.5, we have

$$\begin{aligned}\sum_{\substack{\tau_2 \in \Gamma(2)\backslash\mathcal{H} \\ \mathrm{disc}\,(\tau_2) = d_2}} v(\lambda - \lambda(\tau_2)) &= \sum_{(E', P_1', P_2') \in \mathcal{L}(d_2)} v(\lambda(E, P_1, P_2) - \lambda(E', P_1', P_2)) \\ &= \frac{1}{2} \sum_{n \geq 1} \sum_{(E', P_1', P_2') \in \mathcal{L}(d_2)} \#\mathrm{Iso}_{W/\pi^n}((E, P_1, P_2), (E', P_1', P_2')),\end{aligned}$$

and

$$\sum_{\substack{\tau_2 \in \Gamma\backslash\mathcal{H} \\ \mathrm{disc}\,(\tau_2) = d_2}} v(j - j(\tau_2)) = \sum_{E' \in \mathcal{J}(d_2)} v(j(E) - j(E')) = \frac{1}{2} \sum_{n \geq 1} \sum_{E' \in \mathcal{J}(d_2)} \#\mathrm{Iso}_{W/\pi^n}(E, E').$$

So we just need to show that

$$\sum_{(E', P_1', P_2') \in \mathcal{L}(d_2)} \#\mathrm{Iso}_{W/\pi^n}((E, P_1, P_2), (E', P_1', P_2')) = \sum_{E' \in \mathcal{J}(d_2)} \#\mathrm{Iso}_{W/\pi^n}(E, E')$$

for all $n \geq 1$. Fix $E' \in \mathcal{J}(d_2)$ and $f \in \mathrm{Iso}_{W/\pi^n}(E, E')$. Then $f : (E, P_1, P_2) \xrightarrow{\sim} (E', f(P_1), f(P_2))$ is an isomorphism of enhanced elliptic curves over W, so we get a

[1] One can also see this by studying how $\mathrm{Aut}_W(E)$ acts on the set of $\Gamma(2)$-structures on E.

natural map

$$\mathrm{Iso}_{W/\pi^n}(E,E') \to \bigsqcup_{(P_1',P_2')} \mathrm{Iso}_{W/\pi^n}((E,P_1,P_2),(E',P_1',P_2')),$$

where the disjoint union runs over all $\Gamma(2)$-structures (P_1', P_2') for E'. This is clearly a bijection, and so

$$\#\mathrm{Iso}_{W/\pi^n}(E,E') = \sum_{(P_1',P_2')} \#\mathrm{Iso}_{W/\pi^n}((E,P_1,P_2),(E',P_1',P_2')),$$

with the sum running over all $\Gamma(2)$-structures for E'. Summing over all $E' \in \mathcal{J}(d_2)$ completes the proof. □

Now, we generalize the above lemma to allow for the cases where one or more d_i is -3 or -4.

Lemma 4.2.10. *Fix $\tau_1 \in \Gamma(2)\backslash\mathcal{H}$ of discriminant d_1. Write $j = j(\tau_1)$ and $\lambda = \lambda(\tau_1)$. Then*

$$\sum_{\substack{\tau_2 \in \Gamma(2)\backslash\mathcal{H} \\ \mathrm{disc}\,\tau_2 = d_2}} v(\lambda - \lambda(\tau_2)) = \frac{2}{w_2} \sum_{\substack{\tau_2 \in \mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H} \\ \mathrm{disc}\,(\tau_2) = d_2}} v(j - j(\tau_2)).$$

Proof. As in the previous lemma, it is enough to show that

$$\sum_{(E',P_1',P_2') \in \mathcal{L}(d_2)} \#\mathrm{Iso}_{W/\pi^n}((E,P_1,P_2),(E',P_1',P_2')) = \frac{2}{w_2} \sum_{E' \in \mathcal{J}(d_2)} \#\mathrm{Iso}_{W/\pi^n}(E,E').$$

So fix $E' \in \mathcal{J}(d_1)$. As before, we get a bijection

$$\mathrm{Iso}_{W/\pi^n}(E,E') \to \bigsqcup_{(P_1',P_2')} \mathrm{Iso}_{W/\pi^n}((E,P_1,P_2),(E',P_1',P_2')),$$

where the disjoint union runs over all $\Gamma(2)$-structures (P_1', P_2') for E. Let $F : \mathcal{L}(d_2) \to \mathcal{J}(d_2)$ be the natural map sending (E', P_1', P_2') to E'. An analysis of the action of $\mathrm{Aut}\,(E)$

on $E[2]$ shows that the map

$$\bigsqcup_{(P_1',P_2')} \mathrm{Iso}_{W/\pi^n}((E,P_1,P_2),(E',P_1',P_2')) \to \bigsqcup_{(E',P_1',P_2')\in F^{-1}(E')} \mathrm{Iso}_{W/\pi^n}((E,P_1,P_2),(E',P_1',P_2'))$$

is $\frac{w_2}{2}$-to-1, so we get

$$\begin{aligned}\#\mathrm{Iso}_{W/\pi^n}(E,E') &= \sum_{(P_1,P_2)} \#\mathrm{Iso}_{W/\pi^n}((E,P_1,P_2),(E',P_1',P_2')) \\ &= \frac{w_2}{2} \sum_{(E',P_1',P_2')\in F^{-1}(E')} \#\mathrm{Iso}_{W/\pi^n}((E,P_1,P_2),(E',P_1',P_2')).\end{aligned}$$

We complete the proof by summing over all $E' \in \mathcal{J}(d_1)$. □

Now fix $\tau_1 \in \Gamma\backslash \mathrm{SL}_2(\mathbb{Z})$ of discriminant d_1, and let $j = j(\tau_1)$. Note that there are $\frac{12}{w_1}$ values of $\tau_1' \in \Gamma(2)\backslash\mathcal{H}$ with $j(\tau_1') = j$. Applying Lemma 4.2.10 to each of them gives

$$\sum_{\tau_1'\in\Gamma(2)\backslash \mathrm{SL}_2(\mathbb{Z})\tau_1} \left(\sum_{\substack{\tau_2\in\Gamma(2)\backslash\mathcal{H} \\ \mathrm{disc}\,\tau_2 = d_2}} v(\lambda(\tau_1') - \lambda(\tau_2)) \right) = \frac{24}{w_1 w_2} \left(\sum_{\substack{\tau_2\in \mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H} \\ \mathrm{disc}\,(\tau_2) = d_2}} v(j - j(\tau_2)) \right).$$

Summing over all $\tau_1 \in \mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H}$ of discriminant d_1 completes the proof of Theorem 4.2.3.

Chapter 5

Berwick's congruences and the modular lambda function

In 1928, Berwick [1] conjectured several results on the valuation of j and $j - 1728$ above certain rational primes p, where j is a singular modulus. In 1985, some of these congruences were proven by Gross and Zagier [17], in the cases where $p = 2, 3, 5, 7$ or 11 and the discriminant d of j satisfies $\left(\frac{d}{p}\right) = -1$. We've already seen Gross and Zagier's result earlier on, in Corollary 3.2.17. The general case remained unsolved until 2004, when it was proven by Bettner [2].

In this section, I will give a similar result for singular values of the modular lambda function λ. If $\tau \in \mathcal{H}$ is imaginary quadratic, then $\lambda = \lambda(\tau)$ is related to the singular modulus $j = j(\tau)$ by the polynomial equation

$$f_j(\lambda) := (1 - \lambda + \lambda)^3 - \frac{j}{256}\lambda^2(1 - \lambda)^2 = 0.$$

From this relation, and the well-known fact that j is an algebraic integer, one can deduce that λ, as well as $1 - \lambda$, is a 2-unit (see Lemma 5.3.2). So we are interested in finding the valuation of j at primes dividing 2. To do this, I will study the Newton polygon of $f_j(X)$ in order to relate the valuation of λ to the valuation of j. This can then be combined with Bettner's result in order to give a similar result for the valuation of λ.

5.1 Berwick's congruences

In this section, I will recall Berwick's congruences for $p = 2$. If H is a number field, and $\mathfrak{p}$ is a prime of H dividing 2, let $v_\mathfrak{p}$ be the valuation

$$v_\mathfrak{p}(x) := \frac{1}{[H_\mathfrak{p} : \mathbb{Q}_2]} \log_2 \left| \mathrm{Nm}_{H_\mathfrak{p}/\mathbb{Q}_2}(x) \right|, \quad x \in H^\times. \tag{5.1.1}$$

This is a representative for the finite place of H corresponding to the prime $\mathfrak{p}$, and it is normalized so that $v_\mathfrak{p}(2) = 1$.

Theorem 5.1.2. (Berwick's congruence for $p = 2$) *Let $\tau \in \mathcal{H}$ be imaginary quadratic of discriminant $d < 0$. Let $K = \mathbb{Q}(\sqrt{d})$, let d_K be the discriminant of K, and write $d = f^2 d_K$ (so f is the conductor of τ). Let $s = \mathrm{ord}_2(f)$. Then for every prime $\mathfrak{p}$ of $K(j(\tau))$ dividing 2, we have*

$$v_\mathfrak{p}(j(\tau)) \begin{cases} \geq 15, & \text{if 2 is inert in } K \text{ and } s = 0 \\ = 2^{3-s}, & \text{if 2 is inert in } K \text{ and } s \geq 1 \\ = 3 \cdot 2^{1-s}, & \text{if 2 is ramified in } K \\ = 0, & \text{if 2 is split in } K. \end{cases}$$

Proof. If 2 is split in K, then we can use the same argument as in Corollary 3.2.16. Let $\mathcal{O} \subseteq \mathcal{O}_K$ be the imaginary quadratic order of discriminant d. By [25], we can find a field extension L of $K(j(\tau))$, a prime $\mathfrak{p}'$ of L dividing $\mathfrak{p}$, and an elliptic curve E over L with complex multiplication by $\mathcal{O}$, j-invariant $j(E) = j(\tau)$ and with good reduction mod $\mathfrak{p}'$. Then, since 2 is split in K, E has ordinary reduction mod $\mathfrak{p}$. But $j = 0$ is a supersingular j-invariant in characteristic 2, so we cannot have $j(\tau) \equiv 0 \mod \mathfrak{p}$.

For the case where 2 is inert in K and d is a fundamental discriminant, see [17, Corollary 2.5] or [24, §9.2]. The general case is proven in [2]. □

The following proposition allows us to replace the condition that 2 is inert, ramified, or split in K to a condition on the Kronecker symbol $\left(\frac{d_K}{2}\right)$, or equivalently to a condition on $d_K \mod 8$.

Proposition 5.1.3. *Let K be a quadratic field of discriminant d_K, and let p be prime. Then*

1. *if $\left(\frac{d_K}{p}\right) = 0$, then $p\mathcal{O}_K = \mathfrak{p}^2$ for some prime $\mathfrak{p}$ of $\mathcal{O}_K$, i.e. p is ramified in K,*
2. *if $\left(\frac{d_K}{p}\right) = 1$, then $p\mathcal{O}_K = \mathfrak{p}\mathfrak{p}'$ for some primes $\mathfrak{p} \neq \mathfrak{p}'$ in $\mathcal{O}_K$, i.e. p is split in K, and*
3. *if $\left(\frac{d_K}{p}\right) = -1$, then $p\mathcal{O}_K$ is prime in $\mathcal{O}_K$, i.e. p is inert in K.*

In particular, for $p = 2$,

1. *if $4|d_K$ then 2 is ramified in K,*
2. *if $d_K \equiv 1 \mod 8$ then 2 is split in K, and*
3. *if $d_K \equiv 5 \mod 8$ then 2 is inert in K.*

Proof. See [9, Proposition 5.16]. □

Corollary 5.1.4. (Berwick's congruence, alternate formulation) *Let $\tau \in \mathcal{H}$ be imaginary quadratic of discriminant $d < 0$. Let $K = \mathbb{Q}(\sqrt{d})$, let d_K be the discriminant of K, and write $d = f^2 d_K$ (so f is the conductor of τ). Let $s = \mathrm{ord}_2(f)$. Then for every prime $\mathfrak{p}$ of $K(j(\tau))$ dividing 2, we have*

$$v_{\mathfrak{p}}(j(\tau)) \begin{cases} \geq 15, & \text{if } d_K \equiv 5 \mod 8 \text{ and } s = 0 \\ = 2^{3-s}, & \text{if } d_K \equiv 5 \mod 8 \text{ and } s \geq 1 \\ = 3 \cdot 2^{1-s}, & \text{if } 4|d_K \\ = 0, & \text{if } d_K \equiv 1 \mod 8. \end{cases}$$

Table 5.1 gives the result of applying Theorem 5.1.2 to the rational j-invariants.

5.2 Newton polygons

In this section, I will introduce the basic theory of Newton polygons, following [21, Chapter IV].

τ	K	d_K	f	$d_K \mod 8$	s	$\mathrm{ord}_2(j(\tau))$	$j(\tau)$
i	$\mathbb{Q}(i)$	-4	1	4	0	6	$2^6 \cdot 3^3$
$2i$	$\mathbb{Q}(i)$	-4	2	4	1	3	$2^3 \cdot 3^3 \cdot 11^3$
$\sqrt{-2}$	$\mathbb{Q}(\sqrt{-2})$	-8	1	0	0	6	$2^6 \cdot 5^3$
$\omega = \frac{1+\sqrt{-3}}{2}$	$\mathbb{Q}(\sqrt{-3})$	-3	1	5	0	≥ 15	0
2ω	$\mathbb{Q}(\sqrt{-3})$	-3	2	5	1	4	$2^4 \cdot 3^3 \cdot 5^3$
3ω	$\mathbb{Q}(\sqrt{-3})$	-3	3	5	0	≥ 15	$-2^{15} \cdot 3 \cdot 5^3$
$\frac{1+\sqrt{-7}}{2}$	$\mathbb{Q}(\sqrt{-7})$	-7	1	1	0	0	$-3^3 \cdot 5^3$
$1+\sqrt{-7}$	$\mathbb{Q}(\sqrt{-7})$	-7	2	1	1	0	$3^3 \cdot 5^3 \cdot 17^3$
$\frac{1+\sqrt{-11}}{2}$	$\mathbb{Q}(\sqrt{-11})$	-11	1	5	0	≥ 15	-2^{15}
$\frac{1+\sqrt{-19}}{2}$	$\mathbb{Q}(\sqrt{-19})$	-19	1	5	0	≥ 15	$-2^{15} \cdot 3^3$
$\frac{1+\sqrt{-43}}{2}$	$\mathbb{Q}(\sqrt{-43})$	-43	1	5	0	≥ 15	$-2^{18} \cdot 3^3 \cdot 5^3$
$\frac{1+\sqrt{-67}}{2}$	$\mathbb{Q}(\sqrt{-67})$	-67	1	5	0	≥ 15	$-2^{15} \cdot 3^3 \cdot 5^3 \cdot 11^3$
$\frac{1+\sqrt{-163}}{2}$	$\mathbb{Q}(\sqrt{-163})$	-163	1	5	0	≥ 15	$-2^{18} \cdot 3^3 \cdot 5^3 \cdot 23^3 \cdot 29^3$

Table 5.1: Theorem 5.1.2 applied to the rational j-invariants. Notation is the same as in Theorem 5.1.2

Fix a prime p, and let Ω be the completion of the algebraic closure $\overline{\mathbb{Q}}_p$ of $\mathbb{Q}_p$. Let $f(X) \in \Omega[X]$ be a polynomial of the form

$$f(X) = 1 + a_1 X + a_2 X^2 + \ldots + a_n X^n, \ a_n \neq 0.$$

Consider the points

$$(0,0), (1, \mathrm{ord}_p(a_1)), \ldots, (n, \mathrm{ord}_p(a_n)),$$

omitting $(i, \mathrm{ord}_p(a_i))$ if $a_i = 0$. The *Newton polygon* of f is the *convex hull* of these points, i.e. the highest polygonal line from $(0,0)$ to $(n, \mathrm{ord}_p a_n)$ which is lower than all of these points.

We can construct the Newton polygon explicitly as follows. Let $v_i = \mathrm{ord}_p a_i$ and $v_0 = 0$, so that we're looking at the points $(0, v_0), (1, v_1), \ldots, (n, v_n)$. For $1 \leq i < j \leq n$, let $L_{i,j}$ be the line from (i, v_i) to (j, v_j). It has *slope*

$$\frac{v_j - v_i}{j - i}$$

and *length* $j - i$. First, let $i_0 = 0$, and take from among the lines $L_{0,j}, i = 1, \ldots, n$, the line

L_{0,i_1} of minimal slope. Next, if $i_1 \neq n$, take from among the lines $L_{i_1,j}, j = 1, \ldots, n$, the line L_{i_1,i_2} of minimal slope. Continue inductively, taking $L_{i_l,i_{l+1}}$ to be the line of minimal slope out of the lines $L_{i_l,j}, j = i_l, \ldots, n$. Stop when $i_{l+1} = n$. Then the Newton polygon of f is

$$N = \bigcup_{m=0}^{l} L_{i_m,i_{m+1}}.$$

The *vertices* of N are the points (i_m, v_{i_m}) where the slope changes. If we choose $i_1, \ldots, i_l$ so that l is minimal, i.e. so that $L_{i_m,i_{m+1}}$ and $L_{i_{m+1},i_{m+2}}$ have different slopes for each $m = 0, \ldots, l-1$, then the vertices of N are exactly $i_0, \ldots, i_{l+1}$. In this case, we'll call the slopes of $L_{i_0,i_1}, \ldots, L_{i_l,i_{l+1}}$ the *slopes of the Newton polygon* N.

The following result relates the slopes of the Newton polygon of f to the valuation of its roots.

Lemma 5.2.1. *Let $f \in \Omega[X]$ be as above, and let $\alpha_1, \ldots, \alpha_n \in \Omega$ be the roots of f, so that*

$$f = \prod_{i=1}^{n} \left(1 - \frac{X}{\alpha_i}\right).$$

If s is a slope of the Newton polygon of f with length l, then exactly l of the α_i's have

$$\operatorname{ord}_p(\alpha_i) = -s.$$

Proof. This is [21, Chapter IV.3, Lemma 4]. □

Example 5.2.2. Consider the polynomial

$$\begin{aligned} f(X) &= \left(1 - X + X^2\right)^3 - \frac{1728}{256} X^2 (1 - X)^2 \\ &= 1 - 3X - \frac{3}{4}X^2 + \frac{13}{2}X^3 - \frac{3}{4}X^4 - 3X^5 + X^6 \\ &= \left(X - \frac{1}{2}\right)^2 (X + 1)^2 (X - 2)^2. \end{aligned}$$

Note that $f = f_{1728}$, where, for $j \in \mathbb{C}$, f_j is the polynomial

$$f_j(X) = \left(1 - X + X^2\right)^3 - \frac{j}{256} X^2 (1 - X)^2,$$

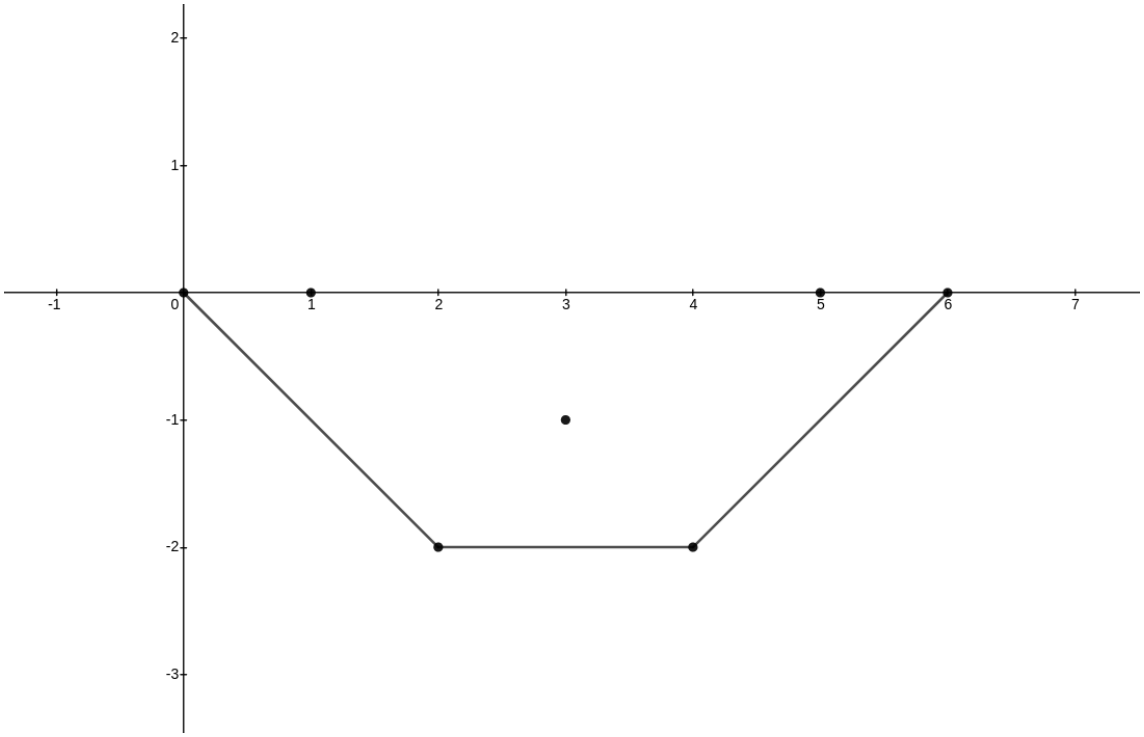

Figure 5.1: The Newton polygon of $f(X) = 1 - 3X - \frac{3}{4}X^2 + \frac{13}{2}X^3 - \frac{3}{4}X^4 - 3X^5 + X^6$.

so the roots of f are exactly the singular λ-values of discriminant -4. The Newton polygon of f is given in Figure 5.1, it is the lower convex hull of the points

$$(0,0),\ (1,0),\ (2,-2),\ (3,-1),\ (4,-2),\ (5,0),\ (6,0).$$

It has slopes 1, 0 and -1, each of length 2. So f has

1. 2 roots α with $\mathrm{ord}_2(\alpha) = 1$,
2. 2 roots α with $\mathrm{ord}_2(\alpha) = 0$, and
3. 2 roots α with $\mathrm{ord}_2(\alpha) = -1$.

On the other hand, by looking at the factorization of f we see that f has roots 2, -1 and $\frac{1}{2}$, each with multiplicity 2. This agrees with the Newton polygon of f.

5.3 A Berwick-like congruence for the modular lambda function

Fix $\tau \in \mathcal{H}$ imaginary quadratic of discriminant $d < 0$. Let $K = \mathbb{Q}(\sqrt{d})$, let d_K be the discriminant of K, and write $d = f^2 d_K$, so f is the conductor of τ. Let $j = j(\tau)$ and $\lambda = \lambda(\tau)$. Then j and λ satisfy the relation

$$j = 256\frac{(1-\lambda+\lambda^2)^3}{\lambda^2(1-\lambda)^2}. \tag{5.3.1}$$

It is a well-known result that the singular modulus j is an algebraic integer. Moreover, by [3, Theorem 1.1], j is not an algebraic unit. It follows from this and Equation (5.3.1) that λ is a 2-unit:

Lemma 5.3.2. *If $\tau \in \mathcal{H}$ is imaginary quadratic, then $\lambda = \lambda(\tau)$ is a 2-unit.*

Proof. Let $K = \mathbb{Q}(\tau)$, let $\mathfrak{p}$ be a prime of $K(\lambda)$ not dividing 2, and let $v = v_{\mathfrak{p}}$ be the valuation of K corresponding to $\mathfrak{p}$. Since $j = j(\tau)$ is an algebraic integer, we have $v(j) \geq 0$.

First, if $v(\lambda) > 0$, then

$$\begin{aligned} 0 \leq v(j) &= v\left(256\frac{(1-\lambda+\lambda^2)^3}{\lambda^2(1-\lambda)^2}\right) \\ &= v(256) + 3v(1-\lambda+\lambda^2) - 2v(\lambda) - 2v(1-\lambda) \\ &= -2v(\lambda) && \text{by the ultrametric inequality} \\ &< 0, \end{aligned}$$

which is a contradiction. Conversely, if $v(\lambda) < 0$, then

$$\begin{aligned} 0 \leq v(j) &= v(256) + 3v(1-\lambda+\lambda^2) - 2v(\lambda) - 2v(1-\lambda) \\ &= 2v(\lambda) && \text{again by the ultrametric inequality} \\ &< 0, \end{aligned}$$

which is again a contradiction. So we must have $v(\lambda) = 0$. □

Note that

$$\frac{1}{\lambda}, \quad 1-\lambda, \quad \frac{1}{1-\lambda}, \quad \frac{\lambda-1}{\lambda}, \quad \frac{\lambda}{\lambda-1}$$

are all 2-units as well, since they are all related to j in the same way as λ is (that is to say, they satisfy the relation in Equation (5.3.1)).

We can use the same argument to bound the valuation of λ at primes dividing 2:

Lemma 5.3.3. *Let $\mathfrak{p}$ be a prime of $K(\lambda)$ dividing 2, and $v = v_{\mathfrak{p}}$ the corresponding valuation. Normalize v so that $v(2) = 1$. Then*

$$-4 \leq v(\lambda) \leq 4.$$

Proof. If $v(\lambda) > 4$, then

$$\begin{aligned} 0 \leq v(j) &= v\left(256\frac{(1-\lambda+\lambda^2)^3}{\lambda^2(1-\lambda)^2}\right) \\ &= v(256) + 3v(1-\lambda+\lambda^2) - 2v(\lambda) - 2v(1-\lambda) \\ &= 8 - 2v(\lambda) && \text{by the ultrametric inequality} \\ &< 0, \end{aligned}$$

which is a contradiction. And if $v(\lambda) < -4$, then

$$\begin{aligned} 0 \leq v(j) &= v(256) + 3v(1-\lambda+\lambda^2) - 2v(\lambda) - 2v(1-\lambda) \\ &= 8 + 2v(\lambda) && \text{again by the ultrametric inequality} \\ &< 0, \end{aligned}$$

which is again a contradiction. So we must have $-4 \leq v(\lambda) \leq 4$. □

We can do better than this by applying Newton polygons to Equation (5.3.1). The solutions to

$$j = 256\frac{(1-X+X^2)^3}{X^2(1-X)^2},$$

i.e. the roots of the polynomial

$$f_j(X) := (1 - X + X^2)^3 - \frac{j}{256}X^2(1-X)^2, \tag{5.3.4}$$

are exactly the values $\lambda(\tau')$, where $j(\tau') = j$. These values are

$$\lambda, \quad 1-\lambda, \quad \frac{1}{\lambda}, \quad \frac{1}{1-\lambda}, \quad \frac{\lambda-1}{\lambda}, \quad \frac{\lambda}{\lambda-1}.$$

Alternatively, S_3 acts on $\Gamma(2)$-structures for the complex elliptic curve $E_\tau = \mathbb{C}/(\mathbb{Z}+\tau\mathbb{Z})$, which induces an action on $K(\lambda)$, by taking

$${}^{\sigma}\lambda(E_\tau, P_1, P_2) = \lambda(E_\tau, P_{\sigma(1)}, P_{\sigma(2)})$$

for $\sigma \in S_3$, (P_1, P_2) an ordered basis of $E_\tau[2]$ and $P_3 = P_1 + P_2$. The roots of f_j are the values ${}^{\sigma}\lambda, \sigma \in S_3$.

Theorem 5.3.5. *Let $\tau \in \mathcal{H}$ be imaginary quadratic of discriminant d, and let $j = j(\tau)$ and $\lambda = \lambda(\tau)$. Let*

$$\Lambda = S_3 \cdot \lambda = \left\{\lambda, 1-\lambda\frac{1}{\lambda}, \frac{1}{1-\lambda}, \frac{\lambda-1}{\lambda}, \frac{\lambda}{\lambda-1}\right\}.$$

Fix a prime $\mathfrak{p}$ of $L = \mathbb{Q}(\tau, \lambda)$ lying above 2, and let $v = v_{\mathfrak{p}}$ be the valuation corresponding to $\mathfrak{p}$, normalized so that $v(2) = 1$.

1. *If $v(j) < 8$, then, counting multiplicity, there are exactly*
   (a) *two $\lambda' \in \Lambda$ with $v(\lambda') = \frac{1}{2}v(j) - 4 < 0$,*
   (b) *two $\lambda' \in \Lambda$ with $v(\lambda') = 4 - \frac{1}{2}v(j) > 0$, and*
   (c) *two $\lambda' \in \Lambda$ with $v(\lambda') = 0$.*
2. *If $v(j) \geq 8$, then $v(\lambda') = 0$ for all $\lambda' \in \Lambda$.*

Proof. Fix an embedding $i : L \hookrightarrow \overline{\mathbb{Q}}_2$ such that $\mathfrak{p} = i^{-1}\left(\mathfrak{m}_{\overline{\mathbb{Q}}_2}\right)$. Then $v(\alpha) = \operatorname{ord}_2(i(\alpha))$ for $\alpha \in L$.

The values $\lambda' \in \Lambda$ are exactly the roots of the polynomial

$$\begin{aligned} f_j(X) &= (1 - X + X^2)^3 - \frac{j}{256} X^2 (1 - X)^2 \\ &= 1 - 3X + \left(6 - \frac{j}{256}\right) X^2 + \left(\frac{j}{128} - 7\right) X^3 + \left(6 - \frac{j}{256}\right) X^4 - 3X + X^6. \end{aligned}$$

The Newton polygon of f_j over $\overline{\mathbb{Q}}_2$ is the lower convex hull of the points

$$(0,0), (1,0), \left(2, v\left(6 - \frac{j}{256}\right)\right), \left(3, v\left(\frac{j}{128} - 7\right)\right), \left(4, v\left(6 - \frac{j}{256}\right)\right), (5,0), (6,0).$$

Note that

$$v\left(6 - \frac{j}{256}\right) = v(3 \cdot 2^9 - j) - 8 \geq \min(9, v(j)) - 8$$

and

$$v\left(\frac{j}{128} - 7\right) = v(j - 7 \cdot 2^7) - 7 \geq \min(v(j), 7) - 7.$$

If $v(j) \geq 8$, then

$$v\left(6 - \frac{j}{256}\right) \geq 8 - 8 = 0$$

and

$$v(j - 7 \cdot 2^7) - 7 \geq 7 - 7 = 0,$$

so the Newton polygon of f_j is just the line from $(0,0)$ to $(6,0)$. So, by Lemma 5.2.1, all of the roots λ' of f_j have $v(\lambda') = 0$.

If $v(j) < 8$, then

$$v\left(6 - \frac{j}{256}\right) = v(3 \cdot 2^9 - j) - 8 = v(j) - 8 < 0$$

and

$$v\left(\frac{j}{128} - 7\right) = v(j - 7 \cdot 2^7) - 7 \geq \min(v(j), 7) - 7 = \min(v(j) - 7, 0) > v(j) - 8.$$

So the Newton polygon of f_j consists of

1. the line from $(0,0)$ to $\left(2, v\left(6-\frac{j}{256}\right)\right)$, which has length 2 and slope

$$\frac{1}{2}v\left(6-\frac{j}{256}\right) = \frac{1}{2}\left(v(j)-8\right) = \frac{v(j)}{2} - 4,$$

2. the line from $\left(2, v\left(6-\frac{j}{256}\right)\right)$ to $\left(4, v\left(6-\frac{j}{256}\right)\right)$, which has length 2 and slope 0, and

3. the line from $\left(4, v\left(6-\frac{j}{256}\right)\right)$ to $(6,0)$, which has length 2 and slope

$$-\frac{1}{2}v\left(6-\frac{j}{256}\right) = -\frac{1}{2}\left(v(j)-8\right) = 4 - \frac{v(j)}{2}.$$

So, by Lemma 5.2.1, the valuations of the roots λ' of f_j are distributed as claimed in the first part of the theorem. □

Combining Theorem 5.3.5 and Theorem 5.1.2 immediately gives the following result:

Corollary 5.3.6. (Berwick's congruence for λ) *Let $\tau \in \mathcal{H}$ be imaginary quadratic of discriminant $d < 0$. Let $K = \mathbb{Q}(\sqrt{d})$, let d_K be the discriminant of K, and write $d = f^2 d_K$ (so f is the conductor of τ) and $s = \operatorname{ord}_2 f$. Let*

$$\Lambda = S_3 \cdot \lambda = \left\{\lambda, 1-\lambda\frac{1}{\lambda}, \frac{1}{1-\lambda}, \frac{\lambda-1}{\lambda}, \frac{\lambda}{\lambda-1}\right\}.$$

Let $\mathfrak{p}$ be a prime of $K(\lambda)$ dividing 2, and let $v = v_{\mathfrak{p}}$ be the corresponding valuation, normalized so that $v(2) = 1$. Then

$$\{v(\lambda') : \lambda' \in \Lambda\} = \begin{cases} \{0\}, & \text{if 2 is inert in } K \text{ and } s = 0 \\ \{0, 4-2^{2-s}, 2^{2-s}-4\}, & \text{if 2 is inert in } K \text{ and } s \geq 1 \\ \{0, 4-3\cdot 2^{-s}, 3\cdot 2^{-s}-4\}, & \text{if 2 is ramified in } K, \text{ and} \\ \{0, 4, -4\}, & \text{if 2 is split in } K. \end{cases}$$

Moreover, in the last three cases, each possible value of $v(\lambda')$ occurs an equal number of times (twice, if $d < -4$).

As was the case for j, we can reformulate this in terms of $d_K \mod 8$:

Corollary 5.3.7. (Berwick's congruence for λ, alternate formulation) *Let $\tau \in \mathcal{H}$ be imaginary quadratic of discriminant $d < 0$. Let $K = \mathbb{Q}(\sqrt{d})$, let d_K be the discriminant of K, and write $d = f^2 d_K$ (so f is the conductor of τ) and $s = \mathrm{ord}_2(f)$. Let*

$$\Lambda = S_3 \cdot \lambda = \left\{\lambda, 1-\lambda \frac{1}{\lambda}, \frac{1}{1-\lambda}, \frac{\lambda-1}{\lambda}, \frac{\lambda}{\lambda-1}\right\}.$$

Let $\mathfrak{p}$ be a prime of $K(\lambda)$ dividing 2, and let $v = v_{\mathfrak{p}}$ be the corresponding valuation, normalized so that $v(2) = 1$. Then

$$\{v(\lambda') : \lambda' \in \Lambda\} = \begin{cases} \{0\}, & \text{if } d_K \equiv 5 \mod 8 \text{ and } s = 0 \\ \{0, 4 - 2^{2-s}, 2^{2-s} - 4\}, & \text{if } d_K \equiv 5 \mod 8 \text{ and } s \geq 1 \\ \{0, 4 - 3 \cdot 2^{-s}, 3 \cdot 2^{-s} - 4\}, & \text{if } 4 | d_K, \text{ and} \\ \{0, 4, -4\}, & \text{if } d_K \equiv 1 \mod 8. \end{cases}$$

Moreover, in the last three cases, each possible value of $v(\lambda')$ occurs an equal number of times (twice, if $d < -4$).

Table 5.2 summarizes the result of 5.3.7 when d is a discriminant of class number 1, i.e. when $j(\tau) \in \mathbb{Q}$. One can compare this against the minimal polynomials of the corresponding λ-invariants, given in Table 5.3, to check that Corollary 5.3.7 is correct in these cases.

τ	K	d_K	f	$d_K \mod 8$	s	$v(j(\tau))$	$\{v(\lambda') : \lambda' \in \Lambda\}$
i	$\mathbb{Q}(i)$	-4	1	4	0	6	$\{0, \pm 1\}$
$2i$	$\mathbb{Q}(i)$	-4	2	4	1	3	$\{0, \pm 5/2\}$
$\sqrt{-2}$	$\mathbb{Q}(\sqrt{-2})$	-8	1	0	0	6	$\{0, \pm 1\}$
$\omega = \frac{-1+\sqrt{-3}}{2}$	$\mathbb{Q}(\sqrt{-3})$	-3	1	5	0	≥ 15	$\{0\}$
2ω	$\mathbb{Q}(\sqrt{-3})$	-3	2	5	1	4	$\{0, \pm 2\}$
3ω	$\mathbb{Q}(\sqrt{-3})$	-3	3	5	0	≥ 15	$\{0\}$
$\frac{1+\sqrt{-7}}{2}$	$\mathbb{Q}(\sqrt{-7})$	-7	1	1	0	0	$\{0, \pm 4\}$
$1 + \sqrt{-7}$	$\mathbb{Q}(\sqrt{-7})$	-7	2	1	1	0	$\{0, \pm 4\}$
$\frac{1+\sqrt{-11}}{2}$	$\mathbb{Q}(\sqrt{-11})$	-11	1	5	0	≥ 15	$\{0\}$
$\frac{1+\sqrt{-19}}{2}$	$\mathbb{Q}(\sqrt{-19})$	-19	1	5	0	≥ 15	$\{0\}$
$\frac{1+\sqrt{-43}}{2}$	$\mathbb{Q}(\sqrt{-43})$	-43	1	5	0	≥ 15	$\{0\}$
$\frac{1+\sqrt{-67}}{2}$	$\mathbb{Q}(\sqrt{-67})$	-67	1	5	0	≥ 15	$\{0\}$
$\frac{1+\sqrt{-163}}{2}$	$\mathbb{Q}(\sqrt{-163})$	-163	1	5	0	≥ 15	$\{0\}$

Table 5.2: The results of Corollary 5.3.7 when d has class number one, i.e. when λ lies over a rational j-invariant.

τ	d_K	f	$\{v(\lambda') : \lambda' \in \Lambda\}$	$(1-x+x^2)^3 - \frac{1}{256}jx^2(1-x)^2 = \prod_{\text{disc}\,(\tau')=d} (x-\lambda(\tau'))$
i	-4	1	$\{0, \pm 1\}$	$\left(x-\frac{1}{2}\right)^2 (x+1)^2(x-2)^2$
$2i$	-4	2	$\{0, \pm 5/2\}$	$\left(x^2-x-\frac{1}{32}\right)(x^2+32x-32)(x^2-34x+1)$
$\sqrt{-2}$	-8	1	$\{0, \pm 1\}$	$\left(x^2-x-\frac{1}{4}\right)(x^2+4x-4)(x^2-6x+1)$
$\omega = \frac{-1+\sqrt{-3}}{2}$	-3	1	$\{0\}$	$(x^2-x+1)^3$
2ω	-3	2	$\{0, \pm 2\}$	$\left(x^2-x+\frac{1}{16}\right)(x^2+14x+1)(x^2-16x+16)$
3ω	-3	3	$\{0\}$	$x^6-3x^5+48006x^4-96007x^3+48006x^2-3x+1$
$\frac{1+\sqrt{-7}}{2}$	-7	1	$\{0, \pm 4\}$	$\left(x^2-\frac{1}{16}x+\frac{1}{16}\right)\left(x^2-\frac{31}{16}x+1\right)(x^2-x+16)$
$1+\sqrt{-7}$	-7	2	$\{0, \pm 4\}$	$\left(x^2-x+\frac{1}{256}\right)(x^2+254x+1)(x^2-256x+256)$
$\frac{1+\sqrt{-11}}{2}$	-11	1	$\{0\}$	$x^6-3x^5+134x^4-263x^3+134x^2-3x+1$
$\frac{1+\sqrt{-19}}{2}$	-19	1	$\{0\}$	$x^6-3x^5+3462x^4-6919x^3+3462x^2-3x+1$
$\frac{1+\sqrt{-43}}{2}$	-43	1	$\{0\}$	$x^6-3x^5+3456006x^4-6912007x^3+3456006x^2-3x+1$
$\frac{1+\sqrt{-67}}{2}$	-67	1	$\{0\}$	$x^6-3x^5+574992006x^4-1149984007x^3+574992006x^2-3x+1$
$\frac{1+\sqrt{-163}}{2}$	-163	1	$\{0\}$	$x^6-3x^5+1025536768128006x^4-2051073536256007x^3+1025536768128006x^2-3x+1$

Table 5.3: Comparing the valuations at 2 and the minimal polynomials of the singular λ-invariants of discriminant d_K, for quadratic imaginary fields K of class number 1.

Chapter 6

An integral model for $X(2)$

6.1 Drinfield level structures and modular curves in arbitrary characteristic

In this section, I will generalize the moduli problems from § 2.2 to elliptic curves over general schemes. For a more detailed approach, see Katz and Mazur's book [20].

Fix a base scheme S. An *elliptic curve over* S consists of a smooth curve $E \xrightarrow{f} S$, with geometrically connected fibers[1] of genus one, together with a *zero section* $[0] : S \to E$. One can show (see [20, Theorem 2.1.2]) that an elliptic curve E/S admits a unique S-group scheme structure such that for every S-scheme T,

$$E(T) \cong \mathrm{Pic}_0(E_T/T) = \mathrm{Pic}_0(E \times_S T/T)$$

as groups. Throughout this chapter I will treat all elliptic curves over S as S-group schemes with this structure.

We want to generalize the concepts of enhanced elliptic curves for $\Gamma(N), \Gamma_0(N)$ and $\Gamma_1(N)$, as introduced in § 2.2, to elliptic curves over arbitrary schemes S. To do this, we first introduce the concept of A-structures and A-generators.

[1] This means that for every fiber $E_s = f^{-1}(s), s \in S$, and every field k, the scheme $E_s \times_{\mathrm{Spec}\ (Z)} \mathrm{Spec}\ (k)$ is connected.

Let E be an elliptic curve[2] over S, and A an abelian group. An *A-structure* on E/S is a group homomorphism

$$\varphi : A \to E(S) = \mathrm{Hom}_S(S, E)$$

such that the effective Cartier divisor

$$G = \sum_{a \in A} [\varphi(a)]$$

in C/S of degree $\#A$ is a subgroup-scheme of C/S. We call G the *A-subgroup of C/S generated by φ*, and φ the *A-generator* of the subgroup G.

Now, fix an elliptic curve E/S and $N \geq 1$. We define $[\Gamma(N)]$-structures, $[\Gamma_1(N)]$-structures and $[\Gamma_0(N)]$-structures on E/S as follows.

1. A $[\Gamma(N)]$-*structure* on E/S, is a $(\mathbb{Z}/N\mathbb{Z})^2$-generator for the subgroup-scheme $E[N]$ of E, i.e. a homomorphism

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

   such that, as divisors,

   $$E[N] = \sum_{(a,b) \in (\mathbb{Z}/N\mathbb{Z})^2} [\varphi(a, b)].$$

2. A $\Gamma_1(N)$-*structure* on E/S is a $\mathbb{Z}/N\mathbb{Z}$-structure on $E[N]/S$, i.e. a homomorphism

   $$\varphi : \mathbb{Z}/N\mathbb{Z} \to E[N](S)$$

   such that the Cartier divisor

   $$\sum_{a \in \mathbb{Z}/N\mathbb{Z}} [\varphi(a)]$$

   on E/S is a subgroup-scheme of E.

3. Finally, a $\Gamma_0(N)$-structure on E/S is a finite flat subgroup-scheme K of $E[N]$ which

[2]More generally, E could be any smooth curve over S equipped with an S-group scheme structure.

(a) is locally free of rank N, and

(b) locally f.p.p.f.[3] on S is cyclic. This means that S can be covered by schemes $T \to S$, which are f.p.p.f. over S, such that $K_T = K \times_S T$ admits a $\mathbb{Z}/n\mathbb{Z}$-generator for some $n \geq 1$, i.e. a group homomorphism

$$\varphi : \mathbb{Z}/n\mathbb{Z} \to E_T(T)$$

such that

$$K_T = \sum_{a \in \mathbb{Z}/n\mathbb{Z}} [\varphi(a)]$$

as effective Cartier divisors on E_T/T.

Each of these definitions gives rise to a corresponding *moduli problem*, i.e. a contravariant functor from the category of elliptic curves E/S over arbitrary base scheme to the category of sets. For $N \geq 1$, we define the moduli problems $[\Gamma(N)]$, $[\Gamma_1(N)]$ and $[\Gamma_0(N)]$ to be the functors taking an elliptic curve E/S to the set of $\Gamma(N)$-, $\Gamma_1(N)$, or $\Gamma_0(N)$-structures on E/S, respectively.

If $\mathcal{P}$ is any moduli problem, then for every elliptic curve E/S, there is a functor from the category of schemes over S to the category of sets defined by

$$T \mapsto \mathcal{P}(E_T/T),$$

where $E_T := E \times_S T$. We say that $\mathcal{P}$ is *relatively representable* if this functor is representable for every elliptic curve E/S. In this case, we denote the S-scheme representing this functor (for a fixed elliptic curve E/S) by $\mathcal{P}_{E/S}$. Katz and Mazur [20, First Main Theorem 5.1.1] proved that the moduli problems $[\Gamma(N)]$, $[\Gamma_1(N)]$, and $[\Gamma_0(N)]$ are all relatively representable.

We say that a moduli problem $\mathcal{P}$ is *representable* if it is representable as a functor. In this case, we denote the elliptic curve representing $\mathcal{P}$ by $\mathcal{E}/\mathfrak{M}(\mathcal{P})$. The base scheme $\mathfrak{M}(\mathcal{P})$ is called a *fine moduli scheme* for $\mathcal{P}$, it represents the functor from the category

[3] f.p.p.f. stands for *fidèlement plate de présentation finie*, i.e. faithfully flat and finitely presented.

of schemes to the category of sets taking a scheme S to the set of pairs $(E/S, \alpha)$ up to isomorphism, where

1. E is an elliptic curve over S, and

2. $\alpha \in \mathcal{P}(E/S)$ is a so-called "level $\mathcal{P}$ structure" on E/S.

If $\mathcal{P}$ is a relatively representable moduli problem, then we can define a *coarse moduli scheme* for $\mathcal{P}$, denoted $M(\mathcal{P})$, as follows. Let R be a ring in which some integer $N \geq 3$ is invertible. Choose a representable moduli problem $\mathcal{Q}$ which is finite étale and Galois over R, and let G be the Galois group of $\mathcal{Q}$. Note that such a moduli problem $\mathcal{Q}$ exists, for example take $[\Gamma(N)]$ if $N \geq 3$ and the Legendre problem (see [20, §2.2.8]) if $N = 2$. Then the "product" moduli problem $(\mathcal{P}, \mathcal{Q})$ defined by

$$(\mathcal{P}, \mathcal{Q})(E/S) := \mathcal{P}(E/S) \times \mathcal{Q}(E/S) \tag{6.1.1}$$

is representable (see [20, §4.3.4]), so we can define $M(\mathcal{P})$ locally on R by

$$M(\mathcal{P}) := \mathfrak{M}(\mathcal{P}, \mathcal{Q})/G. \tag{6.1.2}$$

This is a "best approximation" of a fine moduli scheme for $\mathcal{P}$, and is independent of the choice of representable moduli problem $\mathcal{Q}$. If $\mathcal{P}$ is representable, then $M(\mathcal{P}) = \mathfrak{M}(\mathcal{P})$.

In particular, since the moduli problems $[\Gamma(N)], [\Gamma_1(N)]$ and $[\Gamma_0(N)]$, for $N \geq 1$, are relatively representable, we can form the coarse moduli schemes

$$\mathcal{Y}(N) := M([\Gamma(N)]), \quad \mathcal{Y}_1(N) := M([\Gamma_1(N)]), \quad \mathcal{Y}_0(N) := M([\Gamma_0(N)]). \tag{6.1.3}$$

For $N > 2$, the moduli problems $[\Gamma(N)], [\Gamma_1(N)]$ and $[\Gamma_0(N)]$ are affine and rigid[4], hence representable (by [20, Scholie 4.7.0]), so $\mathcal{Y}(N)$, $\mathcal{Y}_1(N)$ and $\mathcal{Y}_0(N)$ are in fact fine moduli schemes for their respective moduli problems. On the other hand, the moduli problems

[4]This means that for any elliptic curve E, the group $\mathrm{Aut}\,(E)$ acts freely on the sets of $\Gamma(N)$-structures, $\Gamma_1(N)$-structures, and $\Gamma_0(N)$-structures (respectively).

$[\Gamma(2)], [\Gamma_1(2)]$ and $[\Gamma_0(2)]$ are not representable, since they are not rigid[5]. Hence $\mathcal{Y}(2)$, $\mathcal{Y}_1(2)$ and $\mathcal{Y}_0(2)$ are *not* fine moduli schemes.

For the rest of this chapter, I will study the coarse moduli scheme $\mathcal{Y}(2)$. The main result of the chapter will be a model for $\mathcal{Y}(2)$ as a scheme over $\mathbb{Z}$.

Remark 6.1.4. It is common to denote the moduli schemes for $[\Gamma(N)]$, $[\Gamma_1(N)]$ and $[\Gamma_0(N)]$ by $Y(N)$, $Y_1(N)$ and $Y_0(N)$ (for example, this is the notation used in [20]). However, I will reserve this notation for modular curves over $\mathbb{C}$ (as defined in § 2.2), and use the notation $\mathcal{Y}(N)$, $\mathcal{Y}_1(N)$ and $\mathcal{Y}_0(N)$ for the moduli schemes over $\mathbb{Z}$ to avoid confusion.

6.2 Embedding $Y(2)$ into a fiber product of modular curves

For now, I will consider the modular curves $Y(n)$, $Y_0(n)$ and $Y_1(n)$ over $\mathbb{C}$, as in § 2.2. Consider the topological space

$$Y := Y_0(2) \underset{Y_0(1)}{\times} Y_0(2), \tag{6.2.1}$$

where the fiber product is taken with respect to the projection map

$$Y_0(2) \xrightarrow{j} Y_0(1), \quad [E, C] \mapsto [E].$$

In this section, I will construct a natural embedding $u : Y(2) \hookrightarrow Y$, which will later be used, along with the integral model for $Y_0(2)$ given by Mestre [23, §5], to find an integral model for $Y(2)$.

[5]If E is an elliptic curve over a ring R in which 2 is invertible, then it has a Weierstrass equation of the form

$$E : y^2 = x^3 + a_2x^2 + a_4x + a_6,$$

and the automorphism of E given by

$$(x, y) \mapsto (x, -y)$$

relative to this Weierstrass equation acts trivially on the 2-torsion points $E[2]$ of E. So this automorphism also acts trivially on the $\Gamma(2)$-structures, $\Gamma_1(2)$-structures and $\Gamma_0(2)$-structures of E

In this setting, note that $Y_0(2) = Y_1(2)$, and so we can also write Y as

$$Y = Y_1(2) \underset{Y_1(1)}{\times} Y_1(2),$$

with the fiber product taken with respect to the projection map

$$Y_1(2) \xrightarrow{j} Y_1(1), \quad [E, P] \mapsto [E].$$

Then, points of Y are pairs $([E, P], [E', P']) \in Y_1(2)^2$ with $[E] = [E']$, i.e. with $E \cong E'$ over $\mathbb{C}$. Such a point can be written as $([E, P], [E, Q])$ for some $Q \in E[2]$. So points of Y are pairs $([E, P], [E, Q])$ of isomorphism classes of enhanced elliptic curves for $\Gamma_1(2)$ lying over the same isomorphism class of elliptic curves in $Y_1(1)$. Also, note that for $i = 1, 2$ we have projection maps

$$Y \xrightarrow{\pi_i} Y_1(2) \cong Y_0(2), \quad ([E, P_1], [E, P_2]) \mapsto [E, P_i].$$

Remark 6.2.2. It may be tempting to say that points of Y correspond to isomorphism classes of data (E, P, Q), where E is an elliptic curve and $P, Q \in E[2]$ are points of exact order 2 of E, which are not necessarily distinct. But, if we were to do this, we would have to be careful about when two triples (E, P, Q) and (E, P', Q') define the same point of Y. This happens if we have isomorphisms $f : (E, P) \to (E', P')$ and $g : (E, Q) \to (E', Q')$ of enhanced elliptic curves for $\Gamma_1(2)$, but f and g need not come from the same isomorphism of elliptic curves $E \to E'$. In particular, two triples (E, P, Q) and (E, P', Q') with the same base elliptic curve could define the same point of Y even if $(P, Q) \neq (P', Q')$. This happens when $\mathrm{Aut}\,(E)$ acts non-trivially on $E[2]$, which is the case only when $j(E) = 0$ or $j(E) = 1728$. To avoid this confusion, I will stick to my earlier notation for points of Y, namely writing them as pairs $([E, P], [E, Q])$.

Now, on the level of moduli problems, we have a map

$$Y(2) \xrightarrow{u} Y, \quad [E, P, Q] \mapsto ([E, P], [E, Q]). \tag{6.2.3}$$

I will start by checking that the function u corresponds to a map of complex manifolds

$$\Gamma(2)\backslash\mathcal{H} \to \Gamma_1(2)\backslash\mathcal{H} \underset{\mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H}}{\times} \Gamma_1(2)\backslash\mathcal{H}.$$

Let $\tau \in \mathcal{H}$. It corresponds to the enhanced elliptic-curve $\left(E_\tau, \frac{1}{2}, \frac{\tau}{2}\right)$ for $\Gamma(2)$, which maps under u to the pair $\left(\left[E_\tau, \frac{1}{2}\right], \left[E_\tau, \frac{\tau}{2}\right]\right)$. The data $\left[E_\tau, \frac{1}{2}\right] \in Y_1(2)$ corresponds to $[\tau] \in \Gamma_1(2)\backslash\mathcal{H}$. Also, by multiplying by $-\frac{1}{\tau}$, we have $\left[E_\tau, \frac{\tau}{2}\right] = \left[E_{-1/\tau}, \frac{1}{2}\right]$, which corresponds to $\left[-\frac{1}{\tau}\right] \in \Gamma_1(2)\backslash\mathcal{H}$. So u should correspond to the map of complex manifolds

$$\begin{aligned} \Gamma(2)\backslash\mathcal{H} &\xrightarrow{\tilde{u}} \Gamma_0(2)\backslash\mathcal{H} \underset{\Gamma_0(1)\backslash\mathcal{H}}{\times} \Gamma_0(2)\backslash\mathcal{H} \\ [\tau] &\longmapsto \left[\tau, -\tfrac{1}{\tau}\right]. \end{aligned} \tag{6.2.4}$$

We check that the map $\tilde{u}$ is well-defined.

We start with the map

$$\begin{aligned} \mathcal{H} &\longrightarrow \Gamma_0(2)\backslash\mathcal{H} \times \Gamma_0(2)\backslash\mathcal{H} \\ \tau &\longmapsto \left([\tau], \left[-\tfrac{1}{\tau}\right]\right). \end{aligned}$$

Since $-\frac{1}{\tau} = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)\tau \in \mathrm{SL}_2(\mathbb{Z})\tau$, the image of this map lies in the fiber product

$$\Gamma_1(2)\backslash\mathcal{H} \underset{\Gamma_1(1)\backslash\mathcal{H}}{\times} \Gamma_1(2)\backslash\mathcal{H} = \{([\tau], [\tau']) : \mathrm{SL}_2(\mathbb{Z})\tau = \mathrm{SL}_2(\mathbb{Z})\tau'\} \subseteq \Gamma_1(2)\backslash\mathcal{H} \times \Gamma_1(2)\backslash\mathcal{H}.$$

So we need to show that this map is $\Gamma(2)$-invariant. But this is clear, since $\Gamma(2) \subseteq \Gamma_1(2)$.

Now, we'd like to show that the map $Y(2) \xrightarrow{u} Y$ is in fact a map of algebraic varieties. However, we run into a problem, namely that $Y(2)$ is not a fine moduli space, so maps on

the moduli data do not necessarily correspond to maps of algebraic varieties $Y(2) \to Y$. To solve this, we will add extra data to our enhanced elliptic curves, namely a $\Gamma(m)$-structure, for some odd integer $m > 2$, in order to get fine moduli spaces.

Fix an odd integer $m > 2$. Define

$$\Gamma(2, m) := \Gamma_1(2) \cap \Gamma(m). \tag{6.2.5}$$

This is a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$ of level $2m$, since $\Gamma(2m) \subseteq \Gamma(m)$ and $\Gamma(2m) \subseteq \Gamma(2) \subseteq \Gamma_1(2)$. I'll show that $\Gamma(2, m)\backslash\mathcal{H}$ is a moduli space for isomorphism classes elliptic curves with both $\Gamma_1(2)$- and $\Gamma(m)$-structures.

Definition 6.2.6. Let $m > 2$ be an odd integer. A $\Gamma(2, m)$-*structure* on an elliptic curve $E/\mathbb{C}$ is a pair (P, φ), where P is a $\Gamma_1(n)$-structure on E, i.e. a point of E of order 2, and φ is a $\Gamma(m)$-structure on E, i.e. a symplectic isomorphism $(\mathbb{Z}/m\mathbb{Z})^2 \to E[m]$. We then call (E, P, φ) a *enhanced elliptic curve for* $\Gamma(2, m)$.

An *isomorphism* $f : (E, P, \varphi) \to (E', P', \varphi')$ of enhanced elliptic curves for $\Gamma(2, m)$ is an isomorphism $f : E \to E'$ of elliptic curves such that $f : (E, P) \to (E', P')$ and $f : (E, \varphi) \to (E', \varphi')$ are both isomorphisms of enhanced elliptic curves. We denote the set of isomorphism classes of enhanced elliptic curves for $\Gamma(2, m)$ over $\mathbb{C}$ by $Y(2, m)$.

Note that giving a $\Gamma(2, m)$-structure on E is equivalent to giving data (E, P, Q, R), where P is a point of order 2 and (Q, R) is a basis for $E[m]$ with $e_m(P, Q) = \zeta_m$.

Proposition 6.2.7. *We have a bijection*

$$\begin{array}{ccc} \Gamma(2, m)\backslash\mathcal{H} & \longrightarrow & Y(2, m) \\ \Gamma(2, m)\tau & \longmapsto & \left[\mathbb{C}/(\mathbb{Z} + \tau\mathbb{Z}), \frac{1}{2}, \frac{1}{m}, \frac{\tau}{m}\right]. \end{array}$$

Proof. Consider the map

$$\begin{array}{ccc} \mathcal{H} & \xrightarrow{f} & Y(2, m) \\ \tau & \longmapsto & \left[\mathbb{C}/(\mathbb{Z} + \tau\mathbb{Z}), \frac{1}{2}, \frac{1}{m}, \frac{\tau}{m}\right]. \end{array}$$

We need to show that this is surjective with kernel $\Gamma(2,m)$.

Let (E,P,Q,R) be an enhanced elliptic curve for $\Gamma(2,m)$. Then (E,P) is an enhanced elliptic curve for $\Gamma_1(2)$ and (E,Q,R) is an enhanced elliptic curve for $\Gamma(m)$. So by Proposition 2.2.6, there exist $\tau,\tau' \in \mathcal{H}$ such that $(E,P) \cong \left(\mathbb{C}/(\mathbb{Z}+\tau\mathbb{Z}), \frac{1}{2}\right)$ and $(E,Q,R) \cong \left(\mathbb{C}/(\mathbb{Z}+\tau'\mathbb{Z}), \frac{1}{m}, \frac{\tau'}{m}\right)$. Then $\mathbb{C}/(\mathbb{Z}+\tau\mathbb{Z}) \cong E \cong \mathbb{C}/(\mathbb{Z}+\tau'\mathbb{Z})$, so $\tau' = \gamma\tau$ for some $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$. Multiplying by $(c\tau+d)$ gives

$$\left(\mathbb{C}/(\mathbb{Z}+\tau'\mathbb{Z}), \frac{1}{m}, \frac{\tau'}{m}\right) = \left(\mathbb{C}/(\mathbb{Z}+\gamma\tau\mathbb{Z}), \frac{1}{m}, \frac{\gamma\tau}{m}\right) \cong \left(\mathbb{C}/(\mathbb{Z}+\tau\mathbb{Z}), \frac{c\tau+d}{m}, \frac{a\tau+b}{m}\right).$$

So

$$(E,P,Q,R) \cong \left(\mathbb{C}/(\mathbb{Z}+\tau\mathbb{Z}), \frac{1}{2}, \frac{c\tau+d}{m}, \frac{a\tau+b}{m}\right).$$

We need the following lemma:

Lemma 6.2.8. *There exists $\gamma' \in \mathrm{SL}_2(\mathbb{Z})$ such that*

$$\gamma' \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mod 2$$

and $\gamma' \equiv \gamma \mod m$.

Proof. We have $\mathrm{SL}_2(\mathbb{Z})/\Gamma(n) \cong \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$ for $n \geq 1$. Also, since m is odd, the Chinese Remainder Theorem gives that

$$\mathrm{SL}_2(\mathbb{Z}/2m\mathbb{Z}) \cong \mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}) \cong \mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z}).$$

So

$$\mathrm{SL}_2(\mathbb{Z})/\Gamma(2m) \cong \mathrm{SL}_2(\mathbb{Z})/\Gamma(2) \times \mathrm{SL}_2(\mathbb{Z})/\Gamma(m).$$

Hence we can find $\gamma_0' \in \mathrm{SL}_2(\mathbb{Z})/\Gamma(2m)$ such that $\gamma_0' \equiv \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \mod \Gamma(2)$ and $\gamma_0' \equiv \gamma \mod \Gamma(m)$, i.e. such that $\gamma_0' \equiv \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \mod 2$ and $\gamma_0' \equiv \gamma \mod m$. Lifting γ_0' to $\gamma' \in \mathrm{SL}_2(\mathbb{Z})$ gives the desired matrix. □

Let $\gamma' = \left(\begin{smallmatrix} a' & b' \\ c' & d' \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ be as in the lemma. Then, by multiplying by $c'\tau + d'$,

$$\begin{aligned}\left(\mathbb{C}/(\mathbb{Z}+\gamma'\tau\mathbb{Z}), \frac{1}{2}, \frac{1}{m}, \frac{\gamma'\tau}{m}\right) &\cong \left(\mathbb{C}/(\mathbb{Z}+\tau\mathbb{Z}), \frac{c'\tau+d'}{2}, \frac{c'\tau+d'}{m}, \frac{a'\tau+b'}{m}\right) \\ &= \left(\mathbb{C}/(\mathbb{Z}+\tau\mathbb{Z}), \frac{1}{2}, \frac{c\tau+d}{m}, \frac{a\tau+b}{m}\right) \\ &\cong (E, P, Q, R)\end{aligned}$$

This shows that f is surjective.

Now, we need to show that $f(\tau) = f(\tau')$ if and only if τ and τ' are in the same $\Gamma(2,m)$-orbit. First, if $\tau = \gamma\tau$ for some $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma(2,m)$, then multiplication by $c\tau + d$ gives an isomorphism

$$\left(\mathbb{C}/(\mathbb{Z}+\tau'\mathbb{Z}), \frac{1}{2}, \frac{1}{m}, \frac{\tau'}{m}\right) = \left(\mathbb{C}/(\mathbb{Z}+\gamma\tau\mathbb{Z}), \frac{1}{2}, \frac{1}{m}, \frac{\gamma\tau}{m}\right) \xrightarrow{\sim} \left(\mathbb{C}/(\mathbb{Z}+\tau\mathbb{Z}), \frac{1}{2}, \frac{1}{m}, \frac{\tau}{m}\right).$$

Conversely, suppose that

$$\left(\mathbb{C}/(\mathbb{Z}+\tau'\mathbb{Z}), \frac{1}{2}, \frac{1}{m}, \frac{\tau'}{m}\right) \cong \left(\mathbb{C}/(\mathbb{Z}+\tau\mathbb{Z}), \frac{1}{2}, \frac{1}{m}, \frac{\tau}{m}\right).$$

Then since $\mathbb{C}/(\mathbb{Z}+\tau\mathbb{Z}) \cong \mathbb{C}/(\mathbb{Z}+\tau'\mathbb{Z})$, $\tau' = \gamma\tau$ for some $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$, and the isomorphism $\mathbb{C}/(\mathbb{Z}+\tau'\mathbb{Z}) = \mathbb{C}/(\mathbb{Z}+\gamma\tau\mathbb{Z}) \xrightarrow{\sim} \mathbb{C}/(\mathbb{Z}+\tau\mathbb{Z})$ is given by multiplication by $c\tau + d$. Choose γ so that this isomorphism induces the isomorphism of enhanced elliptic curves for $\Gamma(2,m)$ from $\left(\mathbb{C}/(\mathbb{Z}+\tau'\mathbb{Z}), \frac{1}{2}, \frac{1}{m}, \frac{\tau'}{m}\right)$ to $\left(\mathbb{C}/(\mathbb{Z}+\tau\mathbb{Z}), \frac{1}{2}, \frac{1}{m}, \frac{\tau}{m}\right)$. Then

$$\left(\mathbb{C}/(\mathbb{Z}+\tau\mathbb{Z}), \frac{c\tau+d}{2}, \frac{c\tau+d}{m}, \frac{a\tau+b}{m}\right) = \left(\mathbb{C}/(\mathbb{Z}+\tau\mathbb{Z}), \frac{1}{2}, \frac{1}{m}, \frac{\tau}{m}\right),$$

so we must have $c \equiv 0 \mod 2$, $c \equiv b \equiv 0 \mod m$ and $a \equiv d \equiv 1 \mod m$, so $\gamma \in \Gamma(2,m)$. $\square$

Now, note that we have a map

$$Y(2,m) \longrightarrow Y(m),$$

$$[E,P,Q,R] \longmapsto [E,Q,R]\,.$$

So we can form the fiber product

$$Y_m := Y(2,m) \underset{Y(m)}{\times} Y(2,m).$$

Points of Y_m are pairs $([E,P,Q,R],[E',P',Q',R'])$ with $(E,Q,R) \cong (E',Q',R')$. Note that if (P,Q) is a basis for $E[2m]$ with $e_{2m}(P,Q) = \zeta_{2m}$, then

1. mP, mQ are points of order 2,
2. $(2P, 2Q)$ is a basis for $E[2m]$, and
3. if $\gamma \in \mathrm{SL}_2(\mathbb{Z}/2m\mathbb{Z})$ is the change of basis matrix from $\left(\frac{1}{2m}, \frac{\tau}{2m}\right)$ to (P,Q), so

$$\begin{pmatrix} P \\ Q \end{pmatrix} = \gamma \begin{pmatrix} 1/(2m) \\ \tau/(2m) \end{pmatrix},$$

then

$$\begin{pmatrix} 2P \\ 2Q \end{pmatrix} = \gamma \begin{pmatrix} 1/m \\ \tau/m \end{pmatrix}.$$

So

$$e_m(2P,2Q) = e^{2\pi i \det\gamma/m} = \zeta_m,$$

which means that $(2P,2Q)$ is a $\Gamma(m)$-structure on E.

Therefore, we have a map

$$\begin{aligned} Y(2m) &\xrightarrow{\quad u_m \quad} Y_m \\ [E,P,Q] &\longmapsto ([E,mP,2P,2Q]\,,[E,mQ,2P,2Q])\,. \end{aligned} \tag{6.2.9}$$

Since $Y(2m)$ is a fine moduli space, this corresponds to a morphism of varieties $Y(2m) \to Y(m)$.

Let us find the corresponding map from $\Gamma(2m)\backslash\mathcal{H}$ to $\Gamma(2,m)\backslash\mathcal{H} \underset{\Gamma(m)\backslash\mathcal{H}}{\times} \Gamma(2,m)\backslash\mathcal{H}$. The point $[\tau] \in \Gamma(2m)\backslash\mathcal{H}$ corresponds to the isomorphism class of $\left(\mathbb{C}/(\mathbb{Z}+\tau\mathbb{Z}), \frac{1}{2m}, \frac{\tau}{2m}\right)$, which maps under u_m to the pair

$$\left(\left[\mathbb{C}/(\mathbb{Z}+\tau\mathbb{Z}), \frac{1}{2}, \frac{1}{m}, \frac{\tau}{m}\right], \left[\mathbb{C}/(\mathbb{Z}+\tau\mathbb{Z}), \frac{\tau}{2}, \frac{1}{m}, \frac{\tau}{m}\right]\right) \in Y_m.$$

Note that

$$\left[\mathbb{C}/(\mathbb{Z}+\tau\mathbb{Z}), \frac{\tau}{2}, \frac{1}{m}, \frac{\tau}{m}\right] = \left[\mathbb{C}/(\mathbb{Z}+\gamma_0\tau\mathbb{Z}), \frac{1}{2}, \frac{1}{m}, \frac{\gamma_0\tau}{m}\right],$$

where

$$\gamma_0 = \begin{pmatrix} 1+m & -m \\ m & 1-m \end{pmatrix}.$$

Indeed, since $\gamma_0 \in \mathrm{SL}_2(\mathbb{Z})$, multiplication by $m\tau + (1-m)$ gives an isomorphism

$$\mathbb{C}/(\mathbb{Z}+\gamma_0\tau\mathbb{Z}) \xrightarrow{\sim} \mathbb{C}/(\mathbb{Z}+\tau\mathbb{Z}).$$

And

1. $\frac{m\tau+(1-m)}{2} \equiv \tau \mod \mathbb{Z}+\tau\mathbb{Z}$ since m is odd,
2. $\frac{m\tau+(1-m)}{m} \equiv \frac{1}{m} \mod \mathbb{Z}+\tau\mathbb{Z}$, and
3. $\frac{m\tau^2+(1-m)\tau}{m} \equiv \frac{\tau}{m} \mod \mathbb{Z}+\tau\mathbb{Z}$.

So for $[\tau] \in \Gamma(2m)\backslash\mathcal{H}$,

$$u_m\left(\left[\mathbb{C}/(\mathbb{Z}+\tau\mathbb{Z}), \frac{1}{2m}, \frac{\tau}{2m}\right]\right) = \left(\left[\mathbb{C}/(\mathbb{Z}+\tau\mathbb{Z}), \frac{1}{2}, \frac{1}{m}, \frac{\tau}{m}\right], \left[\mathbb{C}/(\mathbb{Z}+\gamma_0\tau\mathbb{Z}), \frac{1}{2}, \frac{1}{m}, \frac{\gamma_0\tau}{m}\right]\right).$$

So u_m corresponds to the map

$$\begin{array}{c} \Gamma(2m)\backslash\mathcal{H} \xrightarrow{\tilde{u}_m} \Gamma(2,m)\backslash\mathcal{H} \underset{\Gamma(m)\backslash\mathcal{H}}{\times} \Gamma(2,m)\backslash\mathcal{H} \\ [\tau] \longmapsto ([\tau], [\gamma_0\tau]), \end{array} \tag{6.2.10}$$

where

$$\gamma_0 = \begin{pmatrix} 1+m & -m \\ m & 1-m \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}).$$

Let us check that this map is well defined. To start, we have a map

$$\begin{array}{c} \mathcal{H} \longrightarrow \Gamma(2,m)\backslash\mathcal{H} \times \Gamma(2,m)\backslash\mathcal{H} \\ [\tau] \longmapsto ([\tau], [\gamma_0\tau]). \end{array}$$

Note that $\gamma_0 \in \Gamma(m)$, so the image of this map lies in the fiber product

$$\Gamma(2,m)\backslash\mathcal{H} \underset{\Gamma(m)\backslash\mathcal{H}}{\times} \Gamma(2,m)\backslash\mathcal{H}.$$

So we need to show that it is $\Gamma(2m)$-invariant. But this is clear, since $\Gamma(2m) \subseteq \Gamma(2,m)$, so if $\tau \in \mathcal{H}$ and $\gamma \in \Gamma(2m)$, then $\Gamma(2,m)\gamma\tau = \Gamma(2,m)\tau$ and $\Gamma(2,m)\gamma\gamma_0\tau = \Gamma(2,m)\gamma_0\tau$.

To conclude, I've shown that the map $u : Y(2) \to Y$ defined in Equation (6.2.3) corresponds to the map of complex manifolds

$$\tilde{u} : \Gamma(2)\backslash\mathcal{H} \to \Gamma_0(2)\backslash\mathcal{H} \underset{\Gamma_0(1)\backslash\mathcal{H}}{\times} \Gamma_0(2)\backslash\mathcal{H}$$

defined in Equation (6.2.4). Moreover, if we fix an odd integer $m > 2$, then u sits in a commutative diagram

$$\begin{array}{ccc} Y(2,m) & \xrightarrow{u_m} & Y_m \\ \downarrow & & \downarrow \\ Y(2) & \xrightarrow{u} & Y, \end{array} \tag{6.2.11}$$

where u_m is the map of moduli problems defined in Equation (6.2.9). This corresponds

to a diagram of maps of complex manifolds

$$\begin{array}{ccc} \Gamma(2,m)\backslash\mathcal{H} & \xrightarrow{\tilde{u}_m} & \Gamma(2,m)\backslash\mathcal{H} \underset{\Gamma(m)\backslash\mathcal{H}}{\times} \Gamma(2,m)\backslash\mathcal{H} \\ \downarrow & & \downarrow \\ \Gamma(2)\backslash\mathcal{H} & \xrightarrow{\tilde{u}} & \Gamma_0(2)\backslash\mathcal{H} \underset{\Gamma_0(1)\backslash\mathcal{H}}{\times} \Gamma_0(2)\backslash\mathcal{H}, \end{array} \tag{6.2.12}$$

where $\tilde{u}_m$ is the map defined in Equation (6.2.10). Since $Y(2m)$ and Y_m are fine moduli spaces, the map $\tilde{u}_m$ corresponds to a map of algebraic curves $u_m^{\text{alg}} : Y(2m) \to Y_m$. Then Equation (6.2.12) shows that u_m^{alg} induces a map of algebraic curves $u^{\text{alg}} : Y(2) \to Y$.

In subsequent sections, I will denote this algebraic map u^{alg} simply by u.

6.3 An integral model for $Y_0(2)$

The canonical modular polynomial for $\Gamma_0(2)$ is

$$\psi_2(x, j) := (x + 16)^3 - jx.$$

It is the relation satisfied by the modular j-invariant $j(z)$ and the hauptmodul

$$x(z) = 2^{12}\frac{\Delta(2z)}{\Delta(z)} \tag{6.3.1}$$

for $X_0(2)$. Here,

$$\Delta(z) = q\prod_{n\geq 1}(1-q^n)^{24}, \quad q = e^{2\pi iz},$$

is the modular discriminant function. Mestre [23] says that

$$\psi_2(x, j) = 0 \tag{6.3.2}$$

is a model for the modular curve $X_0(2)$ over $\mathbb{Z}$, but does not provide a proof. In this section, I will prove (see Theorem 6.3.6) that Equation (6.3.2) is indeed an integral model for $X_0(2)$.

Remark 6.3.3. Another classical model for $X_0(2)$ is given by the classical modular polynomial

$$\Phi_2(x,y) := x^3 + y^2 - x^2y^2 + 1488x^2y + 1488xy^2 - 162000x^2 - 162000y^2 + 40773375xy \\ + 8748000000x + 8748000000y - 157464000000000. \tag{6.3.4}$$

This is the polynomial determined by the relation $\Phi_2(j, j_2) = 0$, where j is the modular j-invariant and j_2 is the modular function $j_2(z) = j(2z)$. However, one can check that the curve $\Phi_2(x, y) = 0$ has a singularity at the point $(-3375, -3375)$, so this is not a non-singular model for $X_0(2)$ over $\mathbb{Q}$. This means that $\operatorname{Spec} \mathbb{Z}[x, y]/(\Phi_2(x, y))$ is not isomorphic to the coarse moduli scheme $\mathcal{Y}_0(2)$, since the latter is regular (hence normal).

On the other hand, it is easy to see that the curve $\psi_2(x, j) = 0$ is non-singular over any field who's characteristic is not 2, so Equation (6.3.2) *does* define a non-singular model for $X_0(2)$ over $\mathbb{Q}$. In a field k of characteristic 2, we have

$$\psi_2(x, j) = x(x^2 - j) \mod 2, \tag{6.3.5}$$

so the curve $\psi_2(x, j) = 0$ over k is the union two copies of $\mathbb{A}^1_k$ meeting transversally at the singular point $(0, 0)$.

Theorem 6.3.6. *The coarse moduli scheme $\mathcal{Y}_0(2)$ is isomorphic to the scheme*

$$\mathcal{G}_0(2) := \operatorname{Spec} \mathbb{Z}[x, j]/(\psi_2(x, j)).$$

Proof. Recall that

$$\mathcal{Y}_0(1) = \operatorname{Spec} \mathbb{Z}[j]$$

is the coarse moduli scheme for $[\Gamma_0(1)]$. Let $\pi : \mathcal{Y}_0(2) \to \mathcal{Y}_0(1)$ be the morphism of schemes corresponding to the natural transformation between the moduli problems $[\Gamma_0(2)]$ and $[\Gamma_0(1)]$ obtained by *forgetting* the $\Gamma_0(2)$-structure on an elliptic curve E/S. By [20, Theorem 5.1.1], the moduli problem $[\Gamma_0(2)]$ is finite, flat, and regular (hence normal). So

$\mathcal{Y}_0(2)$ is normal by [20, Lemma 8.1.2], and the morphism π is finite by [20, Proposition 8.2.2].

On the other hand, there is a morphism of schemes $\pi_{\mathcal{G}} : \mathcal{G}_0(2) \to \mathcal{Y}_0(1)$ coming from the inclusion ring homomorphism

$$\mathbb{Z}[j] \to \mathbb{Z}[x, j]/(\psi_2(x, j)).$$

The morphism $\pi_{\mathcal{G}}$ is finite, since we can write

$$\mathbb{Z}[x, j]/(\psi_2(x, j)) = \mathbb{Z}[j] \oplus \mathbb{Z}[j]x \oplus \mathbb{Z}[j]x^2.$$

Moreover, a calculation using the programming language SINGULAR [10] shows that $\mathbb{Z}[x, j]/(\psi_2(x, j))$ is integrally closed[6], hence $\mathcal{G}_0(2)$ is normal.

Now, I will need the following lemma:

Lemma 6.3.7. *There exists an element $x \in \mathcal{O}(\mathcal{Y}_0(2))$ satisfying $\psi_2(x, j) = 0$.*

Proof. Let $x(z)$ be the hauptmodul defined in Equation (6.3.1). This is a modular form over $\mathbb{C}$ of weight 0 and level $\Gamma_0(2)$. Its q-expansion,

$$x(z) = 2^{12} q \prod_{n \geq 1} (1 - q^n)^{24}, \quad q = e^{2\pi i z},$$

has coefficients in $\mathbb{Z}[1/2]$ (in fact in $\mathbb{Z}$), so by the q-expansion principle (see [6, Proposition 1.8]), $x(z)$ is actually a modular form of weight 0 and level $\Gamma_0(2)$ over $\mathbb{Z}[1/2]$, hence an element of $\mathcal{O}\left(\mathcal{Y}_0(2)_{\mathbb{Z}[1/2]}\right)$ Then, since $\mathcal{Y}_0(2)$ is normal (so $\mathcal{O}(\mathcal{Y}_0(2))$ is integrally closed), and x satisfies the monic polynomial $\psi_2(x, j) = 0$ over $\mathcal{O}(\mathcal{Y}_0(2))$, we have $x \in \mathcal{O}(\mathcal{Y}_0(2))$. □

Hence we have a ring homomorphism

$$\mathcal{O}(\mathcal{Y}_0(2)) \to \mathcal{O}(\mathcal{G}_0(2)) = \mathbb{Z}[x, j]/(\psi_2(x, j)),$$

[6] By which I mean that it is integrally closed in its field of fractions.

sending $j \in \mathbb{Z}[x,j]/(\psi_2(x,j))$ to the function $j \in \mathcal{O}(\mathcal{Y}_0(2))$, and $x \in \mathbb{Z}[x,j]/(\psi_2(x,j))$ to the function $x \in \mathcal{O}(\mathcal{Y}_0(2))$ from Lemma 6.3.7. Since $\mathcal{Y}_0(2)$ and $\mathcal{G}_0(2)$ are affine, this gives a morphism of $\mathcal{Y}_0(1)$-schemes

$$\begin{array}{ccc} \mathcal{Y}_0(2) & \xrightarrow{\quad f \quad} & \mathcal{G}_0(2) \\ & {\scriptstyle\pi}\searrow \quad \swarrow{\scriptstyle\pi_{\mathcal{G}}} & \\ & \mathcal{Y}_0(1) & \end{array}$$

Since π and $\pi_{\mathcal{G}}$ are both finite morphisms, f is finite as well. So, since $\mathcal{G}_0(2)$ is normal, Zariski's Main Theorem [27, Lemma 37.38.1, Tag 03GW] implies that $f(\mathcal{Y}_0(2))$ is an open subscheme of $\mathcal{G}_0(2)$ and f is an isomorphism onto $f(\mathcal{Y}_0(2))$.

Now, since $\mathcal{G}_0(2)$ is normal, it is integral, hence irreducible. So $f(\mathcal{Y}_0(2))$ is dense in $\mathcal{G}_0(2)$, and $f : \mathcal{Y}_0(2) \to \mathcal{G}_0(2)$ is a birational isomorphism. Finally, since $\mathcal{Y}_0(2)$ and $\mathcal{G}_0(2)$ are normal, this means that f is an isomorphism. □

6.4 The embedding u over $\mathbb{Z}[1/2]$

As before, let $Y := Y_0(2) \times_{Y_0(1)} Y_0(2)$. Recall that we have a map $u : Y(2) \to Y$ defined on the corresponding moduli problems by

$$[E, P, Q] \mapsto ([E, P], [E, Q]).$$

In § 6.2, we saw that this gives a map of algebraic varieties.

We can construct a similar map on the moduli scheme $\mathcal{Y}(2)$. Define

$$\mathcal{Y} := \mathcal{Y}_0(2) \underset{\mathcal{Y}_0(1)}{\times} \mathcal{Y}_0(2). \tag{6.4.1}$$

We have a morphism of functors ρ_1 from the moduli problem $[\Gamma(2)]$ to the moduli problem $[\Gamma_0(2)]$, sending the $\Gamma(2)$-structure

$$\varphi : (\mathbb{Z}/2\mathbb{Z})^2 \to E[2](S)$$

on an elliptic curve E/S to the $\Gamma_0(2)$-structure to the sub-group scheme

$$\rho_1(\varphi) := [\varphi(0,0)] + [\varphi(1,0)]$$

of $E[2]$, which is a $\Gamma_0(2)$-structure on E/S. We can use the same trick as was used in § 6.2 to see that this functor gives a morphism of schemes form $\mathcal{Y}(2)$ to $\mathcal{Y}_0(2)$. We do this affine locally over $\mathbb{Z}$. Let R be a ring, and assume without loss of generality that some integer $m > 2$ is invertible in R. Then, over R, we have

$$\mathcal{Y}(2) = \mathfrak{M}([\Gamma(2)], [\Gamma(m)])/\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}), \quad \mathcal{Y}_0(2) = \mathfrak{M}([\Gamma_0(2)], [\Gamma(m)])/\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}).$$

The functor ρ_1 induces a functor from $([\Gamma(2)], [\Gamma(m)])$ to $([\Gamma_0(2)], [\Gamma(m)])$, which operates as ρ_1 on $\Gamma(2)$-structures and trivially on $\Gamma(m)$-structures. Since $\mathfrak{M}([\Gamma(2)], [\Gamma(m)])$ and $\mathfrak{M}([\Gamma_0(2)], [\Gamma(m)])$ represent $([\Gamma(2)], [\Gamma(m)])$ and $([\Gamma_0(2)], [\Gamma(m)])$, this gives a morphism of schemes

$$\tilde{\rho}_1 : \mathfrak{M}([\Gamma(2)], [\Gamma(m)]) \to \mathfrak{M}([\Gamma_0(2)], [\Gamma(m)]),$$

which is $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$-invariant since ρ_1 operates trivially on $\Gamma(m)$-structures. Since $\tilde{\rho}_1$ is $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$-invariant, it induces a map of $\mathcal{Y}_0(1)$-schemes

$$u_1 : \mathfrak{M}([\Gamma(2)], [\Gamma(m)])/\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}) \to \mathfrak{M}([\Gamma_0(2)], [\Gamma(m)])/\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}),$$

i.e. $u_1 : \mathcal{Y}(2) \to \mathcal{Y}_0(2)$.

Similarly, we have a second morphism of functors ρ_2 from $[\Gamma(2)]$ to $[\Gamma_0(2)]$, sending the $\Gamma(2)$-structure

$$\varphi : (\mathbb{Z}/2\mathbb{Z})^2 \to E[2](S)$$

on an elliptic curve E/S to the $\Gamma_0(2)$-structure

$$\rho_2(\varphi) := [\varphi(0,0)] + [\varphi(0,1)].$$

The same argument as above shows that ρ_2 induces a morphism of $\mathcal{Y}_0(1)$-schemes u_2 :

$\mathcal{Y}(2) \to \mathcal{Y}_0(2)$.

So we have a commutative diagram of scheme morphisms

$$\begin{array}{ccc} \mathcal{Y}(2) & \xrightarrow{u_2} & \mathcal{Y}_0(2) \\ {\scriptstyle u_1}\downarrow & & \downarrow \\ \mathcal{Y}_0(2) & \longrightarrow & \mathcal{Y}_0(1), \end{array} \tag{6.4.2}$$

which gives us a morphism of schemes

$$u : \mathcal{Y}(2) \to \mathcal{Y}_0(2) \underset{\mathcal{Y}_0(1)}{\times} \mathcal{Y}_0(2) = \mathcal{Y}. \tag{6.4.3}$$

In the remainder of this section, I will study the extension by scalars to $\mathbb{Z}[1/2]$ of the morphism u. If S is a scheme over $\mathbb{Z}$, write

$$S_{\mathbb{Z}[1/2]} := S \underset{\text{Spec } \mathbb{Z}}{\times} \text{Spec } \mathbb{Z}[1/2].$$

Consider the morphism

$$u : \mathcal{Y}(2)_{\mathbb{Z}[1/2]} \to \mathcal{Y}_{\mathbb{Z}[1/2]} = \mathcal{Y}_0(2)_{\mathbb{Z}[1/2]} \underset{\mathcal{Y}_0(1)_{\mathbb{Z}[1/2]}}{\times} \mathcal{Y}_0(2)_{\mathbb{Z}[1/2]}.$$

In § 6.3, I showed that $\mathcal{Y}_0(2)$ is isomorphic to

$$\mathcal{G}_0(2) := \text{Spec } \mathbb{Z}[x, j]/(\psi_2(x, j))$$

over $\mathbb{Z}$, where

$$\psi_2(x, j) := (x + 16)^3 - jx$$

is the canonical modular polynomial for $\Gamma_0(2)$. So

$$\mathcal{Y}_0(2)_{\mathbb{Z}[1/2]} \cong \mathcal{G}_0(2)_{\mathbb{Z}[1/2]} = \text{Spec } \mathbb{Z}[1/2, x, j]/(\psi_2(x, j)).$$

Note that $\psi_2(x,j) = 0$ gives

$$\frac{1}{x} = \frac{1}{16^3}\left(j - x^2 - 48x - 768\right),$$

so x is invertible in $\mathbb{Z}[1/2, x, j]/(\psi_2(x,j))$ and

$$j = j(x) := \frac{(x+16)^3}{x}.$$

So we can write

$$\mathcal{Y}_0(2)_{\mathbb{Z}[1/2]} \cong \operatorname{Spec} \mathbb{Z}[1/2, x, 1/x].$$

Then we can write $\mathcal{Y}_{\mathbb{Z}[1/2]}$ as

$$\begin{aligned}
\mathcal{Y}_{\mathbb{Z}[1/2]} &\cong \operatorname{Spec} \mathbb{Z}[1/2, x, 1/x] \underset{\operatorname{Spec} \mathbb{Z}[1/2,j]}{\times} \operatorname{Spec} \mathbb{Z}[1/2, x, 1/x] \\
&\cong \operatorname{Spec} \left(\mathbb{Z}[1/2, x, 1/x] \underset{\mathbb{Z}[1/2,j]}{\otimes} \mathbb{Z}[1/2, x, 1/x] \right) \\
&\cong \operatorname{Spec} \mathbb{Z}[1/2, x_1, x_2, 1/x_1x_2]/(x_2 j(x_1) - x_1 j(x_2)) \\
&= \operatorname{Spec} \mathbb{Z}[1/2, x_1, x_2, 1/x_1x_2]/(x_1 - x_2)(G(x_1, x_2)),
\end{aligned}$$

where

$$G(x_1, x_2) := x_1^2 x_2 + x_1 x_2^2 + 48 x_1 x_2 - 16^3. \tag{6.4.4}$$

Proposition 6.4.5. *The pullback map*

$$u^* : \mathcal{O}\left(\mathcal{Y}_{\mathbb{Z}[1/2]}\right) = \mathbb{Z}[1/2, j, x_1, x_2]/(\psi_2(x_1, j), \psi_2(x_2, j)) \to \mathcal{O}\left(\mathcal{Y}(2)_{\mathbb{Z}[1/2]}\right).$$

is given by

$$u^*(x_1) = x_1(\lambda) := 2^4 \frac{\lambda^2}{1-\lambda}, \quad u^*(x_2) = x_2(\lambda) := 2^4 \frac{(1-\lambda)^2}{\lambda}.$$

Proof. By the universal property of fiber products, u is determined by the morphisms

$$u_i = \pi_i \circ u : \mathcal{Y}(2)_{\mathbb{Z}[1/2]} \to \mathcal{Y}_0(2)_{\mathbb{Z}[1/2]} \quad i = 1, 2,$$

where $\pi_1, \pi_2 : \mathcal{Y}_{\mathbb{Z}[1/2]} \to \mathcal{Y}_0(2)_{\mathbb{Z}[1/2]}$ are the projection maps onto the first and second coordinate, respectively. So it is enough to find the pullback maps u_1^* and u_2^*.

To do this, I will construct a hauptmodul $\tilde{x}$ for $X_0(2)$ which is a function of λ, and show that this hauptmodul is in fact the function

$$x(z) := 2^{12} \frac{\Delta(2z)}{\Delta(z)}$$

given in § 6.3. Recall that a *hauptmodul* for $X_0(2)$ is a function $\tilde{x} \in \mathbb{C}(X_0(2))$ such that

1. $\mathbb{C}(X_0(2)) = \mathbb{C}(\tilde{x})$, and
2. $\tilde{x}(Y_0(2)) \subseteq \mathbb{C}$, i.e. any poles of $\tilde{x}$ are at the cusps of $X_0(2)$.

Note that any two hauptmoduls for $X_0(2)$ differ by a Möbius transformation. Indeed, if $\tilde{x}_1$ and $\tilde{x}_2$ are two hauptmoduls for $X_0(2)$, then $\tilde{x}_1 \circ \tilde{x}_2^{-1}$ is an automorphism of $\mathbb{P}^1(\mathbb{C})$, hence is a Möbius transformation.

Now, we have morphisms

$$\begin{array}{ccc} X(2) & \xrightarrow{\sim} & \mathbb{P}^1_\lambda \\ {\scriptstyle 2}\swarrow & & \downarrow{\scriptstyle 6} \\ X_0(2) & & \\ {\scriptstyle 3}\searrow & & \\ & X(1) \xrightarrow{\sim} & \mathbb{P}^1_j \end{array}$$

of the given degrees. Away from cusps, they are given functorially by

$$Y(2) \longrightarrow Y_0(2) \longrightarrow Y(1),$$

$$[E, P, Q] \longmapsto [E, P] \longmapsto [E]\,.$$

We have $\mathrm{Aut}\,(X(2)/X(1)) \cong S_3$, by letting $\sigma \in S_3$ act on $Y(2) \subseteq X(2)$ by permuting the 2-torsion points of an elliptic curve:

$$[E, P_1, P_2]^\sigma = \left[E, P_{\sigma(1)}, P_{\sigma(2)}\right], \quad P_3 = P_1 + P_2.$$

The map $X(2) \to X_0(2)$ is invariant under the action of $(23) \in S_3$. Thus it induces a morphism

$$X(2)/\langle (23) \rangle \to X_0(2),$$

which pulls back to a morphism

$$\mathbb{C}(X(2)/\langle (23) \rangle) = \mathbb{C}(X(2))^{\langle (23) \rangle} \to \mathbb{C}(X_0(2)),$$

where $\mathbb{C}(X(2))^{\langle (23) \rangle}$ is the subfield of $\mathbb{C}(X(2))$ fixed by $\langle (23) \rangle$. The action of S_3 on $\mathbb{P}^1_\lambda \cong X(2)$ is given in Table 2.1. In particular, we see that

$$\lambda^{(23)} = \frac{\lambda}{\lambda - 1},$$

so

$$\tilde{x} := 2^4 \cdot \lambda \cdot \lambda^{(23)} = 2^4 \frac{\lambda^2}{\lambda - 1}$$

is invariant under the action of $\langle (23) \rangle \subseteq S_3$.

Lemma 6.4.6. *The function $\tilde{x}$ is a hauptmodul for $X_0(2)$.*

Proof. First, since $\lambda \neq 0, 1, \infty$ on $Y(2)$, $\tilde{x}$ has no poles or zeroes on $Y_0(2)$.

To see that $\mathbb{C}(\tilde{x}) = \mathbb{C}(X_0(2))$, recall that the function $x(z) = 2^{12} \frac{\Delta(2z)}{\Delta(z)}$ is a hauptmodul for $X_0(2)$, so in particular $\mathbb{C}(X_0(2)) = \mathbb{C}(x)$. Also, x is a root of the irreducible polynomial $\psi_2(T, j) \in \mathbb{C}(X(1))[T]$. Note that for $z \in \mathcal{H}$,

$$j(z) = 2^8 \frac{(1 - \lambda(z) + \lambda(z)^2)^3}{\lambda(z)^2 (1 - \lambda(z))^2} = \frac{\left(2^4 + 2^4 \frac{\lambda(z)^2}{1 - \lambda(z)}\right)^3}{2^4 \frac{\lambda(z)^2}{1 - \lambda(z)}} = \frac{(\tilde{x}(z) + 16)^3}{\tilde{x}(z)},$$

so $\tilde{x}$ also satisfies $\psi_2(\tilde{x}, j) = (\tilde{x} + 16)^3 - j\tilde{x} = 0$. Hence $\mathbb{C}(\tilde{x}) = \mathbb{C}(x) = \mathbb{C}(X_0(2))$. $\square$

Cusp of $X(2)$	∞	0	1
Cusp of $X_0(2)$	∞	0	0
λ	0	1	∞
$\tilde{x} = 2^4 \frac{\lambda^2}{1-\lambda}$	0	∞	∞
$x = 2^{12} \frac{\Delta(2z)}{\Delta(z)}$	0	∞	∞

Table 6.1: Values of the hauptmoduls x and $\tilde{x}$ at the cusps of $X_0(2)$.

Since $\tilde{x}$ is a hauptmodul for $X_0(2)$, it is related to the hauptmodul

$$x(z) = 2^{12} \frac{\Delta(2z)}{\Delta(z)}$$

by a Möbius transformation. So

$$\tilde{x} = \frac{ax+b}{cx+d},$$

for some $a, b, c, d \in \mathbb{C}$. We calculate the values of $\tilde{x}$ and x at the cusps of $X_0(2)$. The modular curve $X(2)$ has cusps $[0], [1]$ and $[\infty]$, while $X_0(2)$ has cusps $[0]$ and $[\infty]$. On the cusps, the map $X(2) \to X_0(2)$ is given by

$$\begin{array}{ccc} [\infty] & [0] & [1] \\ \downarrow & \downarrow & \swarrow \\ [\infty] & [0]. & \end{array}$$

Recall that the q-expansion of λ is

$$\lambda(z) = 16q^{1/2} - 128q + 704q^{3/2} + O(q^2), q = e^{2\pi i z},$$

so $\lambda(\infty) = 0$. Looking the action of S_3 on $\mathbb{P}^1_\lambda$ in Table 2.2, we see that $\lambda(0) = 1$ and $\lambda(1) = 0$. Hence $\tilde{x}(\infty) = \infty$ and $\tilde{x}(0) = 0$. To evaluate x at the cusps, note that it has q-expansion

$$x(z) = 2^{12} q \prod_{n \geq 1} (1+q^n)^{24},$$

so $x(\infty) = 0$ and $x(0) = \infty$. These calculations are summarized in Table 6.1.

Now, since $\tilde{x} = \frac{ax+b}{cx+d}$ and $\tilde{x}(\infty) = x(\infty) = \infty$ and $\tilde{x}(0) = x(0) = 0$, we must have

$c = b = 0$, so $\tilde{x} = \frac{ax}{d}$ is a constant multiple of x. And, looking at q-expansions, we see

$$x(z) = 2^{12} q \prod_{n \geq 1} (1 + q^n)^{24} = 2^{12} q + O(q^2), \tag{6.4.7}$$

while

$$\tilde{x}(z) = 2^4 \frac{\lambda(z)^2}{1 - \lambda(z)} = 2^4 \frac{(16q^{1/2} - 128q + O(q^2))^2}{1 - 16q^{1/2} + 128q + O(q^2)} = 2^{12} q + O(q^{3/2}),$$

so we must have $\tilde{x} = x$.

Hence

$$x = 2^4 \frac{\lambda^2}{1 - \lambda}$$

as functions on $\Gamma(2) \backslash \mathcal{H}$, i.e. as modular forms over $\mathbb{C}$ of weight 0 and level $\Gamma(2)$. Moreover, we see from Equation (6.4.7) that the q-expansion of x, and hence of $2^4 \frac{\lambda^2}{1-\lambda}$, have integral coefficients. So, by the q-expansion principle (see [6, Proposition 1.8]), x and $2^4 \frac{\lambda^2}{1-\lambda}$ are both modular forms over $\mathbb{Z}[1/2]$ of weight 0 and level $\Gamma(2)$, hence elements of the function ring $\mathcal{O}\left(\mathcal{Y}(2)_{\mathbb{Z}[1/2]}\right)$, and are equal in this ring. So the pullback if the map $u_1 : \mathcal{Y}(2)_{\mathbb{Z}[1/2]} \to \mathcal{Y}_0(2)_{\mathbb{Z}[1/2]}$ is given by

$$u_1^* : \mathcal{O}\left(\mathcal{Y}_0(2)_{\mathbb{Z}[1/2]}\right) \to \mathcal{O}\left(\mathcal{Y}(2)_{\mathbb{Z}[1/2]}\right), \quad x \mapsto x_1(\lambda) := 2^4 \frac{\lambda^2}{1 - \lambda}. \tag{6.4.8}$$

Now, note that over $\mathbb{C}$, $u_2 = u_1 \circ \alpha$, where α is the automorphism of $Y(2)$ given by

$$\alpha : Y(2) \to Y(2), \quad [E, P_1, P_2] \mapsto [E, P_2, P_1].$$

So $u_2^* = \alpha^* \circ u_1^*$ over $\mathbb{C}$. Looking at Table 2.1, we see that α corresponds to the action of $(12) \in S_3$ on $Y(2)$. From the same table, we see that $\lambda^{(12)} = 1 - \lambda$, so the pullback map α^* is given by $\alpha^*(\lambda) = 1 - \lambda$, and so

$$u_2^*(x) = \alpha^* \circ u_1^*(x) = \alpha^* \left(2^4 \frac{\lambda^2}{1 - \lambda}\right) = 2^4 \frac{(1 - \lambda)^2}{\lambda} =: x_2(\lambda)$$

as functions on $\Gamma(2)\backslash\mathcal{H}$, i.e. as modular forms over $\mathbb{C}$ of weight 0 and level $\Gamma(2)$. On the other hand, Table 2.1 gives that $z^{(12)} = -\frac{1}{z}$ for $z \in \mathcal{H}$, so

$$\alpha^* \circ u_1^*(x) = x(-1/z)$$

as functions on $\Gamma(2)\backslash\mathcal{H}$. Using the fact that $\Delta(-1/z) = z^{12}\Delta(z)$ (see [12, Proposition 1.2.5]), we see that

$$x(-1/z) = \frac{2^{12}}{x(z/2)} = q^{-1/2}\prod_{n\geq 1}\frac{1}{(1+q^{1/2})^{24}} = q^{-1/2}\prod_{n\geq 1}\left(\sum_{m\geq 0}(-1)^m q^{m/2}\right)^{24}. \qquad (6.4.9)$$

So $x(-1/z)$, and hence $u_2^*(x)$ and $x_2(\lambda)$, have q-expansions around the cusp ∞ with integral coefficients, so by the q-expansion principle they are modular forms over $\mathbb{Z}[1/2]$ of weight 0 and level $\Gamma(2)$, i.e. elements of $\mathcal{O}\left(\mathcal{Y}(2)_{\mathbb{Z}[1/2]}\right)$. So the pullback map u_2^* is given over $\mathbb{Z}[1/2]$ by

$$u_2^* : \mathcal{O}\left(\mathcal{Y}_0(2)_{\mathbb{Z}[1/2]}\right) \to \mathcal{O}\left(\mathcal{Y}(2)_{\mathbb{Z}[1/2]}\right), \quad x \mapsto x_2(\lambda) = 2^4\frac{\lambda^2}{1-\lambda}. \qquad (6.4.10)$$

Finally, the pullbacks of the projection maps $\pi_i : \mathcal{Y} \to \mathcal{Y}_0(2)$ are given by

$$\mathcal{O}\left(\mathcal{Y}_0(2)_{\mathbb{Z}[1/2]}\right) = \mathbb{Z}[1/2, x, 1/x] \xrightarrow{\pi_1^*} \mathcal{O}\left(\mathcal{Y}_{\mathbb{Z}[1/2]}\right) = \mathbb{Z}[1/2, x, 1/x] \underset{\mathbb{Z}[1/2,j]}{\otimes} \mathbb{Z}[1/2, x, 1/x]$$

$$x \longmapsto x \otimes 1$$

and

$$\mathcal{O}\left(\mathcal{Y}_0(2)_{\mathbb{Z}[1/2]}\right) = \mathbb{Z}[1/2, x, 1/x] \xrightarrow{\pi_2^*} \mathcal{O}\left(\mathcal{Y}_{\mathbb{Z}[1/2]}\right) = \mathbb{Z}[1/2, x, 1/x] \underset{\mathbb{Z}[1/2,j]}{\otimes} \mathbb{Z}[1/2, x, 1/x]$$

$$x \longmapsto 1 \otimes x$$

Under the isomorphism $\mathcal{Y}_{\mathbb{Z}[1/2]} \cong \operatorname{Spec} \mathbb{Z}[1/2, x_1, x_2, 1/x_1x_2]/(x_1 - x_2)(G(x_1, x_2))$, these become

$$\pi_1^*(x) = x_1, \quad \pi_2^*(x) = x_2.$$

So, using the fact that u^* sits in the commutative diagram

$$\begin{array}{ccccc} & & \mathcal{O}(Y(2)_{\mathbb{Z}[1/2]}) & & \\ & \overset{u_1}{\nearrow} & \uparrow{\scriptstyle u} & \overset{u_2}{\nwarrow} & \\ \mathcal{O}\left(\mathcal{Y}_0(1)_{\mathbb{Z}[1/2]}\right) & \xrightarrow[\pi_1]{} & \mathcal{O}\left(\mathcal{Y}_{\mathbb{Z}[1/2]}\right) & \xleftarrow[\pi_2]{} & \mathcal{O}\left(\mathcal{Y}_0(1)_{\mathbb{Z}[1/2]}\right), \end{array}$$

and the expressions for u_1^* and u_2^* given in Equations (6.4.8) and (6.4.10), we see that u^* is given by

$$u^*(x_1) = x_1(\lambda) = 2^4\frac{\lambda^2}{1-\lambda}, \quad u^*(x_2) = x_2(\lambda) = 2^4\frac{(1-\lambda)^2}{\lambda},$$

as desired. □

Now, a calculation shows that $u^*G(x_1, x_2) = 0$, where G is the polynomial defined in Equation (6.4.4). Hence u factors through a morphism

$$v : \mathcal{Y}(2)_{\mathbb{Z}[1/2]} \to \mathcal{V} := \operatorname{Spec} \mathbb{Z}[1/2, x_1, x_2, 1/x_1x_2]/(G(x_1, x_2)).$$

Note that $\mathcal{V}$ is the subscheme of $\mathcal{Y}_{\mathbb{Z}[1/2]}$ cut out by the equation $G(x_1, x_2) = 0$. Moreover, one can check that the map v is a birational isomorphism, with the inverse of v^* given by

$$\lambda \mapsto \frac{x_1 + 16}{x_1 + x_2 + 32}$$

Hence v lifts to a morphism $\tilde{v} : \mathcal{Y}(2)_{\mathbb{Z}[1/2]} \to \widetilde{\mathcal{V}}$, where $\widetilde{\mathcal{V}}$ is the normalization of $\mathcal{V}$.

The next step in my construction is to give equations for the scheme $\widetilde{\mathcal{V}}$. However, calculating these equations does not require that 2 be invertible, so I will now move on to the next section, where I consider the map $u : \mathcal{Y}(2) \to \mathcal{Y}$ over $\mathbb{Z}$.

Remark 6.4.11. The scheme $\mathcal{Y}_{\mathbb{Z}[1/2]}$ decomposes as $\mathcal{Y}_{\mathbb{Z}[1/2]} = \mathcal{V} \cup \mathcal{D}$, where $\mathcal{D}$ is the "diagonal component" of $\mathcal{Y}_{\mathbb{Z}[1/2]}$, i.e. the subscheme cut out by the equation $x_1 - x_2 = 0$. On the level of moduli problems over $\mathbb{C}$, the subscheme $\mathcal{D}$ corresponds to the points

$([E,P],[E,Q]) \in Y$ such that $(E,P) \cong (E,Q)$ as enhanced elliptic curves for $\Gamma_1(2)$. It is comforting that u sends $\mathcal{Y}(2)_{\mathbb{Z}[1/2]}$ into the component $\mathcal{V}$ of this decomposition, since if (E,P,Q) is an enhanced elliptic curve (over $\mathbb{C}$) for $\Gamma(2)$, then $(E,P) \ncong (E,Q)$ as enhanced elliptic curves if $j(E) \notin \{0, 1728\}$.

6.5 A model for $Y(2)$ over $\mathbb{Z}$

Again, we consider the morphism of schemes

$$u : \mathcal{Y}(2) \to \mathcal{Y} := \mathcal{Y}_0(2) \underset{\mathcal{Y}_0(1)}{\times} \mathcal{Y}_0(2)$$

defined at the beginning of § 6.4. Recall that $\mathcal{Y}_0(2)$ is isomorphic to the scheme $\mathcal{G}_0(2) = \operatorname{Spec} \mathbb{Z}[x,j]/(\psi_2(x,j))$, where

$$\psi_2(x,j) := (x+16)^3 - xj$$

is the canonical modular polynomial for $\Gamma_0(2)$. So we can write $\mathcal{Y}$ as

$$\begin{aligned}
\mathcal{Y} &\cong \mathcal{G}_0(2) \underset{\operatorname{Spec} \mathbb{Z}[j]}{\times} \mathcal{G}_0(2) \\
&\cong \operatorname{Spec} \left(\mathbb{Z}[x,j]/(\psi_2(x,j) \underset{\mathbb{Z}[j]}{\otimes} \mathbb{Z}[x,j]/(\psi_2(x,j) \right) \\
&\cong \operatorname{Spec} \left(\mathbb{Z}[x_1,x_2,j]/(\psi_2(x_1,j), \psi_2(x_2,j)) \right).
\end{aligned}$$

In § 6.4, we studied the extension of scalars of u to $\mathbb{Z}[1/2]$, and calculated that the pullback of

$$u : \mathcal{Y}_0(2)_{\mathbb{Z}[1/2]} \to \mathcal{Y}_{\mathbb{Z}[1/2]} \cong \operatorname{Spec} \left(\mathbb{Z}[1/2, x_1, x_2, 1/x_1x_2] \right)$$

is given by

$$u^*(x_1) = x_1(\lambda) = 2^4 \frac{\lambda^2}{1-\lambda}, \quad u^*(x_2) = x_2(\lambda) = 2^4 \frac{(1-\lambda)^2}{\lambda}.$$

Also, note that we have a morphism of schemes $\mathcal{Y}_{\mathbb{Z}[1/2]} \to \mathcal{Y}$, whose pullback is the map

$$\mathbb{Z}[x_1, x_2, j]/(\psi_2(x_1, j), \psi_2(x_2, j)) \longrightarrow \mathbb{Z}[1/2, x_1, x_2, 1/x_1x_2]$$

$$x_i \longmapsto x_i$$

$$j \longmapsto \frac{(x_1+16)^3}{x_1} = \frac{(x_2+16)^3}{x_2}.$$

So the pullback of the morphism $u|_{\mathcal{Y}(2)_{\mathbb{Z}[1/2]}} : \mathcal{Y}(2)_{\mathbb{Z}[1/2]} \to \mathcal{Y}$ is given by

$$\mathcal{O}(\mathcal{Y}) \cong \mathbb{Z}[x_1, x_2, j]/(\psi_2(x_1, j), \psi_2(x_2, j)) \longrightarrow \mathcal{O}\left(Y(2)_{\mathbb{Z}[1/2]}\right) \cong \mathbb{Z}[1/2, \lambda, 1/\lambda(1-\lambda)]$$

$$x_1 \longmapsto x_1(\lambda) = 2^4\frac{\lambda^2}{1-\lambda}$$

$$x_2 \longmapsto x_2(\lambda) = 2^4\frac{(1-\lambda)^2}{\lambda}$$

$$j \longmapsto j(\lambda) = \frac{(x_1(\lambda)+16)^3}{x_1(\lambda)} = 256\frac{(1-\lambda+\lambda^2)^3}{\lambda^2(1-\lambda)^2}.$$

As in § 6.4, define

$$G(x_1, x_2) := x_1^2x_2 + x_1x_2^2 + 48x_1x_2 - 16^3.$$

A quick calculation shows that $\left(u|_{\mathcal{Y}(2)_{\mathbb{Z}[1/2]}}\right)^* G = 0$, so $u|_{\mathcal{Y}(2)_{\mathbb{Z}[1/2]}}$ factors through a morphism

$$v : \mathcal{Y}(2)_{\mathbb{Z}[1/2]} \to \mathcal{V} := \text{Spec } \left(\mathbb{Z}[x_1, x_2, j]/(\psi_2(x_1, j), \psi_2(x_2, j), G(x_1, x_2))\right). \tag{6.5.1}$$

One can check that this is a birational isomorphism, whose inverse is given by

$$\lambda \mapsto \frac{x_1+16}{x_1+x_2+32}.$$

So v lifts to a morphism

$$\tilde{v} : Y(2)_{\mathbb{Z}[1/2]} \to \widetilde{\mathcal{V}}$$

where $\widetilde{\mathcal{V}}$ is the normalization of $\mathcal{V}$. A calculation using the programming language SINGULAR [10] shows that

$$\widetilde{\mathcal{V}} \cong \operatorname{Spec} \mathbb{Z}[x_1, x_2, t]/(g_1, g_2, g_3),$$

where $g_1, g_2, g_3 \in \mathbb{Z}[x_1, x_2, t]$ are the polynomials

$$\begin{aligned} g_1(x_1, x_2, t) &:= x_1 x_2 - t(16 - t), \\ g_2(x_1, x_2, t) &:= x_1(16 - t) - t^2, \\ g_3(x_1, x_2, t) &:= x_2 t - (16 - t)^2. \end{aligned} \tag{6.5.2}$$

The function j is given on $\widetilde{\mathcal{V}}$ by

$$j = x_1^2 + x_1 x_2 + x_2^2 + 48x_1 + 48x_2 + 768, \tag{6.5.3}$$

and the pullback of $v : Y(2)_{\mathbb{Z}[1/2]} \to \widetilde{\mathcal{V}(2)}$ is given by

$$v^*(x_1) = \frac{16\lambda^2}{1-\lambda}, \quad v^*(x_2) = \frac{16(1-\lambda)^2}{\lambda}, \quad v^*(t) = 16\lambda. \tag{6.5.4}$$

In § 6.5.1, I will show that $\widetilde{\mathcal{V}}$ is in fact a coarse moduli space for the moduli problem $[\Gamma(2)]$, and hence $Y(2) \cong \widetilde{\mathcal{V}}$ over $\mathbb{Z}$.

Remark 6.5.5. From Equation (6.5.4), we see that the modular lambda function λ is given on $\widetilde{\mathcal{V}}$ by the rational function

$$\lambda = \frac{t}{16}.$$

In particular, this means that λ is *not* defined as a function on $\widetilde{\mathcal{V}}$ over $\mathbb{Z}$. Although this may seem surprising, it is consistent with our earlier observation that not all singular λ-values are algebraic integers. On the other hand, we saw in Lemma 5.3.3 that if λ is a singular lambda value[7] then 16λ *is* an algebraic integer, so it makes sense that 16λ does give a function on $\widetilde{\mathcal{V}}$.

[7] I.e. a value of the form $\lambda(\tau)$ with $\tau \in \mathcal{H}$ imaginary quadratic.

6.5.1 Our model is a coarse moduli space for $[\Gamma(2)]$

Theorem 6.5.6. *The coarse moduli scheme $\mathcal{Y}(2)$ is isomorphic to the scheme*

$$\mathcal{G}(2) := \operatorname{Spec} \mathbb{Z}[x_1, x_2, t]/(g_1, g_2, g_3),$$

where $g_1, g_2, g_3 \in \mathbb{Z}[x_1, x_2, t]$ are the polynomials

$$\begin{aligned} g_1(x_1, x_2, t) &:= x_1 x_2 - t(16 - t), \\ g_2(x_1, x_2, t) &:= x_1(16 - t) - t^2, \\ g_3(x_1, x_2, t) &:= x_2 t - (16 - t)^2. \end{aligned}$$

The morphism $\mathcal{G}(2) \cong \mathcal{Y}(2) \to \mathcal{Y}(1) \cong \operatorname{Spec} \mathbb{Z}[j]$ is given by

$$j = x_1^2 + x_1 x_2 + x_2^2 + 48x_1 + 48x_2 + 768.$$

Proof. First, consider the morphism $\pi : \mathcal{Y}(2) \to \mathcal{Y}(1) \cong \operatorname{Spec} \mathbb{Z}[j]$ defined by the functor of moduli problems $[\Gamma(2)] \to [\Gamma(1)]$ sending a $\Gamma(2)$-structure on an elliptic curve E/S to the unique $[\Gamma(1)]$-structure on E/S. The moduli problem $[\Gamma(2)]$ is finite, flat and regular (hence normal) by [20, First Main Theorem 5.1.1]. So $\mathcal{Y}(2)$ is normal by [20, Lemma 8.1.2], and π is finite by [20, Proposition 8.2.2]. The fact that π is finite means that it is affine, hence $\mathcal{Y}(2)$ is an affine scheme.

On the other hand, consider morphism $\pi_{\mathcal{G}} : \mathcal{G}(2) \to \operatorname{Spec} \mathbb{Z}[j]$ corresponding to the map

$$\mathbb{Z}[j] \to \mathbb{Z}[x_1, x_2, t]/(g_1, g_2, g_3), \quad j \mapsto x_1^2 + x_1 x_2 + x_2^2 + 48x_1 + 48x_2 + 768.$$

We saw earlier that $\mathcal{G}(2)$ is the normalization of the scheme

$$\mathcal{V}(2) = \operatorname{Spec} \mathbb{Z}[x_1, x_2, j]/(\psi_2(x_1, j), (x_2, j), G(x_1, x_2)),$$

so $\pi_{\mathcal{G}}$ factors as

$$\begin{array}{ccc} \mathcal{G}(2) & \xrightarrow{f} & \mathcal{V}(2) \\ & \searrow^{\pi_{\mathcal{G}}} & \downarrow{\scriptstyle \pi_{\mathcal{V}}} \\ & & \operatorname{Spec} \mathbb{Z}[j], \end{array}$$

where $\pi_{\mathcal{V}}$ is the projection morphism corresponding to the inclusion homomorphism $\mathbb{Z}[j] \to \mathbb{Z}[x_1, x_2, j]/(\psi_2(x_1, j), (x_2, j), G(x_1, x_2))$. Since $\mathcal{G}(2)$ is the normalization of $\mathcal{V}(2)$, the morphism f is finite. Also,

$$\mathbb{Z}[x_1, x_2, j]/(\psi_2(x_1, j), (x_2, j)) \cong \mathbb{Z}[x, j]/(\psi_1(x, j)) \underset{\mathbb{Z}[j]}{\otimes} \mathbb{Z}[x, j]/(\psi_1(x, j))$$

is the tensor product of two finitely generated $\mathbb{Z}[j]$-modules, hence is a finitely generated $\mathbb{Z}[j]$-module. So $\mathbb{Z}[x_1, x_2, j]/(\psi_2(x_1, j), (x_2, j), G(x_1, x_2))$ is a finitely generated $\mathbb{Z}[j]$-module as well, so the morphism $\pi_{\mathcal{V}}$ is finite. Therefore $\pi_{\mathcal{G}} = \pi_{\mathcal{V}} \circ f$ is finite. Moreover, $\mathcal{G}(2)$ is normal since it is the normalization of $\mathcal{V}(2)$.

Lemma 6.5.7. *There exist elements $x_1, x_2, t \in \mathcal{O}(\mathcal{Y}(2))$ satisfying*

$$g_1(x_1, x_2, t) = 0, \quad g_2(x_1, x_2, t) = 0, \quad g_3(x_1, x_2, t) = 0.$$

Proof. Consider the functions

$$x_1(z) := 2^{12} \frac{\Delta(2z)}{\Delta(z)}, \quad x_2(z) := \frac{\Delta(z/2)}{\Delta(z)} = \frac{2^{12}}{x(z/2)}, \quad t(z) := 16\lambda(z)$$

on $\mathcal{H}$. We saw in § 6.4 that

$$x_1(z) = \frac{16\lambda(z)^2}{1 - \lambda(z)}, \quad x_2(z) = \frac{16(1 - \lambda(z))^2}{\lambda(z)},$$

so a short calculation shows that

$$g_1(x_1(z), x_2(z), t(z)) = 0, \quad g_2(x_1(z), x_2(z), t(z)) = 0, \quad g_3(x_1(z), x_2(z), t(z0) = 0.$$

Now, the functions $x_1(z)$, $x_2(z)$ and $t(z)$ are all $\Gamma(2)$-invariant, so they are modular forms over $\mathbb{C}$ of weight 0 and level $\Gamma(2)$. Their q-expansions are (see Equations (2.3.8), (6.4.7) and (6.4.9))

$$\begin{aligned} x_1(z) &= 2^{12}q^2\prod_{n\geq 1}(1+q^{2n})^{24}, \\ x_2(z) &= q^{-1}\prod_{n\geq 1}\left(\sum_{m\geq 0}(-1)^m q^m\right), \\ t(z) &= 16^2 q\prod_{n\geq 1}\left(\frac{1+q^{2n}}{1+q^{2n-1}}\right)^8 = 16^2 q\prod_{n\geq 1}(1+q^{2n-1})^8\left(\sum_{m\geq 0}(-1)^m q^{(2n-1)m}\right)^8, \end{aligned} \tag{6.5.8}$$

where $q = e^{\pi i z}$. These have coefficients in $\mathbb{Z}[1/2]$ (in fact in $\mathbb{Z}$), so by the q-expansion principle (see [6, Proposition 1.8]), x_1, x_2 and t are modular forms over $\mathbb{Z}[1/2]$ of weight 0 and level $\Gamma(2)$, i.e. elements of $\mathcal{O}\left(\mathcal{Y}(2)_{\mathbb{Z}[1/2]}\right)$.

Finally, recall that x_1 satisfies the relation $\psi_2(x_1, j) = 0$ over $\mathbb{Z}[j]$. The function x_2 satisfies the same relation since $j(-1/z) = j(z)$. Also, we obtain from 2.1.7 that t satisfies the relation

$$(t^2 - 16t + 256)^3 - jt^2(16-t)^2 = 0.$$

Hence the elements $x_1, x_2, t \in \mathcal{O}\left(\mathcal{Y}(2)_{\mathbb{Z}[1/2]}\right)$ are integral over $\mathcal{O}(\mathcal{Y}(2))$. Since $\mathcal{Y}(2)$ is normal, $\mathcal{O}(\mathcal{Y}(2))$ is integrally closed, and so $x_1, x_2, t \in \mathcal{O}(\mathcal{Y}(2))$. □

Lemma 6.5.7 gives a $\mathbb{Z}[j]$-algebra homomorphism $\mathcal{O}(\mathcal{G}(2)) \to \mathcal{O}(\mathcal{Y}(2))$, sending the elements $x_1, x_2, t \in \mathcal{O}(\mathcal{G}(2))$ to the elements $x_1, x_2, t \in \mathcal{O}(\mathcal{Y}(2))$ (respectively) given in the lemma. Since $\mathcal{G}(2)$ and $\mathcal{Y}(2)$ are both affine, this gives us a morphism of $\mathcal{Y}(1)$-schemes

$$\begin{array}{ccc} \mathcal{Y}(2) & \xrightarrow{\quad f \quad} & \mathcal{G}_0(2). \\ & {\scriptstyle\pi}\searrow \quad \swarrow{\scriptstyle\pi_{\mathcal{G}}} & \\ & \mathcal{Y}(1) & \end{array}$$

Since π and $\pi_{\mathcal{G}}$ are both finite morphisms, so is f. Then, since $\mathcal{G}$ is normal, Zariski's Main Theorem [27, Lemma 37.38.1, Tag 03GW] gives us that $f(\mathcal{Y}(2))$ is an open subscheme of

$\mathcal{G}(2)$ and f is an isomorphism onto $f(\mathcal{Y}(2))$.

Now, since $\mathcal{G}$ is normal, it is integral, hence irreducible, so $f(\mathcal{Y}(2))$ is dense in $\mathcal{G}(2)$ and $f : \mathcal{Y}(2) \to \mathcal{G}(2)$ is a birational isomorphism. Since $\mathcal{Y}(2)$ and $\mathcal{G}(2)$ are both normal, this means that f is an isomorphism. □

6.6 Reduction modulo 2 and applications to elliptic curves

In this section, I will study the reduction modulo 2 of the model laid out for $\mathcal{Y}(2)$ in § 6.5. Recall (Theorem 6.5.6) that

$$\mathcal{Y}(2) \cong \text{Spec } \mathbb{Z}[x_1, x_2, t]/(g_1, g_2, g_3),$$

where

$$\begin{aligned} g_1(x_1, x_2, t) &= x_1x_2 - t(16 - t), \\ g_2(x_1, x_2, t) &= x_1(16 - t) - t^2, \\ g_3(x_1, x_2, t) &= x_2t - (16 - t)^2. \end{aligned}$$

Reducing modulo 2, we have

$$\begin{aligned} g_1(x_1, x_2, t) &\equiv x_1x_2 + t^2 \mod 2, \\ g_2(x_1, x_2, t) &\equiv (x_1 + t)t \mod 2, \\ g_3(x_1, x_2, t) &\equiv (x_2 + t)t \mod 2. \end{aligned} \tag{6.6.1}$$

The function j, as given in Theorem 6.5.6, reduces to

$$j = x_1^2 + x_1x_2 + x_2^2 \mod 2. \tag{6.6.2}$$

One can check that

$$(x_1x_2 + t^2, (x_1 + t)t, (x_2 + t)t) = (x_1, t) \cap (x_2, t) \cap (x_1 + t, x_2 + t)$$

as ideals in $\mathbb{F}_2[x_1, x_2, t]$. Hence if we write

$$\begin{aligned} L_1 &= \operatorname{Spec} \mathbb{F}_2[x_1, x_2, t]/(x_2, t) \\ L_2 &= \operatorname{Spec} \mathbb{F}_2[x_1, x_2, t/(x_1, t) \\ L_3 &= \operatorname{Spec} \mathbb{F}_2[x_1, x_2, t]/(x_1 + t, x_2 + t), \end{aligned} \tag{6.6.3}$$

then we find the following:

Corollary 6.6.4. *We have*

$$\mathcal{Y}(2)_{\mathbb{F}_2} = L_1 \cup L_2 \cup L_3,$$

where we identify each L_i with its image under the open immersion $L_i \to \mathcal{Y}(2)$ corresponding to the (natural) quotient homomorphism

$$\mathbb{F}_2[x_1, x_2, t]/(x_1, t)(x_2, t)(x_1 + t, x_2 + t) \to \mathcal{O}(L_i).$$

Now, let k be an algebraically closed field of characteristic 2. Since $\mathcal{Y}(2)$ is a coarse moduli space for $[\Gamma(2)]$, there is a bijection between points of $\mathcal{Y}(2)(k)$ and isomorphism classes of pairs (E, φ), where E is an elliptic curve over k and $\varphi : (\mathbb{Z}/2\mathbb{Z})^2 \to E[2](k)$ is a $\Gamma(2)$-structure on E/k (see [20, Lemma 8.1.3.1]). By Corollary 6.6.4, a point of $\mathcal{Y}(2)(k)$ is a pair (x_1, x_2, t) lying on one of the lines $x_1 = t = 0$, $x_2 = t = 0$, or $x_1 = x_2 = t$ in $\mathbb{A}^3_k$. If a point (x_1, x_2, t) corresponds to the elliptic curve (E, φ), then by Equation (6.6.2) the j-invariant of E is $j(E) = x_1^2 + x_1x_2 + x_2^2$. Let $\pi : \mathcal{Y}(2)(k) \to \mathcal{Y}(1)(k)$ be the usual projection map. Then

$$\pi^{-1}(j) = \begin{cases} \{(\sqrt{j}, 0, 0), (0, \sqrt{j}, 0), (\sqrt{j}, \sqrt{j}, \sqrt{j})\}, & \text{if } j \neq 0, \quad \text{and} \\ \{(0, 0, 0)\}, & \text{if } j = 0. \end{cases} \tag{6.6.5}$$

If $j \neq 0$, then $\#(\pi^{-1}(j) \cap L_i(k)) = 1$ for each of the lines L_1, L_2, L_3 from Equation (6.6.3). Therefore, we conclude that

Corollary 6.6.6. *The map*

$$\pi|_{L_i} : L_i(k) \subseteq \mathcal{Y}(2)(k) \to \mathcal{Y}(1)(k)$$

is an isomorphism for $i = 1, 2, 3$.

On the other hand, $j = 0$ is the unique supersingular j-invariant in characteristic 2, so if E is an elliptic curve over k, then

$$E[2](k) \cong \begin{cases} \mathbb{Z}/2\mathbb{Z}, & \text{if } j(E) \neq 0, \text{ and} \\ 0, & \text{if } j(E) = 0. \end{cases}$$

If $j(E) = 0$, then there is a unique $\Gamma(2)$-structure on E, corresponding to the unique group homomorphism

$$\varphi : (\mathbb{Z}/2\mathbb{Z})^2 \to E[2](k) = 0.$$

If $j(E) \neq 0$, then there are exactly three group homomorphisms

$$\varphi : (\mathbb{Z}/2\mathbb{Z})^2 \to E[2](k) \cong \mathbb{Z}/2\mathbb{Z}.$$

By Equation (6.6.5), each of these homomorphisms defines a $\Gamma(2)$-structure on E/k.

Example 6.6.7. Let W be a complete discrete valuation ring with uniformizer u, field of fractions F, and algebraically closed residue field $k = W/(u)$ of characteristic 2. Denote by ord_u the valuation on W, normalized so that $\mathrm{ord}_u(2) = 1$. Let E be an elliptic curve over W with good reduction modulo u. Write $E_0 := E \mod u$ and $j_0 = j(E_0) = j \mod u$. Suppose that E has a Weierstrass equation over F of the form[8]

$$E : y^2 = x(x-1)(x-\lambda). \tag{6.6.8}$$

[8]Note that E will always have such a Weierstrass equation over a finite extension of W.

Then there is a bijection between $\Gamma(2)$-structures on E/F (up to isomorphism), elements of $\pi^{-1}(j) \subseteq \mathcal{Y}(2)(F)$, and elements of the set

$$S_3 \cdot \lambda = \left\{ \lambda, \frac{1}{\lambda}, 1-\lambda, \frac{1}{1-\lambda}, \frac{\lambda-1}{\lambda}, \frac{\lambda}{\lambda-1} \right\},$$

given by sending $\lambda' \in S_3 \cdot \lambda$ to

1. the $\Gamma(2)$-structure $\varphi : (\mathbb{Z}/2\mathbb{Z})^2 \to E[2](F)$ defined by $\varphi(1,0) = (1,0)$ and $\varphi(0,1) = (0,0)$, or
2. the element $\left(\frac{16(\lambda')^2}{1-\lambda'}, \frac{16(1-\lambda')^2}{\lambda'}, 16\lambda' \right) \in \pi^{-1}(j)$.

Elements of $S_3 \cdot \lambda$ are the roots of the polynomial

$$(1 - X + X^2)^3 - jX^2(1-X)^2 = 0.$$

Since $\operatorname{ord}_u(j) \geq 0$, the same argument as in 5.3.3 shows that $-4 \leq \operatorname{ord}_u(\lambda') \leq 4$ for all $\lambda' \in S_3 \cdot \lambda$. Moreover, if $\operatorname{ord}_u(\lambda') < 0$ then $\operatorname{ord}_u(1-\lambda') = \operatorname{ord}_u(\lambda')$, so $\operatorname{ord}_u\left(\frac{16(\lambda')^2}{1-\lambda'}\right) \geq 0$ and $\operatorname{ord}_u\left(\frac{16(1-\lambda')^2}{\lambda'}\right) \geq 0$ for $\lambda' \in S_3 \cdot \lambda$. Hence

$$\frac{16(\lambda')^2}{1-\lambda'}, \frac{16(1-\lambda')^2}{\lambda'}, 16\lambda' \in W$$

for $\lambda' \in S_3 \cdot \lambda$, and so we can reduce elements of $\pi^{-1}(j)$ modulo u to get a map

$$\pi^{-1}(j) \to \pi^{-1}(j_0).$$

Looking at Equation (6.6.5), we see that

$$\{t \mod u : (x_1, x_2, t) \in \pi^{-1}(j)\} = \begin{cases} \{0, \sqrt{j_0}\}, & \text{if } j_0 \neq 0, \text{ and }, \\ \{0\}, & \text{if } j_0 = 0. \end{cases}$$

In particular, there is an element $(x_1, x_2, t) \in \pi^{-1}(j)$ such that $\operatorname{ord}_u(t) = 0$ if and only if $\operatorname{ord}_u(j) = 0$. Equivalently, there is an element $\lambda' \in S_3 \cdot \lambda$ such that $\operatorname{ord}_u(\lambda') = -4$ if and

only if $\operatorname{ord}_u(j) = 0$, i.e. if and only if $j \not\equiv 0 \mod u$.

In particular, if E is an elliptic curve with complex multiplication, this example gives the following result. Note that this result agrees with Corollary 5.3.6.

Corollary 6.6.9. *Let W be a complete discrete valuation ring with uniformizer u and algebraically closed residue field $k = W/(u)$ of characteristic 2. Let ord_u be the valuation of W, normalized so that $\operatorname{ord}_u(2) = 1$. Let E be an elliptic curve over W with complex multiplication by some order $\mathcal{O}$ in an imaginary quadratic field K. Let*

$$\Lambda = \{\lambda(E, \varphi) : \varphi \text{ a } \Gamma(2)\text{-structure on } E\}.$$

Then there exists $\lambda' \in \Lambda$ with $\operatorname{ord}_u(\lambda) = -4$ if and only if 2 is split in K.

Proof. The elliptic curve E has ordinary reduction modulo u if 2 is split in K, and supersingular reduction modulo u if 2 is inert or ramified in K. Moreover, $j_0 = 0$ is the only supersingular j-invariant in characteristic 2, so 2 is split in K if and only if $j \not\equiv 0 \mod u$. The corollary then follows from the above discussion. □

Chapter 7

Conclusion

In this thesis, I have studied singular values of the modular j function and the modular lambda function λ. I proved several results, some of which are analogues for singular lambda values of known results on singular moduli. These results give rise to a few natural questions.

For example, in chapter 4, I gave an upper bound for the valuation of a singular modulus. If j is a singular modulus of fundamental discriminant d, and v is a valuation of $\mathbb{Q}(j)$ dividing 2, normalized so that $v(2) = 1$, then I found (Theorem 4.1.3) that

$$v(j) \leq 6 \log_2 |d| + 6(\log_2 3 - 1). \tag{7.1}$$

To prove this, I used the fact that

$$N \leq v(j) \leq 12N, \tag{7.2}$$

where

$$N = \max\{n : E \cong E_0 \mod \pi^n\}.$$

Here π is a uniformizer in some complete discrete valuation ring W containing j, with algebraically closed residue field, and E and E_0 are elliptic curves over W with j-invariants j and 0, respectively.

From here, it is natural to ask whether there exist singular moduli of arbitrarily

large valuations. Namely, if we fix a valuation v on $\overline{\mathbb{Q}}$ dividing 2, normalized so that $v(j) = 1$, and an integer $n \geq 1$, does there exist a singular modulus with $v(j) \geq n$? By Equation (7.2), this is equivalent to the following question:

Question 7.3. Fix an integer $n \geq 1$ and a valuation v on $\overline{\mathbb{Q}}$. Let $i : \overline{\mathbb{Q}} \to \overline{\mathbb{Q}}_2$ be an embedding inducing the valuation v. Does there exist

1. a finite extension W of the Witt vectors $W\left(\overline{\mathbb{F}}_2\right)$, with uniformizer π and ramification index e,

2. an elliptic curve E_0 over W with j-invariant $j(E_0) = 0$, complex multiplication by $\mathbb{Z}\left[\frac{-1+\sqrt{-3}}{2}\right]$, and with good reduction modulo π, and

3. an elliptic curve E over W with complex multiplication by the ring of integers $\mathcal{O}_K$ of some imaginary quadratic field K, and with good reduction modulo π,

such that $E \cong E_0 \mod \pi^{en}$?

In chapter 5, I gave a Berwick-like congruence for the modular lambda function above the prime 2. If λ is a singular lambda value of discriminant $d < 0$, write $K = \mathbb{Q}(\sqrt{d})$, and let d_K be the discriminant of K and f the conductor of d. Then I showed (Corollary 5.3.6) that the set

$$\Lambda = \left\{\lambda, \frac{1}{\lambda}, 1-\lambda. \frac{1}{1-\lambda}, \frac{\lambda-1}{\lambda}. \frac{\lambda}{\lambda-1}\right\}$$

satisfies

$$\{v_{\mathfrak{p}}(\lambda') : \lambda' \in \Lambda\} = \begin{cases} \{0\}, & \text{if 2 is inert in } K \text{ and } s = 0, \\ \{0, 4 - 2^{2-\operatorname{ord}_2(f)}, 2^{2-\operatorname{ord}_2(f)} - 4\}, & \text{if 2 is inert in } K \text{ and } s \geq 1, \\ \{0, 4 - 3 \cdot 2^{-\operatorname{ord}_2(f)}, 3 \cdot 2^{-\operatorname{ord}_2(f)} - 4\}, & \text{if 2 is ramified in } K, \text{ and} \\ \{0, 4, -4\}, & \text{if 2 is split in } K, \end{cases} \tag{7.4}$$

for any prime $\mathfrak{p}$ of $K(\lambda)$ dividing 2. A similar formula for norms (over $\mathbb{Q}$) of singular lambda values was proven by Yang, Yin and Yu [31]. It would be interesting to compare my formula to their result.

To prove Equation (7.4), I applied the theory of Newton polygons to the polynomial

$$f_j(X) := (X^2 - X + 1)^3 - \frac{j}{256}X^2(1-X)^2$$

to relate $v_{\mathfrak{p}}(\lambda'), \lambda' \in \Lambda$ to $v_{\mathfrak{p}}(j)$, where j is the singular modulus lying above λ. This suggests a method which can be used to derive Berwick-like congruences for other hauptmoduls μ.

Finally, in chapter 6, I gave an integral model for the modular curve $\mathcal{Y}(2)$. The main idea of my construction was to embed $\mathcal{Y}(2)$ into the fiber product $\mathcal{Y}_0(2) \times_{\mathcal{Y}(1)} \mathcal{Y}_0(2)$, for which we have an integral model coming from the integral model for $\mathcal{Y}_0(2)$ given by the canonical modular polynomial $\psi_2(x, j) = 0$. The morphism $\mathcal{Y}(2) \to \mathcal{Y}_0(2) \times_{\mathcal{Y}_0(1)} \mathcal{Y}_0(2)$ corresponds to the map

$$Y(2) \to Y_0(2) \underset{Y_0(1)}{\times} Y_0(2), \quad [E, P, Q] \mapsto ([E, P], [E, Q])$$

of moduli problems over $\mathbb{C}$. Again, this could suggest a method to obtain an integral model for $\mathcal{Y}(n)$ for integers $n > 2$, by embedding $\mathcal{Y}(n)$ into the fiber product $\mathcal{Y}_0(n) \times_{\mathcal{Y}_0(1)} \mathcal{Y}_0(n)$. One would need to check that the canonical modular polynomial $\psi_n(x, j)$ gives an integral model for $\mathcal{Y}_0(n)$.

Appendix A

The quaternion algebra ramified at l and ∞

Fix a prime $p \leq \infty$. I will use the convention that ∞ is prime, with $\mathbb{Q}_\infty = \mathbb{R}$. Recall that if B is a quaternion algebra, then either

1. $B \otimes_{\mathbb{Q}} \mathbb{Q}_p$ is a division algebra, or

2. $B \otimes_{\mathbb{Q}} \mathbb{Q}_p \cong M_2(\mathbb{Q}_p)$ is the ring of 2×2 matrices over $\mathbb{Q}_p$.

In the first case, we say that B is *ramified* at p, otherwise B is *unramified* at p.

Proposition A.1. (Hilbert) *Any quaternion algebra over $\mathbb{Q}$ is ramified at an (finite) even number of primes, counting ∞.*

Proof. This follows from [29, Theorem 14.6.1]. □

Now, fix a prime $l > 2$. Then there is a unique quaternion algebra $B_{l,\infty}$ which is ramified at l and ∞ (and unramified at all other primes). I will show that $B_{l,\infty}$ has the following form:

Proposition A.2. *Let K be an imaginary quadratic field such that*

1. the discriminant $-p$ of K is prime, and

2. l is either inert or ramified in K.

Then

$$B_{l,\infty} \cong B := \left\{ [\alpha, \beta] := \begin{pmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{pmatrix} : \alpha, \beta \in K \right\} \subseteq M_2(K).$$

Proof. First, note that since $-p$ is a fundamental discriminant and p is prime, we must have $p \equiv 3 \mod 4$.

Fix a prime $q \neq 2, l, \infty$. I need to show that $B \otimes_{\mathbb{Q}} \mathbb{Q}_q$ is not a division algebra. Equivalently, I must show that there exists an element $b \in B \otimes_{\mathbb{Q}} \mathbb{Q}_q$ such that $\det(b) = 0$, since $b \in B \otimes_{\mathbb{Q}} \mathbb{Q}_q$ if and only if $\det(b) \neq 0$. I will consider separately the cases where q is split, inert and ramified in K.

Case 1: q is split in K. Then we can choose an embedding $K \hookrightarrow \mathbb{Q}_1$, which gives an isomorphism

$$K \otimes_{\mathbb{Q}} \mathbb{Q}_p \xrightarrow{\sim} \mathbb{Q}_q \oplus \mathbb{Q}_q, \quad \lambda \otimes t \mapsto (\lambda t, \overline{\lambda} t).$$

We can extend $\mathrm{Nm}_{K/\mathbb{Q}}$ to $K \otimes_{\mathbb{Q}} \mathbb{Q}_q$, by setting $\mathrm{Nm}(\lambda \otimes t) := t^2 \mathrm{Nm}_{K/\mathbb{Q}}(\lambda) = t^2 \lambda \overline{\lambda}$. On $\mathbb{Q}_q \oplus \mathbb{Q}_q \cong K \otimes_{\mathbb{Q}} \mathbb{Q}_q$, this is given by $\mathrm{Nm}(x, y) = xy$.

A general element of $K \otimes_{\mathbb{Q}} \mathbb{Q}_q$ is of the form $\alpha = 1 \otimes x + \sqrt{-p} \otimes y$, with $x, y \in \mathbb{Q}_p$. This corresponds to the element $(x + \sqrt{-p}y, x - \sqrt{-p}y) \in \mathbb{Q}_q \oplus \mathbb{Q}_q \mathrm{m}$ and has norm $\mathrm{Nm}(\alpha) = x^2 + py^2$. So we want to find a pair $x, y \in \mathbb{Q}_q$ such that $x^2 + py^2 = 0$, i.e. such that $(x/y)^2 = -p$. Since q is split in K, we have $\left(\frac{-p}{q}\right) = 1$. So, since $q \neq 2$, $-p$ is a square $\mod q$, so we can find an element $a_0 \in \mathbb{Z}/q\mathbb{Z}$ such that $-p \equiv a_0^2 \mod q$. By Hensel's lemma, a_0 lifts to an element $a \in \mathbb{Q}_q$ such that $-p = a^2$.

This shows that there exists an element $\alpha \in K \otimes_{\mathbb{Q}} \mathbb{Q}_q$ such that $\alpha\overline{\alpha} = 0$. Then

$$[\alpha, 0] = \begin{pmatrix} \alpha & 0 \\ 0 & \overline{\alpha} \end{pmatrix} \in B \otimes_{\mathbb{Q}} \mathbb{Q}_q$$

has determinant 0.

Case 2: q is inert in K. Then $L = K \otimes_{\mathbb{Q}} \mathbb{Q}_q$ is an unramified extension of $\mathbb{Q}_q$. The norm map $\mathrm{Nm}_{K/\mathbb{Q}} : K^\times \to \mathbb{Q}^\times$ extends to a norm $\mathrm{Nm} : L^\times \to \mathbb{Q}_q^\times = \mathbb{Z}_q^\times \times \langle q \rangle$ (every element of $\mathbb{Q}_q$ is of the form uq^n with $u \in \mathbb{Z}_q^\times$ and $n \in \mathbb{Z}$). By [19, Proposition 3.6], we

have $\mathrm{Nm}(L^\times) = \mathbb{Z}_q^\times \times \langle q^2 \rangle$. Then, since $-l \in \mathbb{Z}_q^\times \subseteq \mathbb{Z}_q^\times \times \langle q^2 \rangle$, it must be the norm of some $\alpha \in L$. Then the element

$$[\alpha, 1] = \begin{pmatrix} \alpha & 1 \\ -l & \overline{\alpha} \end{pmatrix} \in B \otimes_{\mathbb{Q}} \mathbb{Q}_q$$

has determinant 0.

Case 3: q is ramified in K. Since K has discriminant $-p$, we must have $q = p$. Then $p \neq l$, and l does not split in K, so $\left(\frac{-p}{l}\right) = -1$. Using quadratic reciprocity and the fact that $p \equiv 3 \mod 4$, we have

$$\begin{aligned}
\left(\frac{-l}{p}\right) &= \left(\frac{-1}{p}\right)\left(\frac{l}{p}\right) \\
&= \left(\frac{-1}{p}\right)\left(\frac{p}{l}\right)(-1)^{\frac{p-1}{2}\frac{l-1}{2}} \\
&= \left(\frac{-1}{p}\right)\left(\frac{-l}{p}\right)\left(\frac{-p}{l}\right)(-1)^{\frac{p-1}{2}\frac{l-1}{2}} \\
&= (-1)^{\frac{p-1}{2}}(-1)^{\frac{l-1}{2}}(-1)(-1)^{\frac{p-1}{2}\frac{l-1}{2}} \\
&= (-1)(-1)^{\frac{l-1}{2}}(-1)(-1)^{\frac{l-1}{2}} \\
&= 1.
\end{aligned}$$

So, since $p \neq 2$, $-l$ is a square mod p, i.e. there exists an element $a_0 \in \mathbb{Z}/p\mathbb{Z}$ such that $a_0^2 + l = 0$. By Hensel's lemma, we can lift a_0 to an element $\alpha \in \mathbb{Z}_p$ such that $\alpha^2 = -l$. Then $\det[\alpha, 1] = 0$.

This shows that if $q \neq 2, l, \infty$, then $B \otimes_{\mathbb{Q}} \mathbb{Q}_q$ is not a division ring, and so B is unramified at $\mathbb{Q}$.

Now, I need to show that B is ramified at l and ∞, i.e. that $B \otimes_{\mathbb{Q}} \mathbb{Q}_l$ and $B \otimes_{\mathbb{Q}} \mathbb{R}$ are division algebras. To do this, note that for any field extension F of $\mathbb{Q}$, we have

$$B \otimes_{\mathbb{Q}} F \cong \left\{ [\alpha, \beta] = \begin{pmatrix} \alpha & \beta \\ -l\overline{\beta} & \overline{\alpha} \end{pmatrix} : \alpha, \beta \in F \otimes_{\mathbb{Q}} K \right\},$$

with the notation $\overline{x \otimes y} = x \otimes \overline{y}$. An element $[\alpha, \beta] \in B \otimes_{\mathbb{Q}} F$ is invertible if and only if

$\det[\alpha, \beta] \neq 0$.

For $F = \mathbb{R}$, we have $F \otimes K = \mathbb{R}(\sqrt{-p}) = \mathbb{C}$, and $\overline{\alpha}, \alpha \in \mathbb{C}$, is just complex conjugation. If $[\alpha, \beta] \in B \otimes_{\mathbb{Q}} \mathbb{R}$, then

$$\det[\alpha, \beta] = \alpha\overline{\alpha} + l\beta\overline{\beta} = |\alpha|^2 + l|\beta|^2,$$

so $\det[\alpha, \beta] = 0$ if and only if $\alpha = \beta = 0$. This shows that $B \otimes_{\mathbb{Q}} \mathbb{R}$ is a division ring, so B is ramified at ∞.

Now, suppose that $F = \mathbb{Q}_l$, and assume that $l \neq 2$. I will handle the case $l = 2$ below. Let $[\alpha, \beta] \in B \otimes_{\mathbb{Q}} \mathbb{Q}_l$. I need to show that $[\alpha, \beta] = 0$. Suppose not. Since $K = \mathbb{Q} \oplus \mathbb{Q}\sqrt{-p}$ as a $\mathbb{Q}$-vector space, we can write $\alpha = a \otimes 1 + a' \otimes \sqrt{-p}$ and $\beta = b \otimes 1 + b' \otimes \sqrt{-p}$ with $a, a', b, b' \in \mathbb{Q}_l$. Then

$$\det[\alpha, \beta] = a^2 + p(a')^2 + lb^2 + lp(b')^2 \in \mathbb{Q}_l \subseteq \mathbb{Q}_l \otimes_{\mathbb{Q}} K.$$

By clearing denominators, we can assume that $a, a', b, b' \in \mathbb{Z}_l$ and that at least one of a, a', b, b' is not divisible by l. Reducing modulo l gives $a^2 + p(a')^2 = 0 \mod l$. We have two cases:

Case 1: $a' \not\equiv 0 \mod l$. Then $-p = (a/a')^2 \mod l$ is a square mod l, so $\left(\frac{-p}{l}\right) = 1$. But l does not split in K, so $\left(\frac{-p}{l}\right) \neq 1$, which gives a contradiction.

Case 2: $a' \equiv 0 \mod l$. Then $a \equiv 0 \mod l$ as well, and so l^2 divides $a^2 + p(a')^2$. Hence l divides $b^2 + p(b')^2$. Repeating the same argument with b and b' shows that l divides both b and b'. This a contradiction, since we assumed that at least one of a, a', b, b' is not divisible by l.

This shows that, when $l \neq 2$, there is no $[\alpha, \beta] \in B \otimes_{\mathbb{Q}} \mathbb{Q}_l$ with $\det[\alpha, \beta] = 0$, and so $B \otimes_{\mathbb{Q}} \mathbb{Q}_l$ is not a division ring. Hence l is ramified in B when $l \neq 2$.

To finish the proof, note that Proposition A.1 implies that B is ramified at 2 if $l = 2$ and unramified at 2 otherwise. $\square$

Bibliography

[1] William E.H. Berwick. Modular invariants expressible in terms of quadratic and cubic irrationalities. *Proceedings of the London Mathematical Society*, s2-28:53–69, 1928.

[2] Stefan Bettner. *Beweis der Kongruenzen von Berwick sowie deren Verallgemeinerung und weitere Anwendungen von Torsionspunkten au elliptischen Kurven.* PhD thesis, Augsburg University, 2004.

[3] Yuri Bilu, Philipp Habegger, and Lars Kühne. No Singular Modulus Is a Unit. *International Mathematics Research Notices*, 2018.

[4] Enrico Bombieri and Walter Gubler. *Heights in Diophantine Geometry*, volume 4 of *New Mathematical Monographs.* Cambridge University Press, Cambridge, 2006.

[5] Jonathan M. Borwein and Peter B. Borwein. *Pi and the AGM: A Study in Analytic Number Theory and Computational Complexity.* Wiley, 1987.

[6] Ching-Li Chai and Gerd Faltings. *Degeneration of Abelian Varieties*, volume 22 of *A Series of Modern Surveys in Mathematics. 3. Folge / A Series of Modern Surveys in Mathematics.* Springer-Verlag, 1990.

[7] Komaravolu Chandrasekharan. *Elliptic Functions*, volume 281 of *Grundlehren der mathematischen Wissenschaften.* Springer-Verlag, 1985.

[8] Brian Conrad. Gross-Zagier revisited. In Henri Darmon and Shou-Wu Zhang, editors, *Heegner Points and Rankin L-Series*, volume 49 of *MSRI Publications*, pages 67–163. Cambridge University Press, 2004.

[9] David A. Cox. *Primes of the Form $x^2 + ny^2$*. Wiley, 2nd edition, 2013.

[10] Wolfram Decker, Gert-Martin Greuel, Gerhard Pfister, and Hans Schönemann. SINGULAR 4-1-3 — A computer algebra system for polynomial computations. `http://www.singular.uni-kl.de`, 2020.

[11] Pierre Deligne. Courbes elliptiques: formulaires. In Bryan J. Birch and Willem Kuyk, editors, *Modular Functions of One Variable IV*, Lecture Notes in Mathematics, pages 53–73. Springer-Verlag, 1972.

[12] Fred Diamond and Jerry Shurman. *A First Course in Modular Forms*, volume 228 of *Graduate Texts in Mathematics*. Springer, 2005.

[13] David Dorman. *Prime factorization of singular moduli*. PhD thesis, Harvard University, 1984.

[14] Eyal Z. Goren and Kristin E. Lauter. Class invariants for quartic cm fields. *Annales de l'Institut Fourier*, 57(2):457–480, 2007.

[15] Benedict H. Gross. On canonical and quasi-canonical liftings. *Inventiones mathematicae*, 84:321–326, 1986.

[16] Benedict H. Gross and M.J. Hopkins. Equivariant vector bundles on the Lubin-Tate moduli space. *Contemporary Mathematics*, 158:23–88, 1994.

[17] B.H. Gross and Don B. Zagier. On singular moduli. *Journal für die reine und angewandte Mathematik*, 355:191–220, 1984.

[18] OEIS Foundation Inc. The On-Line Encyclopedia of Integer Sequences. `https://oeis.org/A115977`, 2020.

[19] Kenkichi Iwasawa. *Local Class Field Theory*. Oxford University Press, 1986.

[20] Nicholas M. Katz and Barry Mazur. *Arithmetic moduli of elliptic curves*, volume 108 of *Annals of mathematics studies*. Princeton University Press, 1985.

[21] Neal Koblitz. *p-adic Numbers, p-adic Analysis, and Zeta-Functions*, volume 58 of *Graduate Texts in Mathematics*. Springer, 2nd edition, 1984.

[22] John H. Littlewood. On the class-number of the corpus $P(\sqrt{-k})$. *Proceedings of the London Mathematical Society*, s2-27:358–372, 1928.

[23] Jean-François Mestre. La méthode des graphes. Exemples et application. In Yoshihiko Yamamoto and Hideo Yokoi, editors, *Proceedings of the International Conference on Class Numbers and Fundamental Units of Algebraic Number Fields: June 24-28, 1986, Katata, Japan*, pages 217–242. Taniguchi Foundation, 1986.

[24] Reinhard Schertz. *Complex Multiplication*. Cambridge University Press, 2010.

[25] Jean-Pierre Serre and John Tate. Good reduction of abelian varieties. *Annals of Mathematics*, 88(3):492–517, 1968.

[26] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, 2nd edition, 2009.

[27] The Stacks Project Authors. *Stacks Project*. `https://stacks.math.columbia.edu`, 2020.

[28] Marie-France Vignéras. *Arithmétique des algèbres de quaternions*, volume 800 of *Lecture Notes in Mathematics*. Springer-Verlag, 1980.

[29] John Voight. *Quaternion algebras*. 2020. Preprint, v0.9.21.

[30] Tonghai Yang and Hongbo Yin. Difference of modular functions and their CM value factorization. *Transactions of the American Mathematical Society*, 371(5):3451–3482, 2019.

[31] Tonghai Yang, Hongbo Yin, and Peng Yu. The lambda invariants at CM points. *International Mathematics Research Notices*, 2019.