Equations For Modular Curves

by

Steven D. Galbraith

Thesis submitted for the Degree of
Doctor of Philosophy
to the University of Oxford

Michaelmas Term 1996

St. Cross College
Mathematical Institute

Abstract

The primary topic of this thesis is the construction of explicit projective equations for the modular curves $X_0(N)$. The techniques may also be used to obtain equations for $X_0^+(p)$ and, more generally, $X_0(N)/W_n$. The thesis contains a number of tables of results. In particular, equations are given for all curves $X_0(N)$ having genus $2 \leq g \leq 5$. Equations are also given for all $X_0^+(p)$ having genus 2 or 3, and for the genus 4 and 5 curves $X_0^+(p)$ when $p \leq 251$. The most successful tool used to obtain these equations is the canonical embedding, combined with the fact that the differentials on a modular curve correspond to the weight 2 cusp forms. A second method, designed specifically for hyperelliptic curves, is given. A method for obtaining equations using weight 1 theta series is also described.

Heights of modular curves are studied and a discussion is given of the size of coefficients occurring in equations for $X_0(N)$.

Finally, the explicit equations are used to study the rational points on $X_0^+(p)$. Exceptional rational points on $X_0^+(p)$ are exhibited for $p = 73, 103, 137$ and 191.

Acknowledgements

I would like to thank Professor Bryan Birch for his supervision over the duration of this research and for sharing with me some of his insight into the world of arithmetic geometry.

It is a pleasure to thank Imin Chen, Carlo Gasbarri, Frazer Jarvis, Andrew Robertson, Richard Taylor, Peter Bending and John Wilson for informative discussions relating to the content of this thesis and also for their help with proofreading.

I would also like to thank the numerous friends and colleagues who, over the years, have inspired, encouraged and guided me. There are far too many of these people for me to name.

I would like to thank my family for their continual support and encouragement, and for allowing me the freedom to pursue my own interests.

Finally, I would like to thank the Commonwealth Scholarships Commission and the Association of Commonwealth Universities, for footing the bill.

“Which of us is to do the hard and dirty work for the rest – and for what pay?”
John Ruskin (1819–1900)

“Better far off to leave half the ruins and nine-tenths of the churches unseen and to see well the rest; to see them not once, but again and often again; to watch them, to learn from them, to live with them, to love them, till they have become a part of life and life’s recollections.”
Augustus Hare (1792–1834)

Contents

Chapter 1

Introduction

The star of this thesis is the modular curve $X_0(N)$ and we will examine its life from several different angles.

The modular curve $X_0(N)$ is very important as it is one of the objects which links the world of elliptic curves with the world of modular forms. Indeed, one of the many equivalent formulations of the famous Shimura-Taniyama-Weil conjecture is that, for every elliptic curve E defined over $\mathbb{Q}$, there is some integer N and some surjective morphism of curves $\phi : X_0(N) \to E$.

There are also practical applications for equations of $X_0(N)$. Notable among these is an algorithm for counting the number of points on an elliptic curve E over a finite field $\mathbb{F}_q$. This algorithm was proposed by Schoof and uses the relation $\#E(\mathbb{F}_q) = q+1-c$, where the Frobenius map $\phi : x \mapsto x^q$ has characteristic polynomial $\phi^2 - c\phi + q = 0$ in $\mathrm{End}(E)$. For various small primes l the trace c of the Frobenius map is computed modulo l. The Chinese Remainder Theorem is then used to obtain the value of $c \in \mathbb{Z}$, and hence the number of points on the curve over the large field $\mathbb{F}_q$. In Schoof's original formulation, the trace of the Frobenius map was calculated by working with the l-division polynomial on E (whose roots are the $(l^2-1)/2$ values of x such that (x, y) has order l in $E\left(\overline{\mathbb{F}}_q\right)$). An idea of Elkies was to work with an equation of $X_0(l)$ and thus find a cyclic l-element subgroup C of E, which is fixed by Frobenius (when such a subgroup exists). The trace of Frobenius may then be calculated by considering its action on just this l-element subgroup C. The use of $X_0(l)$ in this situation gives a very large improvement in the effectiveness of the algorithm. There are further methods, due to Atkin, for using $X_0(l)$ to get information on the trace of Frobenius. It is therefore necessary to have suitable equations for $X_0(l)$.

The primary topic of this thesis is the study of methods for obtaining projective models for $X_0(N)$ which are defined over $\mathbb{Q}$. There is a well-known canonical equation for $X_0(N)$ which is given by the following. Let $j(\tau)$ be the classical modular j-function. There is a symmetric polynomial $\Phi(x, y) \in \mathbb{Z}[x, y]$, of degree $N+1$ in each variable, such that $\Phi(j(\tau), j(N\tau)) = 0$. One may use $\Phi(x, y)$ as an affine model for $X_0(N)$ over $\mathbb{Q}$. This has many theoretical uses but it has practical drawbacks. The main drawbacks are that its degree is very large (so it is highly singular) and that its coefficients are enormous.

It has been noted by Atkin, Elkies and others that modular curves seem to have models with surprisingly small coefficients. One of the aims of this thesis is to try to understand the meaning of the phrase "small coefficients". Therefore we seek methods which will yield suitably nice equations for $X_0(N)$. It is hoped that the coefficient size arising in such equations may be estimated.

The first method for obtaining equations studied is the canonical embedding. The canonical embedding is suitable for practical computation because the differentials on the curve correspond to the weight 2 cusp forms for $\Gamma_0(N)$. The weight 2 cusp forms are well understood and have fallen to the scythe of computational number theory to such an extent that there are very complete and explicit tables describing them.

In Chapter 3 we give an algorithm for computing equations for the image of the canonical embedding of certain modular curves $X_0(N)$ and we provide a large table of models for these curves. The models listed are seen to have small coefficients. Our evidence suggests that there is usually a model for $X_0(N)$ with coefficients of size $O(log(N))$. Furthermore, it seems there is always an equation for $X_0^+(p)$ which has coefficients of size $\leq log(p)$ (i.e., $O(log(p))$ with constant equal to 1).

The canonical embedding is not applicable for hyperelliptic curves. In Chapter 4 we give a method, which is similar in flavour to the methods of Chapter 3, which deals with the case of hyperelliptic curves. Once again we produce a large table (predominantly for curves of genus 2) which contains nice models for many modular curves.

The canonical embedding has a very solid theoretical grounding because it is a purely geometric technique based on the holomorphic differentials on the curve. For the methods of Chapter 3 we choose a basis $\{f_1, \dots, f_g\}$ for the weight 2 cusp forms on $\Gamma_0(N)$. The canonical map is translated into

$$\tau \longmapsto [f_1(\tau) : \cdots : f_g(\tau)] \tag{1.1}$$

which is now purely in the language of modular forms. The fact that this is a well-defined map from $X_0(N)$ to $\mathbb{P}^{g-1}(\mathbb{C})$ is immediate from the modularity of the forms $f_j(\tau)$. One observes that, for any collection of modular forms on $\Gamma_0(N)$ having weight k, it is possible to construct a rational map having the same form as (1.1). This idea gives a large number of possibilities for methods of obtaining projective models of $X_0(N)$.

As our goal is to understand why $X_0(N)$ has a model with small coefficients, it seems potentially fruitful to consider a map of the form (1.1) where the modular forms themselves have very small coefficients. We are led to consider the case of theta series associated to integral binary quadratic forms, as these are known to have sparse coefficients. Indeed, the nth coefficient of the q-expansion of a theta series associated to a quadratic form $Q(x, y)$ is precisely the number of pairs $(x, y) \in \mathbb{Z}^2$ such that $Q(x, y) = n$. Therefore the coefficients grow slowly and many of them are zero. In Chapter 5 a study is made of the weight 1 theta series coming from such quadratic forms. We call the projective map inspired by (1.1) the "hemi-canonical map". For the analysis of this map it is necessary to introduce a slight generalisation of the usual theta series. We prove a basic transformation formula for this generalised theta series.

The hemi-canonical map does, in certain cases, give a good projective model defined over $\mathbb{Q}$ with reasonably small coefficients. Unfortunately though, the coefficients are not as remarkably small as those found using the canonical embedding. Also there are several further drawbacks with this method. One problem is that the hemi-canonical map is never injective. Indeed, in many cases, the map factors through $X_0(N)/W_N$. Another problem is that the image of the hemi-canonical map of the curve $X_0(N)$ will sit in a projective space of dimension related to the class number of the quadratic field $\mathbb{Q}\left(\sqrt{-N}\right)$. When the image lies in $\mathbb{P}^3$ or $\mathbb{P}^4$ it is difficult to control the degree of the equations arising. When the class number is large it is difficult to predict the number of equations arising (whose intersection will be the model for the curve). The reason for this lack of control is that, in contrast to the case of the canonical embedding, we lack a firm link between the space of theta series under consideration and a concrete geometric object.

For the application of counting points on elliptic curves E over $\mathbb{F}_q$, there are other methods for obtaining equations for $X_0(l)$. The basic idea is to choose a suitable modular function $f(\tau)$ (which is found from considering ratios of modular forms) and then to compute a relation between $j(\tau)$ and $f(\tau)$. There are at least two reasons for involving $j(\tau)$ in this process. The first reason is that it is important to be able to pick out the elliptic curve E in question on the projective model. For instance, if one has $\Phi(j(\tau), f(\tau))$ describing the curve $X_0(l)$, then the l-element subgroups of E correspond to the roots x of $\Phi(j(E), x)$. The splitting of this polynomial $\Phi(j(E), x)$ in $\mathbb{F}_q[x]$ is precisely what is used to obtain information about the trace of Frobenius. The second reason for introducing $j(\tau)$ is that it is easy enough to find one special function $f(\tau)$ on $X_0(l)$ but, given f, it is difficult to find another function g such that $\mathbb{C}(f, g)$ is the function field of $X_0(l)$. The price paid for using the function $j(\tau)$ is that the coefficients become large, though when we are working over a finite field this is less of a drawback. In practice, an equation for $X_0(l)$ is computed over $\mathbb{Q}$ and this model is reduced modulo p (where p is the characteristic of $\mathbb{F}_q$) when required. Large amounts of time and space are required for the precomputation of the $X_0(l)$.

The models we obtain in Chapters 3 and 4 are probably not useful, at present, for the application of counting points on elliptic curves over $\mathbb{F}_q$. This is primarily due to the fact that there is no obvious way to use these models to find a polynomial analogous to the $\Phi(j(E), x)$ mentioned above. The methods discussed in this thesis, for calculating equations of modular curves $X_0(N)$, are tailor-made for finding models with very small coefficients and they are less applicable when N increases. On the other hand, models with small coefficients may be useful in the application as they would require less storage space (this does become an issue in practice), potentially less computation time, and would be easily reduced modulo p.

The study of coefficient size of projective models for $X_0(N)$ leads one naturally towards the theory of heights. In Chapter 6, which is very speculative, we discuss a few aspects of this theory. There are two related definitions of the height of a projective variety C. One of these was introduced by Faltings and it requires some quite abstract objects from algebraic geometry. The other definition is more concrete and we discuss it in some detail. These two notions are explicitly related and both of them depend on the actual choice of the embedding of C in projective space. It would be very nice to have a relationship between these heights and a more intrinsic height (such as the height of the Jacobian of C). In the elliptic curve case, we study the height of E, as a projective variety, and show why it seems very difficult to relate this height to the height of E, when E is considered as an abelian variety. We also discuss the relationship between $h(X)$ and $h(Y)$ when X and Y are projective curves related by some morphism $f : X \to Y$. We are interested in this situation because the modular parameterisation $X_0(N) \to E$ is very important. We discuss the height conjecture for modular elliptic curves. Chapter 6 contains several examples and observations that are more explicit than appear elsewhere. It is hoped that the contents of this chapter will provide some concrete examples in what is otherwise a very high-brow and abstract theory.

In Chapter 7, we undertake a study of the rational points on the curves $X_0^+(p)$. There has been interest in this problem since the work of Mazur [24] on rational points of $X_0(N)$ and $X_1(N)$. It has generally been believed that, when the genus is at least 2, most points on $X_0^+(p)$ (or, more generally, $X_0(N)/W_N$) come from either cusps or complex multiplication points. As with $X_0(N)$ we expect, in a few rare cases, exceptional rational points. In Chapter 7 we have been able to exhibit the cusps and complex multiplication points explicitly on many curves $X_0^+(p)$. We have then, occasionally, been able to exhibit exceptional rational points on these curves. To the author's knowledge, these are the first known examples of exceptional rational points on modular curves $X_0^+(p)$ of genus at least 2. It is hoped that the data obtained (suggesting that such points are rare, and also showing that they do exist) may be of use in classifying such points.

We attempt to use standard notation wherever possible. Note that the references given in this thesis tend to be practical rather than historical. By this we mean that references are given to places in the literature where a clear explanation of the idea may be found, rather than the original description. We apologise if it seems we have not given credit where it is due.

Chapter 2

Background

This chapter contains a review of some of the main ideas and tools used in this thesis. There is nothing original in this chapter, although the presentation has been tailored to our needs.

2.1 Modular Curves

The classical modular curves are defined to be quotients of the upper half plane $\mathcal{H} = \{\tau = x + iy \in \mathbb{C} \mid y > 0\}$ by the action of certain subgroups of finite index in $\mathrm{SL}_2(\mathbb{Z})$. This thesis is concerned with the congruence subgroups

$$\Gamma_0(N) = \left\{ \gamma = \left(\begin{array}{cc} a & b \\ c & d \end{array} \right) \in \mathrm{SL}_2(\mathbb{Z}) \middle| c \equiv 0 (\mathrm{mod}\ N) \right\}.$$

In this thesis, subgroups of $\mathrm{SL}_2(\mathbb{Z})$ will usually be viewed as linear fractional transformations, thus both I and $-I$ will act as the identity. A more pedantic approach would be to work with $\mathrm{PSL}_2(\mathbb{Z})$ but the difference is cosmetic.

We write $Y_0(N) = \Gamma_0(N)\backslash\mathcal{H}$. This turns out to be a non-compact Riemann surface. Therefore we consider the "completed" upper half plane $\mathcal{H}^* = \mathcal{H} \cup \mathbb{Q} \cup \{\infty\}$ and define the **modular curve** $X_0(N) = \Gamma_0(N)\backslash\mathcal{H}^*$. The points $\mathbb{Q}$ and ∞ are called the **cusps**. The cusps fall naturally into $\Gamma_0(N)$-equivalence classes. We now give a few comments to explain the name "modular curve".

The set $Y_0(N)$ arises naturally as the moduli space of pairs (E, C), where E is an elliptic curve over $\mathbb{C}$ and C is a cyclic N-element subgroup of E. Indeed, since we are working over $\mathbb{C}$, we may make this totally explicit. Suppose $\tau \in \mathcal{H}$ corresponds to a point of $Y_0(N)$ and write $E_\tau = \mathbb{C}/\langle 1, \tau\rangle$ and $C_\tau = \langle 1/N, \tau\rangle$ (here $\langle a, b\rangle$ represents the $\mathbb{Z}$-module generated by a and b). Clearly, the image of C_τ in E_τ is a cyclic subgroup of order N. Also $j(E_\tau) = j(\tau)$ (where the first j is the j-invariant of the elliptic curve and the second j is the classical modular j-function) and the point $\tau \in Y_0(N)$ corresponds to the pair (E_τ, C_τ). Every such pair (E, C) corresponds to a $\Gamma_0(N)$-orbit of some $\tau \in \mathcal{H}$. This notion may be extended to $X_0(N)$ by interpreting the cusps as generalised elliptic curves (see Diamond and Im [10] §9 for a sketch of the details). Thus we have justified the use of the word "modular".

We will now show that $X_0(N)$ has the structure of a Riemann surface. It is obvious that all the points $\tau \in \mathcal{H}$ have sufficiently small neighbourhoods which look like open subsets of $\mathbb{C}$. Such neighbourhoods will be preserved under the passage from $\mathcal{H} \to \Gamma_0(N)\backslash\mathcal{H}$. We write $\lambda : z \mapsto (z - \tau)/(z - \overline{\tau})$, so λ maps a small neighbourhood of τ to an open disc around 0 in $\mathbb{C}$ (clearly $\lambda(\tau) = 0$). In all but a finite number of points $\tau \in \mathcal{H}$, this identification of neighbourhoods gives a local coordinate at τ. If the stabilizer, in $\Gamma_0(N)$, of the point τ is not just $\{\pm I\}$ then we call the point an **elliptic point** of the group $\Gamma_0(N)$. If the stabilizer is a group of n elements (here we mean n elements as a subgroup of $\mathrm{PSL}_2(\mathbb{Z})$) then take λ^n to be the local coordinate at τ. This gives a well defined Riemann surface structure on $Y_0(N)$.

It remains to give local coordinates at the cusps. Define a base for the open sets at ∞ to be

$$U_\epsilon(\infty) = \{x + iy \in \mathcal{H} \mid y > 1/\epsilon\} \cup \{\infty\}$$

for each $\epsilon > 0$. A choice of local coordinate function at ∞ is the map $q : \tau \mapsto \exp(2\pi i\tau)$, which maps $U_\epsilon(\infty)$ to a disc in $\mathbb{C}$, of radius $\exp(-2\pi/\epsilon)$, which is centered at zero. The action of $\mathrm{SL}_2(\mathbb{Z})$ gives corresponding open sets at each of the rational cusps (one needs to take the width into account, see Section 2.3). This choice of topology now gives $X_0(N)$ the structure of a compact Riemann surface. It is possible to choose a connected fundamental domain for the action of $\Gamma_0(N)$, and so the Riemann surface is connected. From a well-known theorem (see the discussions in [41] or Appendix B of [20]) it then follows that $X_0(N)$ may be interpreted as a non-singular irreducible quasi-projective algebraic curve.

Note that, when $X_0(N)$ has genus 2, there isn't a non-singular model in $\mathbb{P}^2$ (though there is an elegant general model in $\mathbb{P}^4$, which is described in Cassels and Flynn [5]). We will generally use a plane model which represents the image of a projection $X_0(N) \longrightarrow \mathbb{P}^2(\mathbb{C})$. It is possible to choose the image curve in $\mathbb{P}^2$ so that it has a single singularity at infinity. We will also use this convention for hyperelliptic curves of higher genus.

It turns out that the algebraic curve $X_0(N)$ may be defined over $\mathbb{Q}$. We refer to Shimura [33] Chapter 6 for the details.

In this thesis we will utilise both aspects of the geometry of $X_0(N)$. The complex analytic (Riemann surface) theory gives links to the theory of modular forms, while the fact that $X_0(N)$ is an algebraic curve is implicit in our quest for good projective models.

2.2 Involutions

We introduce the Atkin-Lehner involutions (see [1]). In this section we will write these as matrices in $\mathrm{SL}_2(\mathbb{R})$, though in the applications we usually write them as elements of $\mathrm{GL}_2^+(\mathbb{Z})$ and therefore the normalisation is implicit.

For each prime $l|N$, let α be such that $l^\alpha \| N$, and choose $a, b, c, d \in \mathbb{Z}$ such that $l^\alpha ad - (N/l^\alpha)bc = 1$. Set

$$W_l = \frac{1}{\sqrt{l^\alpha}} \begin{pmatrix} l^\alpha a & b \\ Nc & l^\alpha d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{R}). \tag{2.1}$$

It follows that $(l, bc) = 1$, but we may have $l|a$ and $l|d$. Note that there are many possible choices of W_l and we do not prefer any over the others, as they are all equivalent up to multiplication by an element of $\Gamma_0(N)$ (see Lemma 1). Also note that W_l^{-1} is of the same form as W_l.

For composite numbers $n|N$ we may set

$$W_n := \prod_{l|n} W_l. \tag{2.2}$$

If $(n, N/n) = 1$ then W_n has the same shape as W_l in equation (2.1) but where l^α is replaced by n. In the case $n = N$ we do choose a canonical representative, namely

$$W_N = \frac{1}{\sqrt{N}} \begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix}.$$

The definition (2.2) of W_n only depends on the primes dividing n. In practice there are many different choices of n which would give the same W_n, for example if $N = 2^3 3^2 5$ then $W_6 = W_{12} = W_{18} = W_{24} = W_{36} = W_{72}$. For theoretical purposes one may assume that $(n, N/n) = 1$ without any loss of generality.

The crucial property of the matrices W_n is the following.

Lemma 1 *([1] Lemma 8) For any two choices W_n and W_n' we have*

$$W_n \Gamma_0(N) W_n' = \Gamma_0(N). \tag{2.3}$$

Proof. That $W_n \Gamma_0(N) W_n' \subseteq \Gamma_0(N)$ is a simple calculation. The equality follows from the fact that, for any W_n, the matrix W_n^{-1} is also of the same form. Thus, for all $\gamma \in \Gamma_0(N)$, we set $\gamma' = W_n^{-1} \gamma W_n'^{-1} \in \Gamma_0(N)$ and clearly $W_n \gamma' W_n' = \gamma$. □

Suppose $\tau_1, \tau_2 \in \mathcal{H}^*$ are in the same $\Gamma_0(N)$-orbit, i.e., there is some $\gamma \in \Gamma_0(N)$ such that $\tau_1 = \gamma\tau_2$. Then $W_n \gamma W_n^{-1} = \gamma' \in \Gamma_0(N)$ and $W_n\tau_1 = W_n\gamma\tau_2 = \gamma' W_n \tau_2$ and thus $W_n\tau_1$ and $W_n\tau_2$ are in the same $\Gamma_0(N)$-orbit. Therefore there is a well-defined action of the W_n on $X_0(N)$.

Clearly $W_n W_n^{-1}$ acts as the identity on $X_0(N)$. Since all the possible choices W_n act in the same way up to $\Gamma_0(N)$, it then follows that they give an **involution** on the curve $X_0(N)$ (i.e., a map such that its square is the identity).

We want to consider, for any $n|N$, the set $X_0(N)/W_n$ (i.e., where we identify points of $X_0(N)$ which are mapped to each other by W_n). This corresponds to the upper half plane modulo the group $G = \Gamma_0(N) \cup W_n\Gamma_0(N) \subset \mathrm{SL}_2(\mathbb{R})$. So we have

$$X_0(N)/W_n = G \backslash \mathcal{H}^*$$

and thus $X_0(N)/W_n$ is a Riemann surface. The index $[G : \Gamma_0(N)] = 2$ and so the obvious map $\phi : X_0(N) \to X_0(N)/W_n$ is a degree 2 meromorphic map ramified at certain points (namely, those $\Gamma_0(N)$-orbits which are fixed by W_n). Once again we translate these statements into the language of algebraic geometry and see that we have algebraic curves $X_0(N)$ and $X_0(N)/W_n$ with a rational map between them.

2.3 Modular Forms

We briefly state a few of the properties of modular forms which will be used in depth in our later work.

Definition 1 *A* **meromorphic modular form** *of weight k, level N and character χ is a mapping $f : \mathcal{H}^* \to \mathbb{C}$ such that*

(1) *f is meromorphic as a function $\mathcal{H} \to \mathbb{C}$*

(2) *For all $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$ and all $\tau \in \mathcal{H}^*$, $f(\gamma(\tau)) = \chi(d)(c\tau + d)^k f(\tau)$.*

(3) *f is meromorphic at the cusps*

If the character χ is not mentioned then assume it is identically 1.

Condition (2) is the most significant. We define an action of $\mathrm{SL}_2(\mathbb{R})$ on the space of modular forms by

$$f(\tau) \left| \begin{pmatrix} a & b \\ c & d \end{pmatrix} \right. := (c\tau + d)^{-k} f\left(\frac{a\tau + b}{c\tau + d}\right). \tag{2.4}$$

Thus the second condition may be rephrased as $f(\tau) \mid \gamma = \chi(d)f(\tau)$ for all $\gamma \in \Gamma_0(N)$. Note also that we may generalise equation (2.4) to give an action of $\mathrm{GL}_2(\mathbb{R})$ on the space of modular forms by defining $f(\tau)|\gamma := det(\gamma)^{k/2}(c\tau + d)^{-k}f(\gamma(\tau))$ in the obvious way.

The third condition of Definition 1 requires some explanation. Any cusp c of $X_0(N)$ may be mapped to ∞ by some $\sigma \in \mathrm{SL}_2(\mathbb{Z})$. This σ is determined up to multiplication by an element of $\Gamma_0(N)$. The **width** of the cusp c is defined to be the smallest $d \in \mathbb{N}$ such that $\sigma^{-1}\begin{pmatrix} 1 & d \\ 0 & 1 \end{pmatrix}\sigma \in \Gamma_0(N)$. A tedious calculation shows that the width is independent of the representative for σ chosen. Clearly the width of the cusp ∞ is $d = 1$. Note that, if $\gamma \in \Gamma_0(N)$ fixes c, then $\sigma\gamma\sigma^{-1}$ fixes ∞, and therefore $\sigma\gamma\sigma^{-1} = \pm T^n = \pm \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$ for some $n \in \mathbb{Z}$. Hence $\gamma = \pm\sigma^{-1}T^n\sigma$ and so n is a multiple of d. We need to choose a local parameter, q_c, from an open neighbourhood of ∞ as before, but in this case the open set at ∞ is only invariant under $\begin{pmatrix} 1 & \lambda d \\ 0 & 1 \end{pmatrix}$ where $\lambda \in \mathbb{Z}$. The map we choose is $q_c : \tau \mapsto \exp(2\pi i\tau/d)$. The function f is said to be **meromorphic at the cusp** c if the function $f|\sigma \circ q_c^{-1}$ is meromorphic at zero. This process gives the expansion

$$f|\sigma^{-1} = \sum_{n\in\mathbb{Z}} a_n \mathrm{exp}(2\pi i\tau)^{n/d}. \tag{2.5}$$

It is usual to write q =exp$(2\pi i\tau)$ and call (2.5) the q-expansion of the modular form f at the cusp c. We will often use this representation of modular forms.

The meromorphic modular forms clearly form a $\mathbb{C}$-vector space.

Definition 2 *A* **cusp form** *of weight k, level N and character χ is a meromorphic modular form as above but with the additional conditions*

1. *f is holomorphic on $\mathcal{H}$*
2. *f is zero at each cusp, i.e., the q-expansions have the form $\sum_{n>0} a_n q^{n/d}$.*

Write $S_k(N)$ for the $\mathbb{C}$-vector space of all cusp forms of weight k, level N and trivial character.

A **modular function** is a meromorphic modular form of weight zero. This is the same as being a meromorphic function on the Riemann surface $X_0(N)$. The derivative of such a function will be a form of weight 2 for $\Gamma_0(N)$. Thus there is a correspondence between the $\mathbb{C}$-vector space of all objects *df* (for all meromorphic functions f on $X_0(N)$) and the space of weight 2 forms. We will describe this correspondence in more detail in the following section.

2.4 Differentials

We will need a few results from the geometry of Riemann surfaces, particularly the Riemann-Roch theorem. We give a brief description here, following Griffiths and Harris [17] and several other sources. Write $\mathcal{K}$ for the $\mathbb{C}$-algebra of meromorphic functions on $X_0(N)$. All these definitions are for general Riemann surfaces but we state them only for $X_0(N)$ so that we may treat special cases (such as behaviour at cusps or elliptic points) as we go.

Definition 3 *The space of* **meromorphic differential forms** *on $X_0(N)$ is the $\mathcal{K}$-vector space generated by all symbols df where $f \in \mathcal{K}$ and where d is $\mathbb{C}$-linear and satisfies the properties*

1. $d(fg) = fdg + gdf$

2. $dc = 0$ *if c is a constant function.*

Thus we may view the set of differentials as $\{df \mid f \in \mathcal{K}\}$ or as $\{fdz \mid f \in \mathcal{K}\}$ for some fixed non-constant function $z \in \mathcal{K}$.

We now define the divisor of a meromorphic function f. Every point $P \in Y_0(N)$ corresponds to some (equivalence class of) $\tau_0 \in \mathcal{H}$. Let n be the size of the stabilizer in $\mathrm{PSL}_2(\mathbb{Z})$ of τ_0 (so n is the order of the elliptic point or 1 if P isn't an elliptic point). There is a local coordinate function $\lambda : \mathcal{H} \to \mathbb{C}$ which takes τ_0 to 0. So the function f may be viewed as a meromorphic function in a neighbourhood of 0, and thus as a Laurent series in the local parameter $t = \lambda^n$. Write ν for the valuation of this locally defined meromorphic function at 0. Define the valuation of f at P to be $\nu_P(f) = \nu/n$. Now suppose P is a cusp of $X_0(N)$. By the usual method (mapping P to ∞ and then taking a local parameter) we may view f as a meromorphic function on $\mathbb{C}$ at zero. Again we define $\nu_P(f)$ to be the valuation of this complex valued function at zero. If the cusp has width m then the valuation will lie in $\frac{1}{m}\mathbb{Z}$.

Definition 4 *The* **divisor of a modular function** f *is*

$$div(f) = \sum_{P \in X_0(N)} \nu_P(f)P.$$

We define the valuation of a differential ω at a point $P \in C$ to be the following. Choose any function $t \in \mathcal{K}$ such that $\nu_P(t) = 1$. That is to say that t has a simple zero at P. Consider the ratio ω/dt. This is a ratio of two differential forms and thus it is a function. We define the valuation of ω at P to be the valuation of the ratio. Using the notation of the previous paragraphs we have

$$\nu_P(\omega) := \nu_P(\omega/dt).$$

Definition 5 *The* **divisor of a meromorphic differential** ω *is*

$$div(\omega) = \sum_{P \in X_0(N)} \nu_P(\omega)P.$$

The **space of holomorphic differentials** *(sometimes called differentials of the first kind) is the $\mathbb{C}$-vector space*

$$\Omega^1(X_0(N)) = \{\textit{differentials } \omega \mid div(\omega) \geq 0\}.$$

Recall that two divisors are said to be **equivalent** if their difference is the divisor of a function. Since the ratio of two differentials on a curve is always a function on the curve, it follows that the divisors of differentials are all in the same equivalence class. This divisor class is called the **canonical class** and is denoted κ.

Proposition 1 *(Shimura [33] Proposition 2.16) Let $Q_1, \ldots, Q_u$ be the cusps of $X_0(N)$ and let $P_1, \ldots, P_r$ be the elliptic points (having orders $e_1, \ldots, e_r$ respectively). Then*

$$div(f) = div(fdz) + \sum_{i=1}^{r} \left(1 - \frac{1}{e_i}\right) P_i + \sum_{j=1}^{u} Q_j.$$

Since $0 \leq (1 - 1/e_i) < 1$ it is clear that

$$div(fdz) \geq 0 \text{ if and only if } div(f) \geq \sum_{j=1}^{u} Q_j.$$

The condition on the right hand side states that f is holomorphic and indeed zero at the cusps Q_j. So this proves the following.

Proposition 2 *The map $f \mapsto f dz$ gives an isomorphism of $\mathbb{C}$-vector spaces between $S_2(N)$ and the space of holomorphic differentials.*

In this thesis we are also interested in the curves $X_0(N)/W_n$. The following lemma will be useful.

Lemma 2 *The holomorphic differentials, $\Omega^1(X_0(N)/W_n)$, on $X_0(N)/W_n$ are isomorphic as a $\mathbb{C}$-vector space to the $\mathbb{C}$-span of the set*

$$S_n = \{f \in S_2(N) \mid f \mid W_n = f\}.$$

Proof. Let $\omega \in \Omega^1(X_0(N)/W_n)$. Then at each $\tau \in \mathcal{H}^*$ we may write ω locally as $f(z)dz$ for some function f. Thus ω may be equally interpreted as a holomorphic differential on $X_0(N)$, and thus as a weight 2 cusp form which (to abuse notation) we will call f. That $\omega(W_n(\tau)) = \omega(\tau)$ translates to the fact that $f \mid W_n = f$. Conversely, all the forms $f \in S_n$ clearly give holomorphic differentials on $X_0(N)/W_n$. Thus the vector spaces are isomorphic. □

2.5 The Riemann-Roch Theorem

The Riemann-Roch theorem will be used in several places in this work. We will state the result and mention some aspects of it. For proof we refer to Hartshorne [20].

Suppose we have a curve C of genus g and let D be a divisor on C. Define

$$L(D) = \{\text{meromorphic functions } f \text{ on } C \mid div(f) \geq -D\} \quad \text{and} \quad l(D) = \dim_{\mathbb{C}} L(D).$$

Let κ be the canonical class. Here we will be quite concrete and fix some differential, ω, and set $\kappa = div(\omega)$. The Riemann-Roch theorem states

$$l(D) - l(\kappa - D) = deg(D) + 1 - g.$$

We gather together some consequences of the Riemann-Roch theorem (for proof see, for instance, Iitaka [22] Chapter 6).

Proposition 3 *Let C be a curve of genus g. Then*

(1) $deg(\kappa) = 2g - 2$

(2) $l(\kappa) = g$

(3) *If $g \geq 1$ then $l(P) = 1$ for all points P on C.*

We now follow Clemens [6] and set

$$i(D) = \dim_{\mathbb{C}} I(D) \quad \text{where} \quad I(D) = \{\text{meromorphic differentials } \omega \mid div(\omega) \geq D\}.$$

Lemma 3 $i(D) = l(\kappa - D)$.

Proof. Let $f \in L(\kappa - D)$. Then $div(f) \geq D - \kappa$. Thus $div(f\omega) = div(f) + div(\omega) \geq D$ and so the differential $f\omega$ is in $I(D)$. The converse clearly also holds. □

Combining Lemma 3 with Proposition 2 and taking $D = 0$ shows that $\dim_{\mathbb{C}} S_2(N) = \text{genus}(X_0(N))$.

2.6 Hyperelliptic Curves

Hyperelliptic curves appear, in this thesis, as a special case, for which separate methods should be used. We will show that the canonical map is not an embedding for these curves. Hyperelliptic curves cannot be ignored as there certainly are significant hyperelliptic modular curves and quotients.

We will always be considering modular curves and these will always have at least one rational point (the cusp at infinity) therefore curves of genus 1 will always be elliptic curves. The Shimura-Taniyama-Weil conjecture states that every elliptic curve defined over $\mathbb{Q}$ is parameterised by some modular curve $X_0(N)$. Recent work of Wiles, Taylor and Diamond has proved this conjecture in a large number of cases. As the study of elliptic curves is already very advanced we don't expect to be able to contribute anything new to the theory here. We will generally be more interested in curves having genus at least 3.

Definition 6 *A* **hyperelliptic curve** *is a curve C with a degree 2 map $\phi : C \to \mathbb{P}^1(\mathbb{C})$.*

The following proposition gives two more possible definitions of a hyperelliptic curve.

Proposition 4 *Let C be a genus g curve over $\mathbb{C}$. Then the following are equivalent.*

(1) *C is hyperelliptic*

(2) *There is a function z on C which has precisely 2 poles (counted with multiplicity).*

(3) *The curve C has an equation in the following (so-called "hyperelliptic") form*

$$w^2 = p(z)$$

where $p(z)$ is some polynomial of degree $2g + 2$.

Proof. That (1) ⇒ (2) is just a restatement of the definition since ϕ itself is a degree 2 map (and any non-constant ϕ must have a pole). The statement (2) ⇒ (1) is immediate.

To show (2) ⇒ (3), consider the ramification points in $\mathbb{P}^1$ for $z = \phi$. Since the map has degree two, each point can have ramification index at most 2. By the Hurwitz formula there must be $2g + 2$ distinct ramification points. We may assume that none of these points are at ∞. Label their pre-images $P_1, \ldots, P_{2g+2}$. Now consider the "multivalued function"

$$w = \sqrt{\prod_{j=1}^{2g+2} (z - z(P_j))}. \tag{2.6}$$

It can be shown (see Farkas and Kra [13] Proposition III.7.4) that this may be chosen to be a meromorphic function on C. Hence $w^2 = p(z)$ (where p is the polynomial given by the right hand side of (2.6)) is an equation for the curve.

Finally, it is clear that (3) ⇒ (1), as the function z will have degree 2 and $2g+2$ ramification points and thus (by the Hurwitz formula) will map to a genus zero curve. □

Moreover, it can be shown (see Farkas and Kra [13] III.7.3) that the function $z = \phi$ above is unique up to a linear fractional transformation on $\mathbb{P}^1$.

From the hyperelliptic equation, $w^2 = p(z) = \prod_j (z - z(P_j))$, of a hyperelliptic curve C it can be seen that there is an obvious involution, namely the map $\iota : w \mapsto -w$. The $2g + 2$ ramification points of the map $z = \phi$ are precisely the fixed points of ι and these are also known as the **Weierstrass points**. When $g \geq 2$ it is a fact that if i is any other involution fixing $2g + 2$ points then, since there cannot be a non-trivial Möbius transformation fixing 6 or more points, $i = \iota$ (see Farkas and Kra [13] page 102). The involution ι is therefore unique and is called the **hyperelliptic involution**.

We will use the following result later in this chapter.

Lemma 4 *Let C be a hyperelliptic curve with hyperelliptic involution ι. Then $\iota(P) = Q$ if and only if there is a function f on C which has simple poles precisely at P and Q.*

Proof. If $\iota(P) = Q$ then it follows that P and Q have the same image (say $[a : b] \in \mathbb{P}^1(\mathbb{C})$) under the hyperelliptic projection $\pi : C \to \mathbb{P}^1$. Consider the function f on $\mathbb{P}^1$ defined by $f([x : y]) = x/(ay - bx)$ (or $y/(ay - bx)$ if $a = 0$). Then f has a simple pole at $[a : b]$ and thus $\pi^* f$ has simple poles at precisely P and Q.

Conversely, suppose $div(f) = -P - Q + D$ (where $D \geq 0$). Then f induces a hyperelliptic projection $f : C \to \mathbb{P}^1$. The projection obtained from f induces an involution which fixes the $2g + 2$ Weierstrass points and, by uniqueness, this involution must be ι. □

This lemma allows us to prove the following result.

Proposition 5 *The hyperelliptic involution ι on a hyperelliptic curve C commutes with every $\sigma \in$Aut(C).*

Proof. We must show that $\iota(\sigma(P)) = \sigma(\iota(P))$. For an arbitrary P let $Q = \iota(P)$. Then by the previous lemma there is a function f with simple poles precisely at P and Q. Now σ is an automorphism of C so we may consider $g = (\sigma^{-1})^* f = f \circ \sigma^{-1}$. This function g has simple poles precisely at $\sigma(P)$ and $\sigma(Q)$, i.e., $\iota(\sigma(P)) = \sigma(Q) = \sigma(\iota(P))$. □

Suppose $X_0(N)$ is a modular curve such that, under one of the involutions W_n, the curve $X_0(N)/W_n$ has genus zero. Then it follows that $X_0(N)$ is hyperelliptic and that the involution W_n is the hyperelliptic involution.

The preceding paragraph gives a simple way to identify hyperelliptic modular curves. For instance the curves $X_0(35)$ and $X_0(39)$ are hyperelliptic. The reason for this is that Table 5 of Antwerp 4 [2] shows that the weight 2 forms for these curves split as $0, 1, 2, 0$. This notation (for more detail about the use of Table 5 of [2], see Section 3.4 or the introduction to the tables in Antwerp 4 [2]) represents the dimensions of the eigenspaces of weight 2 cusp forms of composite level $p^a q^b$. The sequence $0, 1, 2, 0$ means that there are no forms which have eigenvalue $+1$ with respect to both W_p and W_q, there is a one dimensional space of forms having eigenvalue $+1$ with respect to W_p and eigenvalue -1 with respect to W_q etc. Thus in both cases the quotient curves $X_0(N)/W_N$ have genus zero.

Some care should be taken with this trick. Consider, for instance, $X_0(34)$. The eigenforms split (again using [2] Table 5) as $0, 1, 1, 1$. It is tempting to say that $X_0(34)/W_{34}$ has genus 0 but this is false. There is a form with eigenvalue -1 with respect to both W_2 and W_{17}, and thus it has eigenvalue $+1$ under $W_{34} = W_2 W_{17}$. Hence $X_0(34)/W_{34}$ has genus 1. What can be said is that the curve $X_0(34)/\langle W_2, W_{17}\rangle$ has genus zero. However the group $\langle W_2, W_{17}\rangle$ has order 4, so the covering map in this case has degree 4.

Note that there are several hyperelliptic modular curves. The most well-known example is $X_0(37)$, whose hyperelliptic involution is not an Atkin-Lehner involution. Also there are the cases $X_0(40)$ and $X_0(48)$ where the hyperelliptic involution is not an Atkin-Lehner involution though, it does come from an element of $\mathrm{SL}_2(\mathbb{Z})$. Ogg [30] gives a full list of all the hyperelliptic modular curves $X_0(N)$.

Finally we make a comment about the point at infinity on a genus 2 hyperelliptic equation. Usually our genus 2 curves will arise as some smooth projective variety which we then project into $\mathbb{P}^2(\mathbb{C})$. In these cases the point $[x : y : z] = [0{:}1{:}0]$ at infinity will be singular. Topologically there are actually two points, ∞^+ and ∞^-, on the curve above $[0{:}1{:}0]$. The hyperelliptic projection $\phi : [x : y : z] \mapsto [x : z]$ is not defined at $[0{:}1{:}0]$. We set $\phi([0{:}1{:}0]) = [1{:}0]$ and this is compatible with the action of ϕ away from $[0{:}1{:}0]$. In the case of a degree 5 curve, y^2 =quintic, there is only one point on the curve above the singularity $[0{:}1{:}0]$ and this point is a Weierstrass point.

2.7 Canonical Projective Models

It will be useful, in the later chapters, to know what equations of higher genus projective curves may look like. For genus 3, 4 and 5 we will generally have one canonical non-hyperelliptic equation.

The image of the canonical embedding into $\mathbb{P}^2$ of a non-hyperelliptic genus 3 curve will always be a plane quartic (see Hartshorne [20] Example IV.5.2.1). This follows since such a curve must have degree 4.

Hartshorne [20] Example IV.5.2.2, shows that the image of the canonical embedding into $\mathbb{P}^3$ of a non-hyperelliptic genus 4 curve will be the complete intersection of a degree 2 surface with a degree 3 surface in $\mathbb{P}^3$. We will describe such curves by giving equations for the two surfaces.

The image of the canonical embedding of a non-hyperelliptic genus 5 curve in $\mathbb{P}^4$ does not have a single standard form. We will find that most of our examples may be expressed as the intersection of three 3-folds of degree 2 in $\mathbb{P}^5$. Such curves will have degree 8. We now show why such a situation may be expected to occur often.

We will use the Riemann-Roch theorem and the canonical divisor class κ to understand the functions on a general curve. Recall that $\deg(\kappa) = 2g - 2$. Also recall that we have shown the existence of holomorphic differentials. Thus we may choose a *positive* divisor $div(\omega) \in \kappa$ and this will simplify some of our later arguments. It is easy to show that, for genus $g \geq 3$,

$$l(n\kappa) = \begin{cases} 1 & n = 0 \\ g & n = 1 \\ (2n-1)(g-1) & n \geq 2 \end{cases} \tag{2.7}$$

We have $l(\kappa) = 5$ so choose a basis $\{1, w, x, y, z\}$ for $L(\kappa)$. Now $l(2\kappa) = 12$ and $L(2\kappa)$ contains the 15 terms $\{1, w, x, y, z, w^2, wx, wy,\ wz, x^2, xy, xz,\ y^2, yz, z^2\}$. By linear algebra there must be at least 3 linear dependencies. In the simplest case these relations will describe three quadric 3-folds in $\mathbb{A}^4(\mathbb{C})$ and they will give a degree 8 curve, of genus 5, which is a complete intersection. There are other cases which arise. In particular, $X_0^+(181)$ and $X_0^+(227)$ are genus 5 curves whose canonical models are the intersection of the three quadric 3-folds (which must exist by our earlier argument) with 2 further cubic 3-folds.

Note that, in this section, we have given the equations in affine space. In the applications we will usually work with projective space. It is clear that these arguments also apply to the projective situation.

If one considers curves of genus at least 6 then there are many more possible forms of model and the geometry becomes much more intricate. In particular, for genus at least 6, the canonical curve is never a complete intersection.

2.8 Hecke Operators

The description of Hecke operators in the general setting may be found in Shimura [33]. Hecke operators will not play a major role in this thesis, so we mention just a few of the key definitions and properties.

We follow the paper of Atkin and Lehner [1] and so restrict to the case of modular forms of *even* weight.

Atkin and Lehner define operators T_p^* and U_l^* (here we assume $(p, N) = 1$ and $l|N$) in the classical manner. They also define operators on the q-expansions of a cusp form $f(\tau) = \sum a_n q(\tau)^n$ in the following way. Note that our k is twice the k used in [1], and also note the convention that $a_{n/p} = 0$ if $p \nmid n$.

$$\begin{aligned} f \mid T_p &:= \textstyle\sum_{n\geq 1} \left(a_{np} + p^{k-1} a_{n/p}\right) q^n \\ f \mid U_l &:= \textstyle\sum_{n\geq 1} a_{nl} q^n \end{aligned}$$

The relation between these two definitions is

$$\begin{aligned} f \mid T_p &= p^{k/2-1} f \mid T_p^* \\ f \mid U_l &= l^{k/2-1} f \mid U_l^*. \end{aligned}$$

Thus the two notions differ only by a constant (which is one in the weight 2 case anyway) and so we will tend to use whichever definition suits our purposes best.

2.9 The Petersson Inner Product

The Petersson inner product is a generalisation of the natural inner product on differentials $\langle \omega, \omega' \rangle = \int_X \omega \wedge \overline{\omega'}$.

Let f and g be cusp forms of *even* weight k and level N. Let $\mathcal{F}$ be a fundamental domain for the action of $\Gamma_0(N)$ on $\mathcal{H}^*$ (we will not discuss fundamental domains in any detail here). Writing $\tau = x + iy$ we make the following definition.

Definition 7 *The* **Petersson inner product** *of f and g is*

$$\langle f, g \rangle = \int_{\mathcal{F}} f(x+iy)\overline{g(x+iy)} y^{k-2} dx dy.$$

One of the most important properties of this inner product is the following proposition. We refer to the paper of Atkin and Lehner [1].

Proposition 6 *For p coprime to N, the Hecke operators, T_p, are Hermitian with respect to the Petersson inner product, i.e.,*

$$\langle f|T_p, g \rangle = \langle f, g|T_p \rangle .$$

This also holds for the Atkin-Lehner involutions W_q when $q|N$.

A corollary of this proposition is that the eigenvalues of a normalised eigenform f (which are simply its q-expansion coefficients) are all real.

2.10 Newforms

Once again we restrict to cusp forms of even weight k on $\Gamma_0(N)$.

For any $m \in \mathbb{N}$ we have $\Gamma_0(N) \supseteq \Gamma_0(mN)$ and so a modular form of level N is evidently a form of level mN. Further, if $f(\tau)$ is a form of level N then $f(m\tau)$ is a form of level mN. For a given N we call a form of level N **old** if it arises as some $f(n\tau)$, for some form $f(\tau)$ of level strictly less than (and necessarily dividing) N. The **old subspace** is the sub-vector-space of $S_2(N)$ which is generated by all the old forms.

The **new** subspace of $S_2(N)$ is the orthogonal complement of the old subspace with respect to the Petersson inner product. We fix a basis of the new subspace of $S_2(N)$ which consists of forms which are eigenforms with respect to all the T_p (for $(p, N) = 1$) and also for the W_q (for $q|N$). The elements of this basis are called the **newforms** of weight k and level N. That these notions are all well-behaved follows from [1]. Note that we use the convention that whenever we say “newform” it is implicit that forms are both cusp forms and eigenforms.

2.11 Atkin-Lehner Theory

The paper of Atkin and Lehner [1] gives more information about the behaviour of the newforms. We quote what we need from their main theorem.

Theorem 1 *([1] Theorem 5) The vector space, of cusp forms of even weight k on $\Gamma_0(N)$, has a basis consisting of oldclasses and newclasses. All forms in a class have the same eigenvalues with respect to the operators T_p (for $(p, N) = 1$). Each newclass consists of a single form f which is also an eigenform for the W_l and U_l $(l|N)$. We choose f to be* **normalised** *(i.e., $a_1 = 1$ in the q-expansion). Then f satisfies*

$$\begin{aligned} f \mid T_p &= a_p f \\ f \mid U_l &= a_l f \\ f \mid W_l &= \lambda_l f \end{aligned}$$

where, if $l||N$ we have $a_l = -l^{k/2-1}\lambda_l$, and if $l^2|N$ then $a_l = 0$. It then follows that the q-expansion coefficients for f satisfy $a_{p^n} = a_p a_{p^{(n-1)}} - p^{k-1} a_{p^{(n-2)}}$ and $a_{mn} = a_m a_n$ (if $(m, n) = 1$). Further, each oldclass is of the form $\{g(d\tau) \mid g$ is a newform of some level M, and d runs through all divisors of $N/M\}$. The oldclasses may be given a different basis consisting of forms which are eigenforms for all the W_l.

In general, there are forms whose eigenvalues lie in a number field. As a result there will often be sets of classes (either newclasses or oldclasses) which are all Galois conjugates of each other.

In later work we will often need to choose certain oldforms having prescribed behaviour with respect to the Atkin-Lehner involutions W_p. For the rest of this section we will discuss how this is done.

Lemma 5 *Suppose $f(\tau)$ is a weight 2 newform of level m and suppose $p \nmid m$. Let $\epsilon = \pm 1$. Then $g(\tau) := f(\tau) + \epsilon p f(p\tau)$ is a cusp form on $\Gamma_0(mp)$ and it has eigenvalue ϵ with respect to W_p. Also, $g(\tau)$ has the same eigenvalues as $f(\tau)$ with respect to W_q for $q|m$.*

Proof. Certainly, $g(\tau)$ is a cusp form on $\Gamma_0(mp)$. Select $a, b \in \mathbb{Z}$ such that $pa - bm = 1$ and set

$$W_p = \frac{1}{\sqrt{p}} \begin{pmatrix} pa & b \\ mp & p \end{pmatrix}, A_p = \frac{1}{\sqrt{p}} \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad \gamma = \begin{pmatrix} a & b \\ m & p \end{pmatrix}.$$

Note that $\gamma \in \Gamma_0(m)$, that $A_p W_p \in \Gamma_0(m)$ and that $W_p = \gamma A_p$. Now $pf(p\tau) = f(\tau)|A_p$ and so we have

$$(f(\tau) + \epsilon p f(p\tau)) \, |W_p = f(\tau)|\gamma A_p + \epsilon f(\tau)|A_p W_p = pf(p\tau) + \epsilon f(\tau).$$

For the other involutions, W_q, it can be shown that $A_p W_q$ is of the same form as $W_q A_p$ and the result follows. □

The following lemmas are proved in a similar manner and clearly one may state generalisations of them.

Lemma 6 *Suppose $f(\tau)$ is a weight 2 newform of level m and suppose $p \nmid m$. Let $\epsilon = \pm 1$. Set $g(\tau) := f(\tau) + \epsilon p^2 f(p^2\tau)$ and $h(\tau) := f(p\tau)$. Then $g(\tau)$ and $h(\tau)$ are forms on $\Gamma_0(p^2 m)$ and g has eigenvalue ϵ with respect to W_p and h has eigenvalue $+1$.*

Lemma 7 *Suppose $f(\tau)$ is a weight 2 newform of level m where, in this case, $p|m$ and suppose $f(\tau)$ has eigenvalue $\epsilon = \pm 1$ with respect to W_p. Then $g(\tau) := f(\tau) \pm \epsilon p f(p\tau)$ is a cusp form on $\Gamma_0(mp)$ and it has eigenvalue $\pm\epsilon$ with respect to W_p.*

2.12 The Canonical Embedding

On a curve C the holomorphic differentials, $\Omega^1(C)$, give rise to a line bundle, and this is called the **canonical bundle**. This line bundle, in certain situations, gives an embedding into projective space. In this section we follow the more concrete approach of Griffiths and Harris [17]. A description of the canonical embedding from the point of view of invertible sheaves is given in Hartshorne [20].

For the time being we work with a general Riemann surface C of genus $g \geq 2$. We will never be concerned with the case of genus 0 or 1 in this thesis.

Let $\omega_1, \ldots, \omega_g$ be a basis for $\Omega^1(C)$. Viewing C as a Riemann surface, we may choose a finite covering of open sets, with local parameters z on each set, such that we can locally write $\omega_j = f_j(z)dz$. Consider the map

$$\begin{aligned} \phi : \quad C &\rightarrow \mathbb{P}^{g-1} \\ P &\mapsto [\omega_1(P) : \cdots : \omega_g(P)]. \end{aligned} \tag{2.8}$$

Note that, away from the cusps, $[\omega_1(P) : \cdots : \omega_g(P)] = [f_1(P) : \cdots : f_g(P)]$.

For this to be a well-defined mapping it must never map to $[0 : \cdots : 0]$. We show that this cannot occur. Let P be any point on the curve and let D be the divisor P. Firstly $l(P) = 1$ (see Proposition 3) so the only functions which have at worst a single pole at P are the constant functions. Hence, applying the Riemann-Roch theorem, we get $i(P) = g-1$. Thus there is a $(g-1)$-dimensional space of differentials vanishing at P but that means there is a one-dimensional space of differentials which do not vanish at P. Another way to phrase this would be to say that the canonical linear system $|\kappa|$ has no base points.

We will give a criterion for the canonical map to be an embedding.

Lemma 8 *If g = genus(C) ≥ 2 and C is not hyperelliptic then the canonical map is injective.*

Proof. This map will fail to be injective if there are points P, Q such that, for all differentials ω, we have $\omega(P) = 0 \Rightarrow \omega(Q) = 0$. This statement may be written (using the notation of Section 2.5) as $i(P+Q) = i(P)$. The Riemann-Roch theorem then states that $l(P+Q) = 1 + l(P)$, which implies that there is a function $f \in L(P+Q) - L(P)$. This function must have a pole at Q as it isn't in $L(P)$, on the other hand $l(Q) = 1$ so it must have a pole at P too. So we have a function with precisely 2 simple poles. □

The image of the canonical map, in the non-hyperelliptic case, is a curve of degree $2g-2$ (see Hartshorne [20] Example IV.3.3.2 on page 309). We call this curve a **canonical curve**.

If one takes the canonical map of a hyperelliptic curve then it is possible to predict what will happen. Indeed, suppose C is a hyperelliptic curve of genus g and let $f : C \rightarrow \mathbb{P}^1(\mathbb{C})$ be the degree 2 map arising from the hyperelliptic involution. Then Hartshorne [20] Proposition IV.5.3 shows that the canonical map $\phi : C \rightarrow \mathbb{P}^{g-1}(\mathbb{C})$ factors through $\mathbb{P}^1(\mathbb{C})$, as f followed by the $(g-1)$-uple embedding of $\mathbb{P}^1$ into $\mathbb{P}^{g-1}$. Thus the image of C in $\mathbb{P}^{g-1}(\mathbb{C})$ will be a smooth curve which is isomorphic to $\mathbb{P}^1(\mathbb{C})$ and which is described by $(g-1)(g-2)/2$ quadric equations. This means that it is possible to distinguish hyperelliptic curves C from non-hyperelliptic ones by examining their images under the canonical embedding.

Now let us specialize the canonical embedding to the case of the curves $X_0(N)$. Here we know that the differentials correspond precisely to the weight 2 cusp forms. There are involutions acting on the space of cusp forms. The behaviour of the cusp forms with respect to the involutions will give us information on the canonical embedding. We give an example.

Example. Consider the genus 3 curve $X_0(41)$. The basis of newforms for $S_2(41)$ consists of 3 forms f_j such that $f_j(\tau) \mid W_{41} = -f_j(\tau)$. We have the canonical map

$$\begin{array}{rcrcl} \phi & : & X_0(41) & \to & \mathbb{P}^2 \\ & & \tau & \mapsto & [f_1(\tau), f_2(\tau), f_3(\tau)]. \end{array}$$

Now $\phi(W_{41}(\tau)) = [f_j(W_{41}(\tau))] = [-(41\tau)^2 f_j(\tau)] = [f_j(\tau)] = \phi(\tau)$ since projective coordinates are defined only up to scalar multiples. Note that, at the cusps, all the $f_j(\tau)$ are zero so one really should work with the differentials $f_j(\tau)d\tau$, however this is not a problem as our construction is generically valid. The fact that $\phi(W_{41}(P)) = \phi(P)$ is equivalent to the statement that ϕ factors through $X_0^+(41) = X_0(41)/W_{41}$. Thus the map ϕ in this case is really

$$\phi : X_0^+(41) \to \mathbb{P}^2$$

and $X_0^+(41)$ is a genus 0 curve. The genus 3 curve $X_0(41)$ is hyperelliptic.

Chapter 3

The Canonical Embedding of Modular Curves

We already know that the modular curves $X_0(N)$ have projective models defined over $\mathbb{Q}$. Furthermore, there is an opinion (championed for instance by Atkin and Elkies) that these models may be chosen to have relatively small coefficients. We are interested in gathering evidence for this claim, in the hope that doing so will allow us to understand the nature of the phenomenon.

In this Chapter we discuss how to compute the image of the canonical embedding of modular curves $X_0(N)$. We give a table of results of our computations, listing mainly models for curves of genus less than or equal to 5.

3.1 Theory

Consider the modular curves $X_0(N)$. As we have seen in the previous chapter, the space of holomorphic differentials $\Omega^1(X_0(N))$ is isomorphic, as a $\mathbb{C}$-vector space, to the space of weight 2 cusp forms, $S_2(N)$, on $\Gamma_0(N)$. Indeed, let $\{f_1(\tau), \ldots, f_g(\tau)\}$ be a basis for $S_2(N)$, then the set $\{f_j(\tau)d\tau\}$ forms a basis for $\Omega^1(X_0(N))$. Thus the canonical map in this situation is simply

$$\phi : \tau \mapsto [f_1(\tau) : \cdots : f_g(\tau)].$$

In this chapter only non-hyperelliptic curves $X_0(N)$ are considered, and so the image of the canonical map ϕ is a projective model for $X_0(N)$. This image is a curve of degree $2g-2$ and it will be described by some set of projective equations of the form $\Phi(f_1, \ldots, f_g) = 0$. In the case that it is a complete intersection, the equations have degrees whose product is $2g-2$. It is possible to interpret each $\Phi(f_1(\tau), \ldots, f_g(\tau))$ as a modular form which is zero at every $\tau \in \mathcal{H}^*$. Thus these forms may be interpreted as the zero cusp form of weight $2deg(\Phi)$.

To construct equations for modular curves we take (from tables) the q-expansions of a basis for the space $S_2(N)$. We compute a set of equations Φ by finding combinations of powers of the q-expansions which yield identically zero series (more details will be given in the next section). When the product of the degrees of the polynomials in Φ is equal to $2g-2$ and the variety defined by them is one dimensional, then the zero locus of Φ contains a model for the embedding of $X_0(N)$ which has the right dimension and degree, and thus it is a model for the canonical curve. For higher genus the canonical curve ceases to be a complete intersection and, though we may find equations which determine the model, it is not so easy to check that they are correct. This situation is not a flaw in the method, however it makes it harder to check against human error in the implementation of the method.

It is possible to choose a basis for $S_2(N)$ such that all the basis elements are eigenforms with respect to the Hecke operators T_p (for $p \nmid N$) and the involutions W_q for all $q|N$ (see Section 2.11). The differentials on the curve $X_0(N)/W_n$ will be those differentials on $X_0(N)$ which are invariant under the action of W_n. Such differentials correspond to those eigenforms in the basis of $S_2(N)$ which have eigenvalue $+1$ with respect to W_n. Thus the image of the canonical mapping of $X_0(N)/W_n$ will be the curve described by the set of polynomials Φ which give relations between forms in the corresponding subset of the basis of eigenforms for $S_2(N)$. If $X_0(N)/W_n$ has genus larger than 2 and is not hyperelliptic then this will give a model for its canonical embedding.

Note that this method may be used for computing equations for any modular curves $\Gamma\backslash\mathcal{H}^*$ as long as there is a method to compute explicit q-expansions for the weight two cusp forms on the group Γ.

3.2 Method

Methods for computing a basis for $S_2(N)$ are already well-known. There are also various tables published which contain such data. For instance, Tingley computed Hecke eigenvalues way back in 1975 [43]. Also Cremona [8] has Hecke eigenvalues for weight 2 cusp forms, although he restricts attention to rational newforms whereas we are interested mainly in those forms whose coefficients lie in larger number fields (as we are interested in curves of genus larger than one). The most complete tables are those generated by Cohen and Zagier [7]. Although these have not been published they are in wide circulation. They list q-expansion coefficients up to q^{100} for all weight 2 newforms of level up to 198.

Using the lemmas at the end of Section 2.11 we may also easily find a basis consisting of Hecke eigenforms (eigenforms with respect to the T_p when $p \nmid N$ and the W_q when $q|N$) for the old subspace. Thus we may easily find a basis of eigenforms for $S_2(N)$.

Let $f = \sum a_n q^n$ be a cusp form of weight 2 for $\Gamma_0(N)$ and let K_f be the field extension of $\mathbb{Q}$ generated by the coefficients of the q-expansion for f. We assume that f is normalised so that the a_n are algebraic integers which generate K_f. We may choose a form f so that its Galois conjugates span the eigenclass associated to f. Suppose $\{\alpha_0, ..., \alpha_m\}$ is an integral basis for K_f. Then we may write the coefficients as

$$a_n = \sum_{i=0}^{m} a_{n,i}\alpha_i$$

where $a_{n,i} \in \mathbb{Z}$. We may therefore consider the formal q-expansions

$$f_i := \sum_n a_{n,i} q^n$$

which have the honourable property that the coefficients of their q-expansions are rational integers. Clearly $f = \sum f_i \alpha_i$. The f_i are no longer eigenforms with respect to the Hecke operators T_p (where $(p, N) = 1$) but they are eigenforms for the W_q. The f_i are linear combinations (over K_f) of the conjugates of f. We use the f_i for computation because working with integers is simpler and also because this will ensure that the equations we construct will be defined over $\mathbb{Q}$. Of course, for computer calculation, we are forced to take only a finite initial segment of the q-expansion. We discuss the number of terms required for these finite q-expansions at the end of this section.

Hence we may assume that we have a basis for $S_2(N)$ consisting of integral q-expansions and such that the forms split into eigenclasses under all the W_q with $q|N$.

The algorithm is as follows. Let $X_0(N)$ (or $X_0(N)/W_n$) be the curve of genus g for which we want to obtain a projective model. Take a set $\{f_0, ..., f_m\}$ of integral q-expansions which are a $\mathbb{C}$-basis for the particular subset of $S_2(N)$ which corresponds to the modular curve we are hunting. Choose an integer d, which may be predicted from knowing the form of the canonical models for curves of genus g in $\mathbb{P}^{g-1}$ (see Section 2.7). Compute all monomials of degree d in the f_i and let n_d be the number of such monomials. They form a set of n_d cusp forms of weight $2d$ on $\Gamma_0(N)$. Construct a matrix M which has n_d columns and as many rows as there are terms in the q-expansions we are using. Thus the (i,j)-th entry in the matrix M is the jth q-expansion coefficient of the ith monomial. We now apply the PARI−GP function `kerint` to the transpose of M. This function produces an LLL-reduced basis for the kernel of this matrix. This gives a collection of linear combinations of rows of the matrix M, each of which equals zero. Since the matrix rows correspond to monomials in the f_i, these linear combinations of matrix rows may be interpreted as homogeneous degree d polynomials in the f_i. The function `kerint` produces a basis for the matrix kernel and therefore, when the curve is described by equations of degree d, we get a generating set for the ideal describing the canonical curve in $\mathbb{P}^{g-1}$. In some cases (e.g., curves of genus 4), the canonical model is given by equations of different degrees. In these cases it is necessary to repeat the above process and then discard the multiples of lower degree polynomials. Note that we obtain models whose coefficients are very small (although we cannot prove that they are minimal) since `kerint` uses LLL-reduction.

The algorithm described above will produce a set of equations whose intersection is an integral model for the canonical curve. Experimental evidence shows that the equations obtained by this method have the property that their coefficients are reasonably small. Certainly the coefficients have size roughly bounded by N. This is perhaps not so surprising since the weight 2 cusp forms have reasonably small coefficients in their q-expansions.

We stress that the algorithm itself is merely simple linear algebra on the q-expansions. The "hard" work has been already done with the computation of the modular forms and hence no special techniques are required. On the other hand, the matrix M gets quite large in practice. Also there is some work in checking the equations in the genus 4 case (and some genus 5 cases) as we need to separate degree 2 and a degree 3 hypersurfaces.

As a final note we need to decide what "precision" must be worked with. The key step is finding a cusp form of weight $2d$ with zero q-expansion at the cusp ∞. The following proposition (which we quote from a paper of Frey [15], though it is well-known) tells us when such a form is zero.

Proposition 7 *Let f be a cusp form of weight k on $\Gamma_0(N)$. Write $\mu = [SL_2(\mathbb{Z}) : \Gamma_0(N)] = N\prod_{p|N}(1+1/p)$. If f has a zero of order $\geq \mu k/12$ then f is the zero form.*

Proof. The form f is a cusp form so it has no poles. Its total number of zeroes is certainly $\geq \mu k/12$. This contradicts the usual bound on the number of zeroes of holomorphic forms (see for instance Schoenenberg [32] Chapter V, Theorem 8). □

We note, once again, that the algorithm we have given will work for any non-hyperelliptic curves $X_0(N)$ or $X_0(N)/W_n$ of genus at least 3. In the applications we will be mainly concerned with curves of genus less than or equal to 5 as, in these cases, it is relatively easy to check our results.

3.3 Example

To embed a modular curve $X_0(p)$ (where p is a prime) of genus 3 we aim (bearing in mind Section 2.7) for a quartic curve in $\mathbb{P}^2(\mathbb{C})$. Therefore, our degree 4 monomials will correspond to forms of weight 8. Thus any form $f(\tau) = \sum_n a_n q^n$ with $a_n = 0$ for all $n \leq 2(p+1)/3$ will in fact be the zero form.

In practice this bound is far larger than necessary, though it pays to keep the extra terms as a check against error.

For example, consider $p = 43$. From the tables we choose a basis $\{f, g, h\}$ for $S_2(43)$ such that each is represented as an integral q-expansion with 30 terms. For all integer triples (i, j, k) with $i + j + k = 4$ and $0 \leq i, j, k \leq 4$ we compute the q-expansion of the monomial $f^j g^j h^k$. We write all these monomials into a matrix M. We find that the transpose of M has a one-dimensional kernel. This space corresponds to a certain linear combination of rows of M and thus to a relation between the weight 2 forms.

Our method only works for non-hyperelliptic curves. Fortunately Ogg [30] has classified all hyperelliptic modular curves. Indeed, $X_0(N)$ is hyperelliptic with genus greater than or equal to 2 for precisely $N \in \{30, 33, 35, 37, 39, 40, 41, 46, 47, 48, 59, 71\}$. It is not completely known in advance which of the quotients $X_0(N)/W_n$ will be hyperelliptic. Clearly $X_0(N)/W_n$ will be hyperelliptic if it has genus 2 or if there is some Atkin-Lehner involution W such that $(X_0(N)/W_n)/W$ has genus zero. It can happen that $X_0(N)/W_n$ is hyperelliptic for neither of these reasons (just as $X_0(37), X_0(40)$ and $X_0(48)$ are hyperelliptic). Some examples of hyperelliptic quotient curves are the genus 2 curves $X_0(52)/W_2$, $X_0(52)/W_{52}$, $X_0(57)/W_3$,$X_0(57)/W_{57}$,$X_0^+(67)$, $X_0(72)/W_2$, $X_0(72)/W_{72}$ and $X_0^+(73)$. The calculations have also revealed the four hyperelliptic genus 3 curves $X_0(51)/W_3, X_0(55)/W_5$, $X_0(56)/W_2$ and $X_0(72)/W_3$. For the first three of these curves, the hyperelliptic involution is an Atkin-Lehner involution W_q. Hyperelliptic curves are detected using the criterion discussed in Section 2.12. One computes the image of their canonical mappings and notes that the image is described by too many quadrics (a hyperelliptic curve will have a canonical image described by $(g-1)(g-2)/2$ quadrics). Thus we conclude (after checking our calculation!) that the curve must be hyperelliptic. In these cases we may construct a model for the quotient curve by using our model for $X_0(N)$ and factoring by W_n using algebraic manipulation. Also it is possible to obtain models for hyperelliptic curves using the techniques given in the next chapter.

3.4 Calculation of Quotient Curves

Our main goal has been to calculate a model for the image of the canonical embedding of genus 3, 4 or 5 curves. Once these equations have been obtained it is possible to find equations for the quotient curves directly. We believe that there is enough interest in these curves to warrant listing their equations too. Note that we are not concerned with equations of genus zero so we do not give equations for such curves.

For each divisor, n, of N, the Atkin-Lehner involution, W_n, gives a degree 2 rational map $X_0(N) \to X_0(N)/W_n$ (though recall that W_n depends only on the primes dividing n). It is possible to exhibit this map algebraically when one has a suitable model for the curve $X_0(N)$. Note that a projective model for the image curve $X_0(N)/W_n$ will be one in which the variables all have the same behaviour under W_n. In general we will arrange that the image curve is described by an equation in variables which have eigenvalue $+1$ under W_n. In certain cases, however, we will write our equation using variables which have eigenvalue -1 with respect to W_n. This is valid because a homogeneous relation between modular forms gives rise (by taking ratios) to a relation between modular functions. Modular forms which have the same eigenvalue under W_n give rise to modular functions which have eigenvalue $+1$ under W_n, and so these are functions on the curve $X_0(N)/W_n$.

Most of the time, the process of finding quotient curves is relatively simple (one must construct a double cover, usually this may be done by eliminating some of the variables). Sometimes the process involves moving a singular point to the point at infinity, by taking a linear change of variable, in these cases the new variable will be denoted u.

This section contains a brief outline of methods for obtaining all the quotient curves of $X_0(51), X_0(42)$ and $X_0(52)$.

There is a very useful table (Table 5 of [2]) which lists the dimensions of the various eigenspaces (with respect to the W_q where $q|N$) of $S_2(N)$. Suppose $q_1, \ldots, q_t$ are the different primes dividing N and choose a basis $f_1, \ldots, f_g$ of $S_2(N)$ such that the f_i are all eigenforms with respect to all the W_q. To each of these basis elements, f, we may associate a sequence of plus and minus signs, $\epsilon_1, \ldots, \epsilon_t$, so that $f|W_{q_j} = \epsilon_j f$. Table 5 of [2] lists, for each combination of $\epsilon_1, \ldots, \epsilon_t$, the number of forms having that sequence of eigenvalues. For $X_0(51)$ we note that $51 = 3.17$ and that Table 5 of [2] gives the entry 0,3,1,1. This shows that the genus of $X_0(51)$ is 5 and that there are no forms which have eigenvalue $+1$ with respect to both W_3 and W_{17}. There is a 3-dimensional space of forms with eigenvalue $+1$ with respect to W_3 and eigenvalue -1 with respect to W_{17}. There are 1-dimensional spaces of forms with sequence $-1, +1$ and $-1, -1$. We therefore choose a basis v, w, x, y, z for $S_2(51)$, of eigenforms, so that v, w, x are the $+1, -1$ forms, y is the $-1, +1$ form, and z is the $-1, -1$ form. The equations describing the image of the canonical embedding of the genus 5 curve $X_0(51)$ are found to be

$$\begin{gathered} v^2 + w^2 - x^2 - 2wx - 2y^2 = 0 \\ v^2 - w^2 + x^2 - 3vx - wx - y^2 + z^2 = 0 \\ 2w^2 - vw + 5x^2 + 3vx - 2wx - y^2 = 0. \end{gathered} \tag{3.1}$$

From the data of [2] Table 5 it follows that $X_0(51)/W_3$ has genus 3. The modular forms v, w, x will give a canonical mapping of $X_0(51)/W_3$ but all their ratios are invariant by W_{17} and $X_0(51)/\langle W_3, W_{17}\rangle$ has genus 0. Therefore, the canonical image has genus 0 and $X_0(51)/W_3$ is hyperelliptic. We also note that $X_0(51)/W_{17}$ and $X_0(51)/W_{51}$ are elliptic curves.

The first and third equations of (3.1) may be used to eliminate y. We therefore obtain the following conic relating v, w and x.

$$v^2 + 2vw - 3w^2 - 6vx + 2wx - 11x^2 = 0 \tag{3.2}$$

It is also quite easy to find the expressions

$$\begin{aligned} z^2 &= -v^2 - vw + 3w^2 + 6vx - wx + 4x^2 \\ y^2 &= 2w^2 - vw + 3vx - 2wx + 5x^2. \end{aligned} \tag{3.3}$$

Together these are enough to give models for all three quotient curves of $X_0(51)$ (see the tables). These models are preferred as they fit with our programme of canonical embeddings (i.e., using variables which correspond to differentials to give equations).

It is possible to obtain plane models for these curves by using equation (3.2) to reduce from $\mathbb{P}^3$ to $\mathbb{P}^2$. First note that (3.2) may be written as

$$(v + w - 3x)^2 - 4(w - x)^2 - 16x^2 = 0.$$

This gives the expression $16x^2 = (v + 3w - 5x)(v - w - x)$ which has the parametric solution (up to scalar multiples) $v + 3w - 5x = 4s^2, v - w - x = 4t^2$ and $x = st$. Rearranging these gives $w = s^2 - t^2 + st$ and $v = s^2 + 3t^2 + 2st$. We set $t = 1$ (i.e., we divide by the function t) to get affine equations.

Now it is possible to rephrase the equations (3.3) in terms of s. We obtain

$$\begin{aligned} z^2 &= s^4 + 4s^3 - 2s^2 - 3. \\ y^2 &= s^4 + 2s^3 + 3s^2 + 6s + 5 \end{aligned} \tag{3.4}$$

The first of these will give a model for $X_0(51)/W_{51}$ which can be seen to be of conductor 17 (i.e., it is a model for $X_0(17)$). The second equation in (3.4) gives a model for $X_0(51)/W_{17}$.

Finally we obtain a model for $X_0(51)/W_3$ by multiplying these two equations (since yz is a function on $X_0(51)/W_3$) to get

$$(yz)^2 = s^8 + 6s^7 + 9s^6 + 14s^5 + 20s^4 + 2s^3 - 19s^2 - 18s - 15.$$

Now we turn to calculating the quotients of $X_0(42)$. We find that $X_0(42)$ is a non-hyperelliptic curve of genus 5 and that $X_0(42)/W_2$ and $X_0(42)/W_7$ are both non-hyperelliptic genus 3 curves. Thus we may obtain models for their canonical embedding using the algorithm already described. Similarly, by looking at the splitting of the weight 2 forms as given in Table 5 of Antwerp 4 [2], we see that $X_0(42)/W_{14}$ has genus 1 and that $X_0(42)/W_n$ for $n \in \{3, 6, 21, 42\}$ has genus 2. We show how to obtain the quotients $X_0(42)/W_3$ and $X_0(42)/W_{14}$ from the equations for $X_0(42)$. The other cases follow in a similar way.

The equations for $X_0(42)$ are

$$\begin{aligned} vx - yz &= 0 \\ 2v^2 + w^2 - 2y^2 - z^2 &= 0 \\ 3v^2 - 2w^2 - x^2 + y^2 - z^2 &= 0 \end{aligned}$$

where v, w, x, y, z correspond to a basis of eigenforms for the weight 2 cusp forms of level 42. First note that the modular forms v and y are $+$ with respect to W_3 and that w, x, z are $-$. From the first equation we solve $x = yz/v$. The second equation remains unchanged and the third becomes $3v^4 - 2v^2w^2 + v^2y^2 - v^2z^2 - y^2z^2 = 0$. Using the second equation and the "new" third equation we may solve for w^2 and z^2 and we get

$$w^2(3v^2 + y^2) = v^4 + v^2y^2 + 2y^4$$

$$z^2(3v^2 + y^2) = 7v^4 - 3y^2v^2.$$

Now multiply these two equations and, again, use the fact that $yz = vx$, to get

$$(3vwz + wxy)^2 = (7v^2 - 3y^2)(v^4 + v^2y^2 + 2y^4).$$

Note that v, y and $(3vwz + wxy)$ all have eigenvalue $+1$ with respect to W_3, so this is a model for the genus 2 curve $X_0(42)/W_3$.

To give an equation for the genus one curve $X_0(42)/W_{14}$ we cannot use variables which are $+$ with respect to W_{14} as there is only one of them. The form which is fixed by W_{14} corresponds to the variable w. Instead we eliminate w^2 and v to obtain

$$x^4 + y^2(3x^2 - 7z^2) + 3x^2z^2 = 0.$$

This equation may be rearranged into the hyperelliptic form

$$((7z^2 - 3x^2)y)^2 = -3x^6 - 2x^4z^2 + 21x^2z^4 = x^2(x^2 + 3z^2)(7z^2 - 3x^2)$$

Note that the forms x and z both have eigenvalue -1 with respect to W_{14} whilst the form $7yz^2 - 3x^2y = 7vxz - 3x^2y$ has eigenvalue $+1$. The proper interpretation of this equation is to divide by x^6. Thus we have the following affine relation between the functions $X = z/x$ and $Y = (7vz - 3xy)/x^2$ (both of which have eigenvalue $+1$ and so they are both functions on $X_0(42)/W_{14}$).

$$Y^2 = 21X^4 - 2X^2 - 3$$

Finally we discuss the quotients of $X_0(52)$. In this case the canonical embedding gives the following equations for the genus 5 curve $X_0(52)$.

$$\begin{aligned} vx - 4vy + 3wz &= 0 \\ 3v^2 + 9w^2 - x^2 - 8xy - 3z^2 &= 0 \\ 6v^2 + 3x^2 + 4xy - 16y^2 + 3z^2 &= 0 \end{aligned} \tag{3.5}$$

The quotient $X_0(52)/W_{13}$ is a non-hyperelliptic genus 3 curve, so we may use the theory of the canonical embedding to find a projective model for it. The genus 2 quotient curves $X_0(52)/W_2$ and $X_0(52)/W_{52}$ may be found by alternative means.

Consider $X_0(52)/W_2$. Note that the variables v and w have eigenvalue $+1$ with respect to W_2. The first formula in (3.5) is a relation between forms of weight 4 with eigenvalue -1 and thus we cannot apply the techniques used to handle $X_0(42)$ above. Indeed the method to use is to solve for v using the first equation in (3.5), i.e., $v = 3zw/(4y - x)$, and then to solve for w^2 using the second equation, to get the formula

$$(x - 4y)^2(3x^4 - 20x^3y + 18x^2z^2 + 192xy^3 + 36xyz^2 - 256y^4 + 27z^4) = 0.$$

The $(x - 4y)^2$ factor arises from the process of elimination and does not come from the curve. The quartic curve has a singularity at the point $[x{:}y{:}z] = [4{:}1{:}0]$, so set $u = x - 4y$ to obtain the equation listed in the tables.

This game may be played all over again in order to find the quotients $X_0(N)/\langle W_n, W_m\rangle$. This is less illuminating and it usually just reveals well-known elliptic curves (or genus zero curves).

3.5 The Tables

These tables list the results of calculations following the ideas mentioned in the previous sections. We try to be as complete as possible subject to the following two restrictions: first that the method does not work when $X_0(N)$ is hyperelliptic, and second that we are only looking for curves of genus 3,4 or 5. More precisely we list all genus three $X_0^+(p)$ (and most genus 4 and 5 curves $X_0^+(p)$ where $p \leq 300$) and we list all non-hyperelliptic $X_0(N)$ of genus 3,4 or 5 and, for each of these, all their non-trivial quotients by Atkin-Lehner involutions.

The reason for our genus restriction is, on one hand, that the canonical embedding is useless for genus 0,1 and 2, and on the other hand, dealing with curves of large genus results in equations which are not complete intersections and therefore it is less easy to check the results for human error.

We give projective equations for the image of the canonical embedding. The variables v, w, x, y, z will correspond to weight 2 forms. In all cases the *alphabetic* order of these variable names will correspond to the ordering given in Table 5 of volume 4 of the Antwerp proceedings [2]. This ordering associates to each form of level N a sequence of $+$ and $-$ signs which are the eigenvalues of the cusp form with respect to the W_q (where q are the primes dividing N, listed in increasing order). Such sequences are then written in the "binary" ordering $++, +-, -+, --$ etc. When there are newforms and oldforms with the same W_q-eigenvalues then the oldforms will be listed first. Note that, for newforms in classes of dimension larger than 1, the q-expansions used are a basis for the eigenclass given by forms with integral coefficients (thus these will not actually be eigenforms with respect to the Hecke operators T_p).

The variable names in equations for quotient curves will match the variable names used for the original curve, though we sometimes introduce changes of variable in order to describe the model.

This work is in part motivated by the quest for projective models for $X_0(N)$ which have small coefficients. The model we obtain via the canonical embedding using eigenforms already has small coefficients. There are clearly many choices of basis for the space of holomorphic differentials on a curve. Any other choice of basis will be related to our basis of eigenforms by some linear map (i.e., an element of $\mathrm{GL}_g(\mathbb{C})$). Therefore any change of variable in $\mathrm{GL}_g(\mathbb{Q})$ will also yield a model for the canonical curve which is defined over $\mathbb{Q}$. In some instances we have been able to find a suitable change of variable which yields a model with smaller coefficients. The changes of variable are given explicitly (up to multiplication by an appropriate scalar). We do not claim that our models have any minimality properties among all projective models. A canonical model should have variables which correspond to a basis for the space of holomorphic differentials, thus we are restricted to considering only invertible linear changes of variable.

Finally we make some comments about correctness. We have generated relations between cusp forms with q-expansions of sufficient length to ensure that our results are correct. If our arithmetic is correct then it follows that the equations obtained really are canonical models for the curves in question. It is a little awkward to perform an independent check on the arithmetic. However in most cases we may consider the quotients of the curve $X_0(N)$ and see that they cover known elliptic curves (see Cremona [8]) with expected ramification. Some of the prime cases have been computed by others (for example Elkies) and we can check our models against theirs.

We expect a model for $X_0(N)$ to have bad reduction at the primes dividing N. Moreover, it is known that there is some model which has bad reduction at only those primes. In the tables we often get extra bad reduction, most commonly at the prime 2. There are also a few cases where there is unexpected bad reduction modulo 3. This situation is not a significant problem as it does not affect the usefulness of our equations.

Note that we have not seriously attempted to reduce the size of coefficients appearing in models for the quotient curves when they have genus 1 or 2 (e.g., see $X_0^+(67)$). The genus 1 cases are already well-known and understood. For the genus 2 case there are better methods for obtaining nice models of these curves (see Chapter 4 or Murabayashi [28]).

We use the notation $X_0^{++}(pq)$ to represent $X_0(pq)/\langle W_p, W_q\rangle$.

Table 1. Canonical Embeddings

$X_0(34)$	Here $x = f_{17}(\tau) + 2f_{17}(2\tau), y = f_{34}(\tau), z = f_{17}(\tau) - 2f_{17}(2\tau)$. $x^4 + 6x^2y^2 + 8x^2z^2 - 8y^4 - 6y^2z^2 - z^4 = 0$
	Setting $X = x + z; Y = 2y; Z = x - z$ gives $X^4 + X^3Z - 2X^2Z^2 + 3XY^2Z + XZ^3 - Y^4 + Z^4 = 0$
$X_0(34)/W_2$	x has eigenvalue $+1$ with respect to W_2 while y and z have eigenvalue -1. Really we should divide by z to get functions y/z, which is $+$, and x/z which is $-$. $(x^2 + 3y^2 + 4z^2)^2 = 17y^4 + 30z^2y^2 + 17z^4$
$X_0(34)/W_{17}$	$(8y^2 - 3x^2 + 3z^2)^2 = 17x^4 + 46z^2x^2 + z^4$
$X_0(34)/W_{34}$	$(z^2 + 3y^2 - 4x^2)^2 = 17x^4 - 18y^2x^2 + y^4$

$X_0(38)$ [†]	Here $w = f_{19}(\tau) + 2f_{19}(2\tau), x, y =$ newforms A,B from [7], $z = f_{19}(\tau) - 2f_{19}(2\tau)$ $w^2 + 10x^2 + 16wx - 18y^2 - 9z^2 = 0$ $2w^3 - 4w^2x - 5x^3 + 4wx^2 - 7xy^2 + 4xz^2 + 4wy^2 + 2wz^2 = 0$
	Set $W = 4w - 4x; X = -8w + 2x - 6y; Y = 5w - 2x + 6y - 3z; Z = -w - 2x + 3z$ $W^2 - WX + -3WY - 4WZ - X^2 + -2XY - 4XZ - 2YZ = 0$ $W^3 + 3W^2X + 3W^2Y + 5W^2Z + WX^2 + 5WXZ - WY^2 + 3WYZ - X^3$ $-3X^2Y - X^2Z - 2XY^2 + 2Y^2Z + 2YZ^2 = 0$
$X_0(38)/W_2$	$(27xyz)^2 = -32w^6 + 12w^5x - 192w^4x^2 + 208w^3x^3 - 3w^2x^4 + 768wx^5 - 32x^6$
	Set $Y = 27xy/z$ and $w = x - z$, then set $X = 3x - z$ $Y^2z^4 = X^6 + 4X^5z - 6X^4z^2 - 4X^3z^3 - 19X^2z^4 - 4Xz^5 - 12z^6$
$X_0(38)/W_{19}$	$32x^3 + 3xw^2 - 8w^3 - 27xz^2 = 0$
$X_0(38)/W_{38}$	$x^3 - 24x^2w - 4w^3 + 27xy^2 = 0$
$X_0(42)$	Ordering v, w, x, y, z corresponds with the splitting 0,1,1,1,1,0,1,0 of [2] Table 5 $vx - yz = 0$ $2v^2 + w^2 - 2y^2 - z^2 = 0$ $3v^2 - 2w^2 - x^2 + y^2 - z^2 = 0$
$X_0(42)/W_2$	$8v^4 - 27v^2w^2 + 9w^4 - v^2x^2 + 9w^2x^2 + 2x^4 = 0$
	Setting $X = (2x + 2z); Y = (2x + 3y - z); Z = (3y - 2x + z)$ gives $X^4 - X^3Y + X^3Z + 3X^2Y^2 - 5X^2YZ + 3X^2Z^2 - 2XY^3 - 4XY^2Z$ $+4XYZ^2 + 2XZ^3 + 4Y^2Z^2 = 0$
$X_0(42)/W_3$	$(3vwz + wxy)^2 = (7v^2 - 3y^2)(v^4 + v^2y^2 + 2y^4)$
$X_0(42)/W_7$	$7w^4 - 22w^2y^2 + 16y^4 - 8w^2z^2 + 6y^2z^2 + z^4 = 0$
	Setting $X = 2y; Y = 2x; Z = 2(z - x)$ gives $2X^4 - 2X^2Y^2 + 3X^2YZ + 3X^2Z^2 - 3Y^3Z - Y^2Z^2 + 4YZ^3 + 2Z^4 = 0$
$X_0(42)/W_6$	$(3vwy + wxz)^2 = (7v^2 - 3z^2)(8v^4 - 5v^2z^2 + z^4)$
$X_0(42)/W_{14}$	$(7vz - 3xy)^2 = (7z^2 - 3x^2)(3z^2 + x^2)$

[†] Note that this model has bad reduction at the prime 3 despite the fact that 38 is not divisible by 3. This bad reduction persists in the models given for $X_0(38)/W_{19}$ and $X_0(38)/W_{38}$. The first model listed for $X_0(38)/W_2$ has bad reduction at the prime 3, but this is eliminated using the given change of variable. It is known that there is a model for $X_0(N)$ with bad reduction only at the primes dividing N, but, in this case, the best model cannot be obtained from the canonical model.

$X_0(42)/W_{21}$	$(7vwy - 3wxz)^2 = x^6 - 2x^4y^2 - 7x^2y^4 + 24y^6$
$X_0(42)/W_{42}$	$(7vwz - 3wyx)^2 = (x^2 + 3z^2)(2x^4 + x^2z^2 + z^4)$
$X_0(43)$ †	$x^4 + 2x^2y^2 - 3y^4 + 8x^2yz + 8y^3z + 16x^2z^2 + 16y^2z^2 + 48yz^3 + 64z^4 = 0$
	Setting $X = (x - y); Y = 2y; Z = 2z$ gives $X^4 + 2X^3Y + 2X^2Y^2 + 2X^2YZ + 4X^2Z^2 + XY^3 + 2XY^2Z$ $+4XYZ^2 + Y^3Z + 2Y^2Z^2 + 3YZ^3 + 4Z^4 = 0$
$X_0^+(43)$	$\left(\frac{1}{2}(x^2 + y^2 + 4yz + 8z^2)\right)^2 = y^4 + 4z^2y^2 + 4z^3y$
$X_0(44)$	Forms $w = f_{11}(\tau) + 4f_{11}(4\tau), x = f_{11}(2\tau), y = f_{44}(\tau), z = f_{11}(\tau) - 4f_{11}(4\tau)$ $3w^2 + 16wx + 32x^2 - 4y^2 + z^2 = 0$ $w^2x + 8x^3 + 2wy^2 - 4xy^2 - 2wz^2 - 5xz^2 = 0$
	Set $W = w + 4x + z; X = w + 2y; Y = w + 2x - 2y - z; Z = w - 2x + z$ gives $3W^2 + 2WX + 2WY - 2WZ + 4XY + Y^2 - 2YZ + Z^2 = 0$ $W^3 - 2W^2X - 2W^2Y + 5W^2Z - 4WXY - 2WXZ - WY^2 - WZ^2 + 4X^2Y$ $-4X^2Z + 5XY^2 - 2XYZ + 5XZ^2 + Y^3 - 4Y^2Z + YZ^2 = 0$
$X_0(44)/W_2$	$(4xyz + wyz)^2 = (w^3 + 4w^2x - 16x^3)(w^3 + 8w^2 + 24wx^2 + 28x^3)$
$X_0(44)/W_{11}$	$w^3 + 4w^2x - 16x^3 - 4xz^2 - wz^2 = 0$
$X_0(44)/W_{44}$	$w^3 + 24wx^2 + 8w^2x + 28x^3 - 4xy^2 - wy^2 = 0$
$X_0(45)$	$x^4 + 7x^2z^2 - 21x^2y^2 + z^4 + 3y^2z^2 + 9y^4 = 0$
	Setting $X = (x + 2z + 3y); Y = (x - 6y - z); Z = (x - z)$ gives $X^4 + 2X^3Y + X^2Y^2 + X^2YZ - X^2Z^2 - XY^2Z + 3XYZ^2 - 2XZ^3$ $-Y^3Z + Y^2Z^2 + YZ^3 + 4Z^4 = 0$
$X_0(45)/W_3$	$\left(\frac{1}{3}(2x^2 - 21y^2 + 7z^2)\right)^2 = 45y^4 - 34z^2y^2 + 5z^4$
$X_0(45)/W_5$	$(6y^2 + z^2 - 7x^2)^2 = 45x^4 - 42z^2x^2 - 3z^4$
$X_0(45)/W_{45}$	$\left(\frac{1}{3}(2z^2 + 3y^2 + 7x^2)\right)^2 = 5x^4 + 14y^2x^2 - 3y^4$

†The forms used to derive this model are all normalised (i.e., they have minimal integral q-expansions) and yet the variable z here is not normalised, in the sense that one may absorb a factor of 2 into z throughout.

$X_0(51)$	$v^2+w^2-x^2-2wx-2y^2=0$ $v^2-w^2+x^2-3vx-wx-y^2+z^2=0$ $2w^2-vw+5x^2+3vx-2wx-y^2=0$
$X_0(51)/W_{17}$	$z^2=-v^2-vw+3w^2+6vx-wx+4x^2$ $v^2+2vw-3w^2-6vx+2wx-11x^2=0$
$X_0(51)/W_{51}$	$y^2=2w^2-vw+3vx-2wx+5x^2$ $v^2+2vw-3w^2-6vx+2wx-11x^2=0$
$X_0(51)/W_3$	$(yz)^2=(-v^2-vw+3w^2+6vx-wx+4x^2)(2w^2-vw+3vx-2wx+5x^2)$ $v^2+2vw-3w^2-6vx+2wx-11x^2=0$
$X_0(52)$ [†]	$vx-4vy+3wz=0$ $3v^2+9w^2-x^2-8xy-3z^2=0$ $6v^2+3x^2+4xy-16y^2+3z^2=0$
$X_0(52)/W_2$	Set $u=x-4y$ and $Z=3z$ $(24u^2y+24Z^2y+7u^3+5uZ^2)^2=13u^6+10u^4Z^2-3u^2Z^4-4Z^6$
$X_0(52)/W_{13}$	$27v^4+18v^2x^2+3x^4+18v^2xy-2x^3y-144v^2y^2-48x^2y^2+128y^4=0$
	Setting $X=(2y+4z); Y=(3x+y-4z); Z=(3x-y+4z)$ gives $YX^3-ZX^3+2X^2Y^2-2X^2YZ+2X^2Z^2+XY^3+2XY^2Z-2XYZ^2$ $-XZ^3+Y^3Z+2Y^2Z^2+YZ^3=0$
$X_0(52)/W_{52}$	Putting $u=x-4y$ and $W=3w$ gives $(24yW^2+5W^2u-u^3)^2=u^6-2u^4W^2+9u^2W^4+8W^6$
$X_0(53)$	$x^2-w^2+2xy+2xz-11y^2-10zy-7z^2=0$ $x^2z+xy^2+xyz+5xz^2+2y^2z+yz^2+6z^3=0$
	Setting $W=2y+2z; X=-2z; Y=w+x-y=z; Z=w-x+y+z$ gives $2W^2+2WX-WY+WZ+2X^2+XZ+YZ=0$ $W^3-W^2X+W^2Y-W^2Z+WX^2-WXY+WXZ-3X^3+3X^2Y$ $-3X^2Z-XY^2+2XYZ-XZ^2=0$
$X_0^+(53)$	w is $+$ and x,y,z are $-$. The second equation, of the model obtained using eigenforms, gives a model for $X_0^+(53)$. $x^2z+xy^2+xyz+5xz^2+2y^2z+yz^2+6z^3=0$

[†] Here the variable y is not "normalised". One may absorb a factor of 4 throughout.

$X_0(54)$	$w^2+2x^2-2y^2-z^2=0$ $w^3+3wz^2-x^3-3xy^2=0$
$X_0(54)/W_2$	$(6wyz+3xyz)^2=-(2w^3-3w^2x-8x^3)(4w^3+6wx^2-x^3)$
$X_0(54)/W_3$	$2w^3-3w^2x-8x^3+6wz^2+3xz^2=0$
$X_0(54)/W_{54}$	$4w^3+6wx^2-x^3-3xy^2-6y^2w=0$
$X_0(55)$	$2v^2+4vx-3vw-6w^2-wx+x^2+7y^2=0$ $3v^2+4vw-8vx-4wx-16x^2-7z^2=0$ $v^2+vw+8vx+5w^2-41wx+x^2-7z^2=0$
$X_0(55)/W_{11}$	$7z^2=3v^2+4vw-8vx-4wx-16x^2$ $2v^2+3vw-5w^2-16vx+37wx-17x^2=0$
$X_0(55)/W_{55}$	$7y^2=-2v^2+3vw+6w^2-4vx+wx-x^2$ $2v^2+3vw-5w^2-16vx+37wx-17x^2=0$
$X_0(55)/W_5$	$(7yz)^2=(3v^2+4vw-8vx-4wx-16x^2)(-2v^2+3vw+6w^2-4vx+wx-x^2)$ $2v^2+3vw-5w^2-16vx+37wx-17x^2=0$
$X_0(56)$	$w^2-2wx-x^2+2y^2-z^2=0$ $3w^2+2wx-y^2+z^2=0$ $v^2+4vw-w^2+2x^2-2wx-3y^2=0$
$X_0(56)/W_7$	$2z^2=v^2+4vw-3w^2-6wx+x^2$ $v^2+4vw+11w^2-2wx-x^2=0$
$X_0(56)/W_{56}$	$y^2=x^2-4w^2$ $v^2+4vw+11w^2-2wx-x^2=0$
$X_0(56)/W_2$	$(2yz)^2=2(x^2-4w^2)(v^2+4vw-3w^2-6wx+x^2)$ $v^2+4vw+11w^2-2wx-x^2=0$
$X_0(57)$	$3wz-4vx+vy=0$ $-5w^2-z^2+8xy+y^2-3v^2=0$ $3w^2-3z^2-4x^2+8xy-4y^2=0$
$X_0(57)/W_3$	Put $u=y-4x$ and $Z=3z$ $(6u^2x+18Z^2x+6u^3+6uZ^2)^2=19u^6+7u^4Z^2-7u^2Z^4-3Z^6$

$X_0(57)/W_{19}$	$80x^4+64x^3y-816x^2y^2-176xy^3+119y^4$ $+432v^2x^2+432v^2xy-54v^2y^2-81v^4=0$
	Setting $X=(2x+y-3v);Y=-(4x+2y);Z=(2y-2x)$ gives $X^4+2X^3Y-X^2Y^2-2X^2YZ+2X^2Z^2-2XY^3-2XY^2Z$ $+2XYZ^2-2Y^3Z-3Y^2Z^2+6YZ^3=0$
$X_0(57)/W_{57}$	Put $u=y-4x$ and $W=3w$ $(18W^2x+30u^2x+6uW^2+6u^3)^2=u^6+u^4W^2+11u^2W^4+3W^6$
$X_0(61)$	$w^2-x^2+2xy-6xz+3y^2+6zy-5z^2=0$ $x^2z+xy^2+xyz+5xz^2+4y^2z+5yz^2+6z^3=0$
$X_0^+(61)$	w is $+$ and all the other forms are $-$ with respect to W_{61}. Therefore the second of the two equations is a model for $X_0^+(61)$.
$X_0(63)$	$w^2+3x^2-yz=0$ $v^2-w^2+2wx+3x^2=0$ $2v^2+12wx+y^2-3z^2=0$
$X_0(63)/W_3$	$v^2-w^2+2wx+3x^2=0$ $(3z^2-v^2-6wx)^2=v^4+3w^4+12v^2wx+54w^2x^2+27x^4$
$X_0(63)/W_7$	$7v^4+v^2y^2+y^4-15y^2z^2-3v^2z^2+9z^4=0$
$X_0(63)/\langle W_7,W_9\rangle$	$\frac{1}{4}(3z^2-w^2-4wx+3x^2)^2=w^4+2w^3x+7w^2x^2-6wx^3+9x^4$
$X_0(64)$	$x^4+6x^2y^2+y^4-8z^4=0$
$X_0(64)/W_2$	$\frac{1}{4}(x^2+3y^2)^2=2y^4+2z^4$
$X_0(65)$	$v^2-y^2+2x^2+2z^2=0$ $v^2-2y^2+z^2+w^2-2wx=0$ $y^2+2yz+2z^2-w^2-x^2=0$
$X_0(65)/W_5$	$13v^4-18v^2w^2+5w^4+40v^2wx-40w^3x+80v^2x^2-48w^2x^2+96wx^3+112x^4=0$
	Setting $X=2w+2x;Y=v-w-2x;Z=v+w+2x$ gives $8X^4+10X^3Y-10X^3Z-3X^2Y^2-12X^2YZ-3X^2Z^2-2XY^3-2XY^2Z$ $+2XYZ^2+2XZ^3X+3Y^4+7Y^2Z^2+3Z^4=0$

$X_0(65)/W_{13}$	$5v^4 + 2v^2y^2 - 7y^4 + 8v^2yz + 16y^3z + 34v^2z^2 + 46y^2z^2$ $+128yz^3 + 137z^4 = 0$
	Setting $X = x + y + x; Y = y + z - x; Z = 2z$ gives $3X^3Y - 8X^2YZ + 9XYZ^2 - 7YZ^3 - 3X^3Z + X^2Z^2 - 7XZ^3 - 2Z^4$ $3XY^3 - 3Y^3Z + X^2Y^2 - 8XY^2Z + Y^2Z^2 = 0$
$X_0(65)/W_{65}$	$(2wz - 2xz - 2xy)^2 = 13x^4 - 2x^2z^2 + 5z^4$
$X_0(67)$	$5vz - 2wx - 3wy + wz = 0$ $15v^2 - 5wv + 5w^2 + 8x^2 - 12xy - 14xz - 11y^2 - 3yz + 15z^2 = 0$ $10v^2 + 5wv - 5w^2 + 4x^2 - 12xy + 2xz - 2y^2 - 35yz - 12z^2 = 0$
$X_0^+(67)$	Put $u = 2x/3 + y$ and $Z = 5z; U = z - 3u$ $\left(\frac{1}{3}\left((10U^2 + 20UZ + 20Z^2)x + 5U^3 + 9U^2Z + 2UZ^2 + Z^3\right)\right)^2$ $= U^6 + 2U^5Z + U^4Z^2 - 2U^3Z^3 + 2U^2Z^4 - 4UZ^5 + Z^6$
$X_0(72)$	$vy - wz = 0$ $v^2 - 2x^2 + y^2 = 0$ $v^2 - 3w^2 + y^2 + z^2 = 0$
$X_0(72)/W_2$	$(2vxz + 2wxy)^2 = 2(v^4 + 3w^4)(3w^2 - v^2)$
$X_0(72)/W_3$	$v^2 - 2x^2 + y^2 = 0$ $(6w^2 - 2x^2)^2 = v^4 + 14v^2y^2 + y^4$
$X_0(72)/W_{72}$	$(6vwx - 2xyz)^2 = 2(v^2 + z^2)(3v^4 + z^4)$
$X_0(73)$	$3vz + 2wx + wy - 5wz = 0$ $3v^2 + 6vw - 3w^2 + 4x^2 + 8xz - 7y^2 - 4yz + 6z^2 = 0$ $3v^2 - 3vw + 6w^2 - 4x^2 - 8xy + 6xz + 9y^2 + 13yz + 16z^2 = 0$
$X_0^+(73)$	Put $u = 2x + y$ $(6u^2x - 78uzx + 240z^2x - 3u^3 + 36u^2z - 99uz^2 - 57z^3)^2$ $= u^6 - 24u^5z + 234u^4z^2 - 1018u^3z^3 + 957u^2z^4 + 5058uz^5 - 8111z^6$
	Set $X = u - 5z; Z = 3z$ $\left((6XZ - 6X^2)x + 3X^3 + 3X^2Z - 4XZ^2 + Z^3\right)^2$ $= X^6 + 2X^5Z + X^4Z^2 + 6X^3Z^3 + 2X^2Z^4 - 4XZ^5 + Z^6$

$X_0(75)$	$3v^2+w^2-2wx+x^2-2yz-z^2=0$ $3w^2-3x^2+5y^2-4yz-z^2=0$ $w^2+4wx+4x^2-5y^2-8yz+4z^2=0$
$X_0(75)/W_3$	$37v^4+126v^2w^2-243w^4-76v^3x+396vw^2x-120v^2x^2$ $-360w^2x^2+320vx^3-80x^4=0$
	Setting $X=v-3w+2x; Y=2v-2w; Z=-6x$ gives $3x^4+6x^3y+6x^3z+x^2y^2+3x^2yz+4x^2z^2-2xy^3-5xy^2z$ $-2xyz^2+xz^3-3y^4-4y^3z-2y^2z^2-yz^3=0$
$X_0(75)/W_5$	$9v^4+30v^2y^2+108v^2yz-48v^2z^2+25y^4-60y^3z-80y^2z^2+16z^4=0$
	Setting $X=2z-2y; Y=y+2z-3v$ and $Z=-2y-4z$ gives $4X^4+9X^3Z-4X^2Y^2-4X^2YZ+3X^2Z^2+9XY^2Z+9XYZ^2$ $+Y^4+2Y^3Z+4Y^2Z^2+3YZ^3=0$
$X_0(75)/W_{75}$	Set $u=x+2w$ and $Z=3z$ $(36wz-24uz)^2=5u^4+14u^2Z^2-3Z^4$
$X_0(81)$	$w^2-x^2+12z^2=0$ $w^2x+3xz^2+9z^3-y^3=0$
$X_0(81)/W_3$	$x^3-9xz^2+9z^3-y^3=0$
$X_0^+(97)$	$-x^2y^2+xy^3-x^3z+x^2yz-xy^2z+2y^3z-3x^2z^2+2xyz^2$ $+y^2z^2-2xz^3+yz^3=0$
$X_0^+(109)$	$-xy^3+x^3z+x^2yz-xy^2z-2y^3z+4x^2z^2+2xyz^2-4y^2z^2+4xz^3-yz^3+z^4=0$
$X_0^+(113)$	$x^2y^2+xy^3+x^3z+3x^2yz+5xy^2z+2y^3z+4x^2z^2$ $+8xyz^2+7y^2z^2+6xz^3+7yz^3+3z^4=0$
	Setting $X=x+z; Y=z; Z=-y-z$ gives $X^3Y+X^3Z-X^2Y^2+X^2YZ+XY^3-XY^2Z-XZ^3+Y^2Z^2-YZ^3=0$
$X_0^+(127)$	$x^2y^2+xy^3+x^3z+3x^2yz+5xy^2z+4y^3z+6x^2z^2$ $+13xyz^2+11y^2z^2+13xz^3+17yz^3+10z^4=0$
	Setting $X=-z-y; Y=-y; Z=-x-y-2z$ gives $X^4-X^3Y-X^3Z+2X^2Y^2+X^2YZ-X^2Z^2-2XY^3+2XY^2Z$ $+XZ^3-Y^3Z-YZ^3=0$

$X_0^+(137)$	$xy + wy + 2y^2 + 2wz + xz + 6yz + 3z^2 = 0$ $x^3 + wx^2 + 6x^2z - 2xy^2 - 5xyz + xzw + 13xz^2 + 2y^3 + 3wy^2$ $+w^2y + 3wyz - 6yz^2 + zw^2 - 4z^2w + 14z^3 = 0$
	Set $W = w - x + y - z; X = x + z; Y = w - x - 2z; Z = z$ $2W^2 + 2WX - 3WY + 2WZ - 2XY + XZ + Y^2 - YZ = 0$ $2W^3 + W^2X - 3W^2Y - W^2Z + WX^2 - 2WXZ + WY^2 + WYZ - WZ^2$ $+2X^3 + 3X^2Z - XY^2 + XYZ + 2XZ^2 - 3YZ^2 + 3Z^3 = 0$
$X_0^+(139)$	$x^2y^2 + xy^3 - y^4 + x^3z + 3x^2yz + 3xy^2z - 2y^3z + 5x^2z^2$ $+8xyz^2 - 2y^2z^2 + 8xz^3 + 3yz^3 + 4z^4 = 0$
	Setting $X = y + z; Y = -x - y - 2z; Z = -y$ gives $X^3Y + X^3Z - X^2Y^2 - 2X^2ZY + 2XY^2Z - XZ^3 + ZY^3 + 2Z^2Y^2 + 2Z^3Y = 0$
$X_0^+(149)$	$x^2y^2 + xy^3 + y^4 + x^3z + 2x^2yz + 6xy^2z + 4y^3z + 4x^2z^2 + 7xyz^2$ $+7y^2z^2 + 4xz^3 + 5yz^3 + z^4 = 0$
	Setting $X = z; Y = -x - 2z; Z = -y$ gives $X^4 + X^3Z - 2X^2Y^2 - X^2YZ - X^2Z^2 - XY^3 - 2XY^2Z - 2XYZ^2$ $-2XZ^3 + Y^2Z^2 + YZ^3 + Z^4 = 0$
$X_0^+(151)$	$xy^3 + y^4 - x^3z - x^2yz + 5xy^2z + 8y^3z - 3x^2z^2 + 6xyz^2 + 20y^2z^2 + 17yz^3 + 4z^4 = 0$
	Setting $X = y + z; Y = x + 2y + 2z; Z = y$ gives $X^3Z + 3X^2Y^2 - 2X^2YZ - X^2Z^2 - XY^3 - XY^2Z + XYZ^2$ $-XZ^3 + ZY^3 - 2Z^2Y^2 + 2Z^3Y = 0$
$X_0^+(157)$	$-vx + 2wx - 5vy - 8vz + 5wz - 2xz + 5yz + z^2 = 0$ $w^2 + wx + 4wy - xy + y^2 + vz + 4wz - 2xz - 9yz - 12z^2 = 0$ $w^2 + 3wx + x^2 - vy + 9wy + 2xy + 6y^2 + vz + 12wz + 5xz + 3yz - z^2 = 0$

$X_0(169)/W_{13}$	$x^2y^2 + xy^3 + x^3z + 3x^2yz + 5xy^2z + 2y^3z + 6x^2z^2$ $+10xyz^2 + 4y^2z^2 + 10xz^3 + 5yz^3 + 4z^4 = 0$
$X_0^+(173)$	$x^2 + wy + xy - wz + 4xz - 3yz = 0$ $xy^2 + y^3 + w^2z + wxz + 2x^2z + 5wyz + 6xyz + 9y^2z + 3wz^2$ $+11xz^2 + 14yz^2 + 12z^3 = 0$
	Setting $W = x + y + 2z; X = -y - z; Y = w + y; Z = z$ gives $W^2 + WX + WZ - X^2 - XY + 2XZ - 2YZ - Z^2 = 0$ $2W^2Z + WX^2 + WXZ + WYZ + 3WZ^2 - 2XYZ + 2XZ^2 + Y^2Z - YZ^2 = 0$
$X_0^{++}(178)$ †	$x^4 - 2x^2y^2 + y^4 - 12x^2yz - 4y^3z - 4x^2z^2 + 20y^2z^2 + 32yz^3 = 0$
$X_0^+(179)$	$xy^3 + x^3z + 2x^2yz + 2xy^2z + 2y^3z + 4x^2z^2 + 7xyz^2 + 5y^2z^2$ $+6xz^3 + 7yz^3 + 3z^4 = 0$
	Put $X = -x - z; Y = -y - z; Z = z$ $x^3z + x^2z^2 + 2x^2yz - xz^3 - 2xyz^2 - xy^2z - xy^3x - yz^3 + y^3z = 0$
$X_0^+(181)$ ‡	$xy + y^2 - wz + xz + 3yz + 4z^2 = 0$ $vw + 3wx + 3vy + wy + 4xy - 2y^2 + vz + 16wz - 2xz + 18yz - 10z^2 = 0$ $vx + 3x^2 + vy - 6xy - 9y^2 + 5vz + 10wz + 16xz - 14yz + 14z^2 = 0$ $-v^2w - vw^2 + w^3 - 3vwx - w^2x + vx^2 + 2x^3 + v^2y - vwy + 5w^2y - 3vxy$ $+2wxy - 4x^2y - vy^2 + 3wy^2 - 10y^3 + 3v^2z + vwz - 2w^2z + 7vxz + 15wxz$ $+9x^2z - 2vyz + wyz + 3xyz + 8y^2z - vz^2 - 4wz^2 + xz^2 - 4yz^2 + 2z^3 = 0$ $v^2w + vw^2 - w^3 + v^2x + 3vwx + w^2x + 3vx^2 + x^3 + 2v^2y + 3vwy - 7w^2y + 8wxy$ $-6vy^2 - 7wy^2 + xy^2 - 2y^3 + 4v^2z + 14vwz - 8w^2z + 14vxz + 5x^2z - 5vyz$ $+4wyz - xyz + 4y^2z + 6vz^2 - 6wz^2 + 3xz^2 = 0$
$X_0^+(199)$	$2wy - x^2 + 3xy - 6xz - 5wz + 3yz - 6z^2 = 0$ $-wx^2 + 3w^2y + 3wxy + 3wy^2 + xy^2 + y^3 - 7w^2z - 5wxz - 8wyz - 2xyz - 3y^2z$ $+6wz^2 + 4yz^2 - 3z^3 = 0$

† This equation is not normalised. One may absorb a factor of 2 into z.

‡ This is an example of a canonical genus 5 curve which is not a complete intersection. By Hartshorne [20] exercise IV.5.5, one sees that $X_0^+(181)$ has a linear system of dimension 1 and degree 3. This curve may therefore be written as a plane quintic with one node, however it is not possible to obtain this model from the canonical embedding.

$X_0^{++}(217)$	$3x^2y^2 + 3xy^3 + 2y^4 - 3x^3z - 6x^2yz - 4xy^2z + 2y^3z - 13x^2z^2$ $+xyz^2 - 26y^2z^2 - 26xz^3 + 43yz^3 - 34z^4 = 0$
	Setting $X = z; Y = z - y; Z = -x - 2z$ gives $X^4 + X^3Y + 2X^3Z + 6X^2Y^2 - 2X^2YZ - 2X^2Z^2 + 4XY^3 - 7XY^2Z$ $-3XZ^3 - 2Y^4 - 3Y^3Z - 3Y^2Z^2 = 0$
$X_0^+(227)$ †	$-3vw - 2w^2 + vx - wx - x^2 - 3vy - 11wy - xy - 2y^2$ $+5vz + 7wz + 7xz + 7yz - 3z^2 = 0$ $-vw - 3w^2 - vx - 2wx + x^2 + vy - 4xy + 3y^2 + vz - 2wz + 8xz - 13yz + 12z^2 = 0$ $2v^2 + 3vw + 5w^2 + 2vx + wx - 4x^2 + 2vy - 7wy + 2xy + 2y^2 - 2vz$ $+12wz - 10xz - 7yz + 3z^2 = 0$ $2w^3 + 2v^2x - vwx - 3wx^2 - 2x^3 - 2v^2y - 4vwy - w^2y - vxy - 6wxy - x^2y$ $-vy^2 - y^3 + 3v^2z - vwz - 2w^2z + 2vxz - 4wxz + 3vyz - 6wyz - 3xyz$ $+2y^2z - 3vz^2 - wz^2 + 5xz^2 - yz^2 - 2z^3 = 0$ $v^3 + v^2w + 5vw^2 + 2w^3 - vwx - w^2x - 2vx^2 - wx^2 + x^3 - 3vwy - w^2y$ $+vxy + wxy - 2x^2y - vy^2 - 3wy^2 - xy^2 - y^3 - v^2z + 3vwz + 8w^2z - vxz$ $-4wxz + 5x^2z + vyz + 6xyz + 2y^2z + 3wz^2 - 3xz^2 + 4yz^2 - 3z^3 = 0$
$X_0^+(239)$	$x^2y^2 - xy^3 - y^4 + x^3z - 2x^2yz + 4xy^2z + 2y^3z$ $+5x^2z^2 - 5xyz^2 + 8xz^3 - yz^3 + 4z^4 = 0$
	Setting $X = -x - z; Y = z; Z = y - z$ gives $-X^3Y + X^2Y^2 + X^2Z^2 - XY^3 + XYZ^2 + XZ^3 + Y^4 + ZY^3 - Z^3Y - Z^4 = 0$
$X_0^+(251)$	$wx - wy + xy - 2y^2 + 2wz + xz + 4yz + z^2 = 0$ $w^2x - w^2y + x^2y - wy^2 - 2xy^2 + 2y^3 + w^2z - wxz - 3x^2z + 2wyz$ $+7xyz - 3y^2z - 21xz^2 + 10yz^2 - 28z^3 = 0$
	Set $W = x - y + 2z; X = -w - y + 2z; Y = -z; Z = x + 2z$ $W^2 + WX - 2WZ + Y^2 + 3YZ + Z^2 = 0$ $2W^3 + W^2X - 5W^2Z - WX^2 + 2WY^2 + 5WZ^2 - X^2Y - 2XY^2 - 3XYZ - XZ^2$ $+2Y^3 + 5Y^2Z - 3YZ^2 - 2Z^3 = 0$

† This is another example of a genus 5 curve whose canonical model is not a complete intersection. See the footnote to $X_0^+(181)$ for further discussion.

3.6 Some Tables for Genus larger than 5

We have also performed a few calculations of the canonical map when the genus is 6 or 7. Note that, for genus ≥ 6, the image curve is never a complete intersection. Therefore it is difficult to verify that the equations are correct (for instance, because it is hard to know if one has already gathered all the equations needed). We already know when $X_0(N)$ is hyperelliptic but we do not know in advance when $X_0^+(p)$ is hyperelliptic. If a curve C of genus g is hyperelliptic then we expect the image, of the canonical map in $\mathbb{P}^{g-1}$, to be given by $(g-1)(g-2)/2$ equations, so we may detect hyperelliptic curves in this way. The tables do give some experimental support for our claims that the models have small coefficients, although we have not been able to perform the usual process of choosing a linear change of variable to minimise the coefficients.

Table 2. Higher Genus Curves

$X_0(58)$	$-ux + vy + wy + vz = 0$
$g = 6$	$-uv + xy + 2xz = 0$
	$v^2 - vw - w^2 - x^2 + yz + z^2 = 0$
	$u^2 + v^2 + 3vw + 4w^2 - 2x^2 + yz = 0$
	$-u^2 - 2v^2 + 3vw - 4w^2 + 2x^2 + y^2 + yz = 0$
	$-vx + 6wx + uy = 0$
$X_0(79)$	$-wx + 2vy + wy + 2y^2 + 2vz - 2wz + xz + yz + z^2 = 0$
$g = 6$	$wx - vy + 2xy + y^2 - vz + 3wz + 8yz + z^2 = 0$
	$-vx - x^2 - vy + wy + 4y^2 - 4vz - 5xz + 2yz - 5z^2 = 0$
	$-w^2 - 2vx - 2wx - x^2 + vy - 3wy - xy - 6vz - 5wz - 3xz + yz = 0$
	$-vx - 2vy + wy - xy + 4y^2 - 5vz + 2xz - yz + 8z^2 = 0$
	$u^2 - v^2 + 2vw + 2w^2 - 2vx + 2wx - x^2 + 9vy + 6wy + 4xy - 4y^2$
	$-4vz + 4wz - 5xz - yz = 0$

$X_0(83)$ $g = 7$	$3uv + 3uw + 2vw + 2w^2 + 4ux + wx - x^2 + 6uy + 9vy + 11wy + 2xy$ $-2y^2 - 2uz - 4vz - 6wz - 7xz + 6z^2 = 0$ $uv + uw + 2ux + vx + 2wx + x^2 + 2uy - 3vy - wy + 4y^2 + 2uz + 8vz + 15wz$ $+8xz + 23yz + 4z^2 = 0$ There are 8 further equations. The largest coefficient occurring is 23.
$X_0(121)$ $g = 6$	$uw - 2vw + 2ux - 6vx + 2uy + 2vy + uz = 0$ $uw + vw + 2ux - 2vx + 2uy - 10vy - 5uz + 11vz = 0$ $-6u^2 + 6uv - 3v^2 - w^2 + 6wx - x^2 - 8wy + 10xy - 9y^2 - 4wz + 10xz = 0$ $6u^2 + 12uv + 12v^2 - 17wx - 2x^2 - 5wy + 4xy + 14y^2 - 6wz - 7xz - 11yz = 0$ $-9v^2 - 8w^2 + wx + 9x^2 + 7wy - 10xy + y^2 - 7wz + 27xz - 11yz = 0$ $-6u^2 - 12uv - 12v^2 - 3w^2 + 7wx - 6x^2 + 11wy + 12xy + 10y^2 + 4wz$ $+17xz - 11yz - 11z^2 = 0$
$X_0^+(163)$ $g = 6$	$u^2 - uv + uw + 4vw - 2w^2 - ux + 3vx + wx + 3uy + 14vy - 6wy$ $+2xy + 5y^2 + uz + 22vz - 4wz - 2xz + 3yz - 14z^2 = 0$ $u^2 - v^2 + 3uw + 4vw + 2w^2 + 2ux - vx + 5wx + 17uy + 5vy + 23wy - 9xy$ $+33y^2 + 23uz + 5vz + 29wz - 9yz - 6z^2 = 0$ There are 4 further equations. The largest coefficient is 33.

3.7 Coefficient Size of Equations for $X_0(N)$

Now that we have accumulated a large number of examples, we may consider the size of coefficients arising in models for $X_0(N)$. In a later chapter we will discuss heights of projective varieties and discuss coefficient size further.

First let us consider models for the whole curve $X_0(N)$. We have computed equations for the image of the canonical embedding (using eigenforms) for all non-hyperelliptic curves $X_0(N)$ which have genus $3 \leq g \leq 5$. The "worst case" examples are $X_0(43)$, which has a coefficient 64 (though we may simply absorb a factor of 2 into z making the coefficients much smaller), $X_0(44)$, $X_0(55)$ and $X_0(67)$. So in every case we have coefficients of size less than N.

We have also (for most of the genus 3 and 4 cases) managed to reduce coefficient size using a suitable linear change of variable. I make the assumption that, for the higher genus curves, it would be possible to reduce the coefficient size in the models to a similar extent. When the genus is larger than 4 it is too difficult to find such changes of variable. The "worst case" examples here are $X_0(38)$ (largest coefficient 5) and $X_0(57)$ (largest coefficient 8). Certainly we appear to be able to find a model with coefficients of size $\leq 2log(N)$ (this logarithm is to base e).

Now let us consider the curves $X_0^+(p)$ when they are not hyperelliptic. In our examples we can find models for the canonical embedding (using eigenforms) of $X_0^+(p)$ (here we only consider genus at least 3) with coefficients of size $O(p)$. The worst examples here are $X_0^+(127)$, $X_0^+(151)$ and $X_0^+(251)$. Now consider the results of reducing the coefficients using appropriate linear changes of variable. We see that the coefficients are generally less than $log(p)$. The results obtained seem to suggest that it is always possible to find canonical models of $X_0^+(p)$ with coefficients $\leq log(p)$.

It is important to stress that we have only computed models for curves of genus ≤ 5 (except for the few cases in Table 2) and that we have only had access to q-expansion data for $N < 300$. Therefore our results only represent a small initial segment of all the modular curves $X_0(N)$. The claims made in this section about coefficient size therefore cannot be considered as watertight conjecture.

To emphasise the results obtained in our tables consider the general affine model for $X_0(N)$, which is given by the relation between $j(\tau)$ and $j(N\tau)$. The coefficients which appear in this model really are enormous. The only equation of this form I have ever computed was for $X_0(2)$. The largest coefficient appearing in that degree 3 affine model is 1.57464×10^{14}.

At this stage we have not included the results for genus 1 or genus 2 curves. Some genus 2 curves will be given in the next section. Certainly the elliptic curve case seems to follow the pattern (see Section 6.7). From the point of view of coefficient size, the hyperelliptic curves might be viewed more successfully as intersections in $\mathbb{P}^3$ or $\mathbb{P}^4$. For instance, the quotients of $X_0(N)$ when N is equal to 51,55 or 56 were viewed as varieties in $\mathbb{P}^3(\mathbb{C})$. In these cases, though, the coefficients didn't seem to be any nicer than those of the corresponding plane hyperelliptic models.

Chapter 4

Equations for Hyperelliptic Curves

The main drawback of the canonical embedding is that it cannot be used to obtain equations for hyperelliptic curves. In this chapter we discuss a practical method to obtain equations for hyperelliptic curves which appear as a quotient of a modular curve $X_0(N)$. We first discuss the genus 2 case and then, in Section 4.4, we show that the techniques generalise in a trivial manner to genus $g \geq 3$.

There are various ways to obtain equations for genus 2 curves. Murabayashi [28] has listed all the equations of genus 2 curves which appear as $X_0(p)$ or $X_0^+(p)$ (where p is a prime). I believe that the method used by Murabayashi is essentially the same as ours, except that it is presented, in [28], in a very complicated manner. Also, Murabayashi apparently did not have access to any tables of q-expansion data.

Wang [44] also gives a few equations for genus 2 curves. The paper [44] is concerned with the 2-dimensional abelian variety which is associated to a modular newform having coefficients in a quadratic field. The construction of this abelian variety was given by Shimura. Such abelian varieties will always be isogenous to the Jacobian of a genus 2 curve C, since they are principally polarised and correspond to a 2-dimensional space of cusp forms. In a very few cases Wang gives a model for that curve. The curve C need not be a quotient of the modular curve $X_0(N)$, though the Jacobian of C will be isogenous to a quotient of $J_0(N)$. Our method is therefore quite different from that of Wang, as it is only useful when the curve one is interested in is a quotient of $X_0(N)$ by some Atkin-Lehner involutions.

4.1 A Method for Genus 2 Curves

Let C be a curve of genus 2. Then the space of holomorphic differentials, $\Omega^1(C)$, is a two dimensional vector space over $\mathbb{C}$. Suppose C has the plane hyperelliptic equation

$$C : Y^2 = p_6(X), \tag{4.1}$$

where p_6 is a sextic polynomial. The ramification points of the double cover $C \to \mathbb{P}^1(\mathbb{C})$ are precisely the roots of p_6. Therefore the function X has two distinct order one poles. The following result is well-known, although we provide a proof as it is central to this chapter.

Lemma 9 *The $\mathbb{C}$-vector space of holomorphic differentials $\Omega^1(C)$ has a basis consisting of*

$$\omega_1 = \frac{dX}{Y} \quad \textit{and} \quad \omega_2 = \frac{XdX}{Y}. \tag{4.2}$$

Proof. From equation (4.1) we see that the divisor of poles of Y is 3 times the divisor of poles of X. Thus the meromorphic differentials given in (4.2) are actually holomorphic differentials on C. Furthermore they are linearly independent over $\mathbb{C}$ (as they have different divisors) and thus they form a basis of $\Omega^1(C)$. □

From these differentials it is possible to reconstruct the functions X and Y which generate the function field of the curve C, using the relations

$$X = \frac{\omega_2}{\omega_1} \quad \text{and} \quad Y = \frac{dX}{\omega_1}.$$

Now suppose C is modular. By this we mean that C is isomorphic to some quotient $X_0(N)/W$ (where W is a group generated by Atkin-Lehner involutions). By a suitable linear change of variable we may assume that the cusp ∞ of the modular curve corresponds to one of the order one poles on the model (4.1) of C. Then we may identify, in the usual way, the holomorphic differentials with weight 2 cusp forms. This suggests the following method for constructing equations for such curves C. Suppose we have an explicit basis $\{f, g\}$ for the space of weight 2 cusp forms. Construct functions X and Y by

$$X = \frac{f}{g} \quad \text{and} \quad Y = \frac{dX}{g}.$$

Given these functions (we know their q-expansions explicitly) we may then find a relation between them. For the relation to be in the nice form $Y^2 = p_6(X)$ we will need Y to have a pole of order 3 at the cusp ∞ and we will need X to have an order 1 pole. Thus the choice of basis $\{f, g\}$ needs to be made so that f has an order 1 zero at the cusp infinity and so that g has an order 2 zero.

In practice, using the tables of cusp forms [7], it is very simple to choose a basis $\{f, g\}$ for the space of cusp forms such that f and g have the right zeroes at the cusp ∞. The functions X and Y therefore must span the function field of the curve C and hence they will give a model for the curve.

This seems to be essentially the same method used by Murabayashi [28]. We give an example to illustrate the method.

4.2 Example

The curve $X_0(22)$ has genus 2. We know it must have a plane model defined over $\mathbb{Q}$. The canonical embedding cannot be used to provide this model.

Once again we use the fact that $S_2(22) \cong \Omega^1(X_0(22))$. In this case the weight 2 forms are all old. We take $f(\tau)$ to be the normalised newform of weight 11. A basis for the weight 2 forms of level 22 is thus $\{f(\tau), f(2\tau)\}$. Note that, in some contexts, a more natural basis would be $\{f(\tau) \pm 2f(2\tau)\}$ (as these are both eigenforms with respect to W_2). However, for this application, we want to ensure that X and Y have the right poles at ∞, and so the basis is chosen to satisfy that condition.

Write

$$\begin{aligned} X(\tau) &= f(\tau)/f(2\tau) \\ &= q^{-1} - 2 + q - 2q^2 - 4q^3 - 4q^4 + 5q^5 - 6q^6 + \cdots . \end{aligned} \tag{4.3}$$

This is a ratio of weight 2 forms and so it is a modular function of level 22 (equivalently, a function on the curve C). The derivative of a modular function is a weight two form. Recall that $d/d\tau = d/dq.dq/d\tau = 2\pi i q d/dq$. We tend to ignore the factor of $2\pi i$ here, as we are happy to work up to scalar multiples. Set

$$\begin{aligned} Y(\tau) &= \left(\frac{d}{d\tau}X(\tau)\right)/f(2\tau) \\ &= -q^{-3}-q^{-1}-4+9q-24q^2+44q^3-88q^4+\cdots. \end{aligned} \tag{4.4}$$

Now, X and Y are functions on the curve and we explicitly know their integral q-expansions. Hence we can find (using linear algebra on q-expansions) the following polynomial relation between X and Y.

$$Y^2 = P(X) = X^6 + 12X^5 + 56X^4 + 148X^3 + 224X^2 + 192X + 64. \tag{4.5}$$

Once again we stress that the choice of basis was essentially determined by the condition that X should have an order 1 pole and that Y should have an order 3 pole. Of course we could have taken a basis $\{f(\tau) + \lambda f(2\tau), f(2\tau)\}$ instead, but it is clear that this corresponds to the simple change of variable $X \mapsto X + \lambda$.

The next section contains a table of all the genus 2 modular curves obtained using this method. Many of these curves have already been obtained as quotients of canonical models, although finding the equations using this method usually requires less work.

4.3 Tables of Genus 2 Curves

This section lists the results of our calculations. We demand that the chosen basis $\{f, g\}$ for the weight 2 cusp forms is such that f and g have integral q-expansions of the form $f = q + \cdots$ and $g = q^2 + \cdots$. This makes the choice of g unique. The choice of f is not unique, however the value Y obtained will be independent of the choice of f and the choice of X is well defined up to addition by an integer. We tend to choose X so that the coefficients in the model are minimal.

The following table lists all genus 2 modular curves $X_0(N)$ and probably all genus 2 curves $X_0(N)/W_N$. It also lists many quotients $X_0(N)/W_n$. Many of these equations have been found in the previous chapter or by other authors (e.g., Murabayashi [28]). The table lists the sextic polynomial $p_6(x)$ such that, for the functions X and Y described in Section 4.1, we have $Y^2 = p_6(X)$.

Note that many of these models have bad reduction at the prime 2, despite the fact that they have odd level. This is due to the fact that we have insisted on using the model $y^2 = p_6(x)$ instead of the more general model $y^2 + p_3(x)y = p_6(x)$ (where $p_3(x)$ is a cubic polynomial in x and $p_6(x)$ is a sextic). This extra bad reduction shows that the models do not have minimal discriminant. Nevertheless they are models for the curves in question and they are still of use for studying the arithmetic of the original modular curves.

Table 3. Genus 2 Curves

$X_0(22)$	$x^6 - 4x^4 + 20x^3 - 40x^2 + 48x - 32$ $= (x^3 + 2x^2 - 4x + 8)(x^3 - 2x^2 + 4x - 4)$
$X_0(23)$	$x^6 - 8x^5 + 2x^4 + 2x^3 - 11x^2 + 10x - 7$ $= (x^3 - x + 1)(x^3 - 8x^2 + 3x - 7)$
$X_0(26)$	$x^6 - 8x^5 + 8x^4 - 18x^3 + 8x^2 - 8x + 1$
$X_0(28)$	$x^6 + 10x^4 + 25x^2 + 28$ $= (x^2 + x + 2)(x^2 - x + 2)(x^2 + 7)$
$X_0(29)$	$x^6 - 4x^5 - 12x^4 + 2x^3 + 8x^2 + 8x - 7$
$X_0(31)$	$x^6 - 8x^5 + 6x^4 + 18x^3 - 11x^2 - 14x - 3$ $= (x^3 - 2x^2 - x + 3)(x^3 - 6x^2 - 5x - 1)$
$X_0(33)/W_3$	$x^6 - 4x^5 - 6x^4 - 12x^3 + x^2 + 28x - 8$ $= (x^3 + x^2 + 3x - 1)(x^2 - 4x - 8)(x - 1)$
$X_0(35)/W_7$	$x^6 - 4x^5 + 2x^4 - 32x^3 - 27x^2 - 64x - 76$ $= (x^3 - 5x^2 + 3x - 19)(x^2 + 4)(x + 1)$
$X_0(37)$	$x^6 + 14x^5 + 35x^4 + 48x^3 + 35x^2 + 14x + 1$
$X_0(38)/W_2$	$x^6 - 4x^5 - 6x^4 + 4x^3 - 19x^2 + 4x - 12$ $= (x^3 + x^2 - x + 3)(x^3 - 5x^2 - 4)$
$X_0(39)/W_{13}$	$x^6 - 20x^4 - 6x^3 + 64x^2 - 48x + 9$ $= (x^2 - 5x + 3)(x^2 + 3x - 1)(x + 3)(x - 1)$

$X_0(40)/W_2$	$x^6+4x^5+8x^3-44x^2+48x-16$ $=(x^2+4x-4)(x^4+4x^2-8x+4)$
$X_0(40)/W_5$	$x^6+16x^4+64x^2+64$ $=(x^4+12x^2+16)(x^2+4)$
$X_0(42)/W_3$	$x^6-4x^5-18x^3-4x+1$ $=(x^4+x^3+4x^2+x+1)(x^2-5x+1)$
$X_0(42)/W_6$	$x^6+6x^5+7x^4-14x^3-23x^2+36x-12$
$X_0(42)/W_{21}$	$x^6+2x^5-x^4-6x^3+13x^2-12x+4$ $=(x^4+3x^3+x^2-8x+4)(x^2-x+1)$
$X_0(42)/W_{42}$	$x^6+4x^4-2x^3+4x^2+1$ $=(x^4+x^3+4x^2+x+1)(x^2-x+1)$
$X_0(44)/W_2$	$x^6-4x^4-20x^3-40x^2-48x-32$ $=(x^3+2x^2+4x+4)(x^3-2x^2-4x-8)$
$X_0(46)/W_{46}$	$x^6+4x^5+2x^4-2x^3+x^2-2x+1$
$X_0(48)/W_2$	$x^6+10x^5+27x^4+20x^3+27x^2+10x+1$ $=(x^2+4x+1)(x^2+6x+1)(x^2+1)$
$X_0(48)/W_3$	$x^6+8x^4+32x^2+64$ $=(x^2-2x+4)(x^2+2x+4)(x^2+4)$
$X_0(50)$	$x^6-4x^5-10x^3-4x+1$
$X_0(52)/W_2$	$x^6+8x^5+8x^4+18x^3+8x^2+8x+1$
$X_0(52)/W_{52}$	$x^6+4x^5+8x^4+6x^3+8x^2+4x+1$
$X_0(54)/W_2$	$x^6-6x^4-8x^3-27x^2-12x-20$ $=(x^3+3x^2+3x+5)(x^3-3x^2-4)$
$X_0(57)/W_3$	$x^6+10x^5+15x^4+24x^3+15x^2+10x+1$

$X_0(58)/W_{29}$	$x^6+4x^5+16x^4+22x^3+16x^2+4x+1$
$X_0(62)/W_{62}$	$x^6+4x^5+6x^4+6x^3+x^2-2x-3$ $=(x^3+4x^2+5x+3)(x^3+x-1)$
$X_0^+(67)$	$x^6+2x^5+x^4-2x^3+2x^2-4x+1$
$X_0(72)/W_2$	$x^6+6x^5+15x^4+28x^3+15x^2+6x+1$ $=(x^4+2x^3+6x^2+2x+1)(x^2+4x+1)$
$X_0^+(73)$	$x^6+2x^5+x^4+6x^3+2x^2-4x+1$
$X_0(74)/W_{74}$	$x^6-2x^5-x^4-x^2-2x+1$
$X_0(85)/\langle W_5, W_{17}\rangle$	$x^6+2x^5+7x^4+6x^3+13x^2-8x+4$ $=(x^4+2x^3+3x^2-2x+1)(x^2+4)$
$X_0(87)/W_{29}$	$x^6-2x^4-6x^3-11x^2-6x-3$
$X_0(88)/\langle W_2, W_{11}\rangle$	$x^6-2x^5-x^4-12x^3-x^2-2x+1$ $=(x^3+x^2+3x-1)(x^3-3x^2-x-1)$
$X_0(91)/W_{91}$	$x^6+2x^5-x^4-8x^3-x^2+2x+1$
$X_0(93)/\langle W_3, W_{31}\rangle$	$x^6+6x^5+5x^4-6x^3+2x^2+1$ $=(x^3+5x^2+2x+1)(x^3+x^2-2x+1)$
$X_0(100)/W_2$	$x^6+4x^5+10x^3+4x+1$
$X_0^+(103)$	$x^6+6x^5+5x^4+2x^3+2x^2+1$
$X_0^+(107)$	$x^6+2x^5+5x^4+2x^3-2x^2-4x-3$
$X_0(111)/W_{111}$	$x^6+2x^5-x^4-x^2+2x+1$
$X_0(112)/\langle W_2, W_7\rangle$	$x^6+2x^5+11x^4+4x^3+11x^2+2x+1$ $=(x^4+2x^3+10x^2+2x+1)(x^2+1)$
$X_0(115)/\langle W_5, W_{23}\rangle$	$x^6+6x^5+5x^4+10x^3+2x^2+1$ $=(x^3+5x^2-2x+1)(x^3+x^2+2x+1)$
$X_0(116)/\langle W_2, W_{29}\rangle$	$x^6-4x^5+16x^4-22x^3+16x^2-4x+1$

$X_0(117)/\langle W_3, W_{13}\rangle$	$x^6+4x^4-6x^3+16x^2-12x+9$ $=(x^4+x^3+4x^2-3x+9)(x^2-x+1)$
$X_0(121)/W_{11}$	$x^6+6x^5+11x^4+8x^3+11x^2+6x+1$
$X_0(122)/\langle W_2, W_{61}\rangle$	$x^6+4x^4-6x^3+4x^2+1$
$X_0(125)/W_5$	$x^6+2x^5+5x^4+10x^3+10x^2+8x+1$
$X_0(129)/\langle W_3, W_{43}\rangle$	$x^6+2x^5-9x^4-24x^3-9x^2+2x+1$
$X_0(165)/\langle W_3, W_5, W_{11}\rangle$	$x^6+6x^5+11x^4+14x^3+5x^2-12x$
$X_0^+(167)$	$x^6-4x^5+2x^4-2x^3-3x^2+2x-3$
$X_0(177)/\langle W_3, W_{59}\rangle$	$x^6+2x^4-6x^3+5x^2-6x+1$
$X_0^+(191)$	$x^6+2x^4+2x^3+5x^2-6x+1$

There are genus 2 quotients as far as the eye can see, so we stop at this stage.

4.4 Generalisation to Higher Genus

The methods of this section also apply to hyperelliptic curves of genus $g > 2$.

Let C be a hyperelliptic curve of genus $g > 2$. Then C has a plane model of the form

$$y^2 = p_{2g+2}(x)$$

where $p_{2g+2}(x)$ is a polynomial of degree $2g+2$ in x. The function x has degree 2 and, since the point at infinity on the projective line is not a Weierstrass point, it has two poles of order one. The divisor of poles of y is $g+1$ times the divisor of poles of x. Therefore the differentials

$$\frac{dx}{y}, \frac{xdx}{y}, \cdots \frac{x^{g-1}dx}{y}$$

span the space of holomorphic differentials $\Omega^1(C)$.

Now suppose C is "modular" in the sense that $\Omega^1(C) \cong S$ for some $\mathbb{C}$-vector space S of weight 2 cusp forms. One may give S a basis of forms $\{f_1, \cdots, f_g\}$ such that each f_j has q-expansion $f_j = q^j + \cdots$. It then follows that, up to scalar multiples,

$$\frac{dx}{y} = f_g \quad \text{and} \quad \frac{xdx}{y} = f_{g-1}.$$

Therefore, as in Section 4.1, we may set

$$x = f_{g-1}/f_g \quad \text{and} \quad y = dx/f_g$$

and find, by linear algebra on the q-expansions, the degree $2g+2$ polynomial relating x and y.

We give a few examples.

Table 4. Hyperelliptic curves of genus $g \geq 3$

$X_0(30)$	$x^8+6x^7+9x^6+6x^5-4x^4-6x^3+9x^2-6x+1$ $=(x^2+4x-1)(x^2+x-1)(x^4+x^3+2x^2-x+1)$
$X_0(33)$	$x^8+10x^6-8x^5+47x^4-40x^3+82x^2-44x+33$ $=(x^2-x+3)(x^6+x^5+8x^4-3x^3+20x^2-11x+11)$
$X_0(35)$	$x^8-4x^7-6x^6-4x^5-9x^4+4x^3-6x^2+4x+1$ $=(x^2+x-1)(x^6-5x^5-9x^3-5x-1)$
$X_0(39)$	$x^8-6x^7+3x^6+12x^5-23x^4+12x^3+3x^2-6x+1$ $=(x^4-7x^3+11x^2-7x+1)(x^4+x^3-x^2+x+1)$
$X_0(40)$	$x^8+8x^6-2x^4+8x^2+1$
$X_0(41)$	$x^8-4x^7-8x^6+10x^5+20x^4+8x^3-15x^2-20x-8$
$X_0(46)/W_2$	$x^8+2x^7-13x^6-34x^5-9x^4+10x^3-2x^2+12x-7$ $=(x^3+2x^2+x+1)(x^3+2x^2-3x+1)(x^2-2x-7)$
$X_0(46)$	$x^{12}-2x^{11}+5x^{10}+6x^9-26x^8+84x^7-113x^6+134x^5$ $-64x^4+26x^3+12x^2+8x-7$ $=(x^3+x^2-x+7)(x^3-2x^2+3x-1)(x^6-x^5+4x^4-x^3+2x^2+2x+1)$
$X_0(47)$	$x^{10}-6x^9+11x^8-24x^7+19x^6-16x^5-13x^4+30x^3-38x^2+28x-11$ $=(x^5-x^4+x^3+x^2-2x+1)(x^5-5x^4+5x^3-15x^2+6x-11)$
$X_0(48)$	x^8+14x^4+1

$X_0(51)/W_3$	$x^8 - 6x^7 + 9x^6 - 14x^5 + 20x^4 - 2x^3 - 19x^2 + 18x - 15$ $= (x^4 - 2x^3 + 3x^2 - 6x + 5)(x^3 - 5x^2 + 3x - 3)(x + 1)$
$X_0(55)/W_5$	$x^8 - 6x^7 - x^6 + 38x^5 + x^4 - 84x^3 - 28x^2 + 44x$ $= (x^3 - 4x - 4)(x^2 + x - 1)(x^2 - 7x + 11)x$
$X_0(56)/W_2$	$x^8 - 6x^7 + 9x^6 - 16x^5 + 40x^4 - 32x^3 + 36x^2 - 48x + 16$ $= (x^4 - 4x^3 - 8x + 4)(x^2 + x + 2)(x - 2)(x - 1)$
$X_0(59)$	$x^{12} - 8x^{11} + 22x^{10} - 28x^9 + 3x^8 + 40x^7 - 62x^6 + 40x^5$ $-3x^4 - 24x^3 + 20x^2 - 4x - 8$ $= (x^9 - 7x^8 + 16x^7 - 21x^6 + 12x^5 - x^4 - 9x^3 + 6x^2 - 4x - 4)$ $(x^3 - x^2 - x + 2)$
$X_0(62)/W_2$	$x^{10} + 2x^9 - 5x^8 - 22x^7 - 41x^6 - 30x^5 - 2x^4 + 32x^3 + 21x^2 + 4x - 12$ $(x^3 + 4x^2 + 5x + 3)(x^3 + x - 1)(x^4 - 2x^3 - 3x^2 - 4x + 4)$
$X_0(71)$	$x^{14} + 4x^{13} - 2x^{12} - 38x^{11} - 77x^{10} - 26x^9 + 111x^8 + 148x^7$ $+x^6 - 122x^5 - 70x^4 + 30x^3 + 40x^2 + 4x - 11$ $= (x^7 + 4x^6 + 5x^5 + x^4 - 3x^3 - 2x^2 + 1)$ $(x^7 - 7x^5 - 11x^4 + 5x^3 + 18x^2 + 4x - 11)$

4.5 Summary

In Chapters 3 and 4 we have described methods for obtaining projective models for modular curves and we have given large tables describing the results obtained.

We have given equations for every modular curve $X_0(N)$ having genus $2 \leq g \leq 5$. For each of these curves we have, in most cases, given equations for all their (non genus zero) quotients $X_0(N)/W_n$ where $n|N$. We have also listed equations for all curves $X_0^+(p)$ having genus 2 or 3 and, for $p \leq 251$, all curves $X_0^+(p)$ of genus 4 or 5.

The hyperelliptic models given in this chapter do not seem to share the property of having the strikingly small coefficients of the non-hyperelliptic models. For the hyperelliptic case we have sought the obvious hyperelliptic model. This model is probably not, in general, the one which has the smallest coefficients. One alternative model for genus 2 curves is a plane quartic with a singularity, another choice is an intersection of quadrics in $\mathbb{P}^4$. We have not tried to find alternative models, with small coefficients, for these hyperelliptic cases.

Chapter 5

The Hemi-Canonical Map

The standard way to embed abelian varieties (i.e., certain complex tori) in projective space is to use theta functions. This idea was developed by Mumford [27], and it uses a very general notion of theta function.

A variation on this process may be used to map certain modular curves into projective space. This is described in Igusa [21].

A reason why this notion is appealing to us is that theta series may have q-expansions which are very sparse and have small coefficients. It therefore seems plausible that the models obtained from the projective embedding using theta series will have small coefficients.

There is a tradeoff here in that the most useful *theoretical* notion of theta function may not be so useful from a computational perspective. In this chapter we aim to use a very simple notion of theta series, with which it will be easy to compute. Namely, we will use theta series coming from integral binary quadratic forms. The advantage will be that such theta series are quite easy to work with. The disadvantages will be that the mapping to projective space does not, in general, have the nice properties we desire.

In the first section of this chapter we give a summary of the classical theory of using theta functions to give embeddings of modular curves. We then spend several sections introducing the background on the theta series we will be working with. Later we discuss the application of these ideas to the problem of computing equations for modular curves.

5.1 The Classical Approach

This section follows Chapter 5 of Igusa [21]. We are primarily interested in the one variable case, so we specialise the argument if it helps to do so.

First we define two groups. The **symplectic group** $\mathrm{Sp}_{2n}(\mathbb{R})$ is the subset of $\mathrm{GL}_{2n}(\mathbb{R})$ consisting of γ such that $\gamma E \gamma^t = E$ where

$$E = \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix}.$$

Thus, in the $n = 1$ case, $\mathrm{Sp}_2(\mathbb{R}) = \mathrm{SL}_2(\mathbb{R})$. Also, $\mathrm{O}_{2n}(\mathbb{R})$ is defined to be the subset of $\mathrm{Sp}_{2n}(\mathbb{R})$ consisting of γ such that $\gamma^{-1} = \gamma^t$.

The **Siegel upper half space** of degree n is defined to be

$$\mathbb{H}_n = \left\{ Z = X + iY \in M_n(\mathbb{C}) \mid Z^t = Z \text{ and } Y \text{ is positive definite} \right\}.$$

Clearly for $n = 1$ this is just the usual halfplane $\mathcal{H}$.

There is a formulation of the Siegel upper half space in terms of the symplectic group. Namely, there is a homeomorphism (given by "evaluation at i") between $\mathbb{H}_n$ and

$$\mathrm{O}_{2n}(\mathbb{R})\backslash\mathrm{Sp}_{2n}(\mathbb{R}).$$

Igusa fixes an integer $e \equiv 0(\text{mod } 4)$ and considers the group $G_{\mathbb{Z}}(e, 2e)$. This group is, in the one variable case,

$$G_{\mathbb{Z}}(e, 2e) = \Gamma_0(e) \cap \Gamma^0(2) \subseteq \mathrm{SL}_2(\mathbb{Z}), \tag{5.1}$$

where $\Gamma^0(N)$ is the set of matrices in $\mathrm{SL}_2(\mathbb{Z})$ whose top right entry is divisible by N. As $G_{\mathbb{Z}}(e, 2e) \subset \mathrm{Sp}_2(\mathbb{R})$ it acts on $\mathbb{H}_1$. We define the following "modular curve".

$$Y_e = G_{\mathbb{Z}}(e, 2e)\backslash\mathbb{H}_1. \tag{5.2}$$

One may complete this by introducing cusps, just as one does for the modular curves $Y_0(N)$. The curve Y_e is the object for which Igusa gives an embedding into projective space. To show how this is done it is first necessary to introduce theta functions.

The general notion of theta function, as used by Mumford, is the following. Let r be the dimension we are working in (for this application we take $r = 1$). For $m, m' \in \mathbb{R}^r$, $\tau \in \mathbb{H}_r \subset M_r(\mathbb{C})$ and $z \in \mathbb{C}^r$ define

$$\theta_{m,m'}(\tau, z) = \sum_{n \in \mathbb{Z}^r} \exp\left(2\pi i \left(\frac{1}{2}(n+m)\tau(n+m)^t + (n+m)(z+m')^t\right)\right). \tag{5.3}$$

In the theory of embedding of complex tori, it is z which is the "variable" and τ which is fixed (since τ determines the lattice). When we want to obtain embeddings for modular curves the situation is the other way around.

Igusa defines the **theta constants** to be $\theta_{m,0}(\tau, 0)$. These are modular forms of weight $r/2$.

We are now in a position to quote Theorem 4 of [21] (page 189). We specialise the statement to the one-dimensional situation.

Theorem 2 *Let $e \equiv 0$(mod 4). Then the theta constants give a projective embedding of the modular curve Y_e. Namely we have a well-defined injective map*

$$Y_e \longrightarrow \mathbb{P}^{e-1}$$

given by

$$\tau \mapsto [\theta_{x,0}(\tau, 0)]$$

where x runs through $\frac{1}{e}\mathbb{Z}/\mathbb{Z}$.

This theorem gives a very explicit description of a projective embedding for a modular curve closely related to our $Y_0(N)$. If $N \equiv 0(\text{mod } 4)$ then $G_{\mathbb{Z}}(N, 2N) = \Gamma_0(N) \cap \Gamma^0(2)$ and so $Y_0(N)$ is a quotient of the modular curve Y_N of (5.2) under the involution induced from the coset representatives of $G_{\mathbb{Z}}(N, 2N)$ in $\Gamma_0(N)$. When N is not divisible by 4 then $Y_0(N)$ is still a quotient, but the degree of the covering is larger than 2. There are several practical drawbacks with this embedding.

The main drawback is that the image lies in $(N-1)$-dimensional projective space. So to embed a modular curve Y_N would require very large projective space. The coefficients may well be small in this case, but one couldn't claim that the equation is easy to write down.

Thus we are led to consider a different notion of theta series. We will work with the "average" of the canonical map (weight 2 forms) and the method discussed in this section (weight 1/2) and use weight 1 forms. With that goal in mind we introduce theta series of integral binary quadratic forms. The reason for using theta series of integral binary quadratic forms is that they have small coefficients in their q-expansions, and also that there are usually enough of them for the process to work. The coefficients coming from single variable quadratic forms would be much smaller, however there is only one such quadratic form and so, to obtain more than one theta series, one would have to consider complicated characters etc. The Dedekind function $\eta(\tau)$ is a theta series coming from a single variable quadratic form and it has often been used in the past to calculate equations for modular curves. These calculations, though useful, are less "algorithmic" than the method we will introduce. If we were to consider quadratic forms in at least three variables then the number of different theta series would grow but so would the coefficients. It was hoped that binary quadratic forms would be a suitable balance of these two opposing forces.

5.2 Quadratic Forms

In this section we state a few facts from the elementary and well-known theory of quadratic forms. This is mostly taken from [4] and [29].

A quadratic form in m variables is any expression of the form $\sum_{\underline{n}\in\mathbb{Z}^m} a_{\underline{n}} x_1^{n_1}...x_m^{n_m}$ where the $n_j \in \{0,1,2\}$ and $\sum_j n_j = 2$. It is convenient to introduce a matrix notation for quadratic forms.

Definition 8 *A matrix A is said to be* **even** *if it is symmetric, has integral entries and has even entries on the diagonal.*

To any even $n \times n$ matrix A, we associate the n-variable quadratic form

$$Q_A(x_1,\ldots,x_n) = \frac{1}{2}(x_1,\ldots,x_n)A(x_1,\ldots,x_n)^t.$$

Here t denotes the transpose of a vector or matrix.

A quadratic form Q is said to be **positive definite** if it only takes positive values and if the only solution to $Q(\underline{n}) = 0$ is the trivial one $\underline{n} = \underline{0}$. The **determinant**, D, of a quadratic form Q_A is defined to be the determinant of the matrix A. In the two-variable case, a necessary and sufficient condition that the quadratic form be positive definite is that the diagonal entries of the matrix A are positive and that the determinant is positive. In the case where m (the number of variables of the quadratic form) is an even integer $2k$ then we may also define the **discriminant** $\Delta = (-1)^k\det(A)$. Note that $\Delta \equiv 0, 1 (\mathrm{mod}\ 4)$. In particular, 2×2 quadratic forms have negative discriminant and their determinant is $\equiv 0, -1 (\mathrm{mod}\ 4)$. Note that for 3-variable forms the determinant is necessarily even.

Let X be any $m \times m$ matrix with integer coefficients and determinant ±1. The map $\underline{x} \mapsto \underline{x}X$ induces a bijection of $\mathbb{Z}^m$ to itself. Now

$$Q_A(\underline{x}X) = \frac{1}{2}\underline{x}XA(\underline{x}X)^t = \frac{1}{2}\underline{x}(XAX^t)\underline{x}^t = Q_{(XAX^t)}(\underline{x}).$$

So we see that the quadratic form obtained from A represents exactly the same values as that represented by XAX^t. This motivates the following definition.

Definition 9 *Two matrices A and B (or two quadratic forms Q_A and Q_B) are said to be* **weakly equivalent** *if there is an integral matrix X with determinant ±1 such that $XAX^t = B$. The matrices A and B are said to be* **strongly equivalent** *if there is a matrix $X \in SL_2(\mathbb{Z})$ such that $XAX^t = B$.*

Note that weak equivalence is designed for use with theta series. If the word "equivalent" is used without a qualifier then it is weak equivalence which is to be used. If the application of quadratic forms is for class number calculations then one works with strong equivalence.

Definition 10 *The* **level** *of a quadratic form Q_A is the least positive integer N such that NA^{-1} is an even matrix.*

We will see, in Theorem 3, that a quadratic form of level N will give rise to a theta series of level N. Note that we will usually be concerned with matrices for which $N = D$. Also we will usually demand that NA^{-1} be equivalent to A. These two restrictions are not too severe in the two-variable case as we have

$$A = \begin{pmatrix} 2a & b \\ b & 2c \end{pmatrix} \qquad \text{with} \qquad \det(A) = D \qquad \text{and} \qquad DA^{-1} = \begin{pmatrix} 2c & -b \\ -b & 2a \end{pmatrix}.$$

Thus it is clear that N always divides D and that, to have $N < D$, it is necessary that a, b and c all have a non-trivial common factor. When a, b and c have a common factor, the quadratic form is said to be **imprimitive**. If $(a, b, c) = 1$ then the quadratic form is **primitive**. If Q_A is an imprimitive quadratic form then the matrix A would be a multiple of some primitive matrix A' of smaller determinant. This means that the theta series associated to A is an oldform coming up from level $\det(A')$. Finally, note that A is strongly equivalent to DA^{-1} under

$$X = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

5.3 Reduction of Quadratic Forms

Once again we deal only with the 2-variable case and leave the general situation to the literature (see for instance Cassels [4]).

There are many different equivalent matrices A representing any given positive definite binary quadratic form. The process of reduction gives a way to easily list a set of representatives for all the equivalence classes.

Lemma 10 *Any positive definite binary quadratic form is equivalent to a form of the shape $Q(x, y) = ax^2 + bxy + cy^2$ where $|b| \leq a \leq c$ (recall that we only consider positive definite forms, so $a, c > 0$).*

Note. This lemma is stated in the context of strong equivalence. For weak equivalence observe that, by simply taking the mapping $x = -x$ (which has determinant -1 when written in matrix form), the variables may be chosen with $0 \leq b \leq a \leq c$. For either definition of equivalence we say that the form (or matrix representing it) is **reduced** if the coefficients satisfy the bound $|b| \leq a \leq c$. Note that, if $a = c$ or $|b| = a$, then the two choices of b give equivalent quadratic forms, and so one may as well assume that $b \geq 0$.

Proof. We apply 2 basic operations to the quadratic form. They are

(1) $x = -y'; y = x'$ which maps the form to $cx'^2 - bx'y' + ay'^2$.

(2) $x = x' \pm y'; y = y'$ which maps the form to $ax'^2 + (b \pm 2a)x'y' + (a + c \pm b)y'^2$.

Note that $a + c > |b|$ since the form is positive definite. These two operations are applied repeatedly according to the following rules

(i) If $a > c$ then apply the first operation.

(ii) If $|b| > a$ then apply the second operation (choosing the ± sign to be the opposite of the sign of b).

If neither of these conditions is satisfied then the quadratic form is already reduced and the process halts.

This process will always halt because all applications of the second rule will strictly reduce $|b|$. Hence only a finite number of steps can occur. □

Now, given that every equivalence class contains one of these representatives, we may bound the size of the coefficients. Suppose we wish to find a representative for each (weak) equivalence class of binary quadratic forms with determinant D. This amounts to solving $D = 4ac - b^2$ subject to $0 \leq b \leq a \leq c$. The constraint on a, b and c gives $4ac - b^2 \geq 3b^2$ and thus we see that it suffices to look for quadratic forms with

$$0 \leq b \leq \sqrt{D/3}. \tag{5.4}$$

5.4 Class Numbers

Under strong equivalence, the grouping of quadratic forms into classes is exactly as with weak equivalence, except that it distinguishes

$$\begin{pmatrix} 2a & b \\ b & 2c \end{pmatrix} \text{ and } \begin{pmatrix} 2a & -b \\ -b & 2c \end{pmatrix}$$

when $0 < b < a \leq c$.

It is well known that the number of equivalence classes (using strong equivalence) of primitive integral binary quadratic forms of determinant D is the same as the class number h_D of the number field $\mathbb{Q}(\sqrt{-D})$.

Therefore, one may estimate the number of weak equivalence classes of quadratic forms from the class number of $\mathbb{Q}(\sqrt{-D})$. In particular, if D is square-free, then all forms must be primitive, and so the number of weak equivalence classes is between $h_D/2$ and h_D. In any case, we see that the number of quadratic forms of discriminant D grows in a similar way to the class number of $\mathbb{Q}(\sqrt{-D})$.

5.5 Theta Series

Suppose $Q(\underline{n}) = \frac{1}{2}\underline{n}A\underline{n}^t$ is a quadratic form with determinant $D \equiv 0, -1 \pmod 4$ and level N (usually $N = D$). Define the **theta series** $\theta_Q(\tau)$, as a Fourier series in $q = \exp(2\pi i\tau)$, by

$$\theta_Q(\tau) = \sum_{\underline{n}\in\mathbb{Z}^2} \exp(2\pi i\tau Q(\underline{n})) = \sum_{\underline{n}\in\mathbb{Z}^2} q^{Q(\underline{n})}. \tag{5.5}$$

The series defining θ_Q converges absolutely on $\tau \in \mathcal{H}$. This may be seen by noting that, for $\tau = x + iy \in \mathcal{H}$ (so $y > 0$), we have $|q(\tau)| = \exp(-2\pi y) = \epsilon < 1$. Now Q is positive definite and, in fact, $Q(x, y) \geq k(x^2 + y^2)$ for some constant k (depending on a, b and c). So $|\theta(\tau)| \leq \sum_x \sum_y \epsilon^{k(x^2+y^2)} \leq (1 - \epsilon^k)^{-2}$. Hence the theta series is a holomorphic function on $\mathcal{H}$. In general there may be poles at the cusps. At the cusp ∞ we see that θ_Q takes the value 1.

In order to prove that the θ_Q are modular forms it is usual to generalise slightly and study

$$\theta_Q(\tau; \underline{h}) := \sum_{\substack{\underline{n}\,\in\,\mathbb{Z}^2 \\ \underline{n}\,\equiv\,\underline{h}\,(N)}} q^{Q(\underline{n})/N^2}. \tag{5.6}$$

where $\underline{h} \in \mathbb{Z}^2$. Note that this is a generalisation as $\theta_Q(\tau) = \theta_Q(\tau; \underline{0})$. We quote the following result without proof from Ogg [29] Theorems 20 and 20^+ on pages VI-22 and VI-25, or Shimura [34] Proposition 2.1.

Theorem 3 *For* $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$,

$$\theta_Q(\tau;\underline{h})\,|\gamma = (c\tau+d)^{-1}\theta_Q(\gamma(\tau);\underline{h}) = exp\left(2\pi iabQ(\underline{h})/N^2\right)\chi(d)\theta_Q(\tau;a\underline{h}).$$

Here the character χ *is defined to be the Jacobi symbol (see Shimura [34] pg. 442)*

$$\chi(d) = \left(\frac{\Delta}{d}\right).$$

Note that this is the description of the character, χ, for quadratic forms in two variables. The general formula (for higher weight) is somewhat more complicated (see [29] or [32]).

In the applications we set $\underline{h} = \underline{0}$ and find that $\theta_Q(\tau)$ is a modular form of weight 1, level N and character χ.

Theorem 3 is proved by first showing the following formula, using Poisson summation (as always, the quadratic form Q corresponds to the matrix A).

$$\theta_Q(\tau;\underline{x})\frac{\tau}{i} = D^{-1/2}\sum_{\underline{n}\in\mathbb{Z}^2}\exp\bigl(2\pi i\underline{n}^t\underline{x} - \pi i\tau^{-1}\underline{n}^tA^{-1}\underline{n}\bigr). \tag{5.7}$$

The general case of Theorem 3 may then be obtained by careful use of this basic relation.

In later sections we will need a generalisation of the basic transformation formula (5.7). The rest of this section concerns the statement and proof of this generalisation. It is well known that one may generalise the notion of theta series by putting a character in the definition, namely $\theta_Q(\tau;\psi) = \sum_{\underline{n}}\psi(\underline{n})\,q^{Q(\underline{n})}$. Our analysis is motivated by this example, however we have gone further by noting that the multiplicative property of ψ is not essential.

Definition 11 *Let* P *be a positive integer. A* **function of period** P *is a mapping* $\psi : \mathbb{Z}^2 \to \mathbb{C}$ *such that* $\psi(\underline{n}+\underline{m}) = \psi(\underline{n})$ *for all* $\underline{m} \in P\mathbb{Z}^2$.

Given a function ψ of period P, and any $\underline{x} \in \mathbb{R}^2$, we define the theta series

$$\theta_Q(\tau;\underline{x},\psi) := \sum_{\underline{n}\in\mathbb{Z}^2}\psi(\underline{n})\,q^{Q(\underline{n}+\underline{x})}. \tag{5.8}$$

Note that the usage $\underline{x} \in \mathbb{R}^2$ is similar, but not identical, to the $\underline{h} \in \mathbb{Z}^2$ of equation (5.6). We now give the generalisation of (5.7) in this context.

Proposition 8 *Suppose* ψ *is a function of period* P. *Write* $S = \{(i,j)^t \mid 0 \le i,j < P\}$ *(i.e.,* S *is a set of representatives of* $\mathbb{Z}^2/(P\mathbb{Z}^2)$*). Suppose* Q *is a quadratic form arising from a matrix* A *of the usual form. Then*

$$\theta_Q(\tau;\underline{x},\psi) = iD^{-1/2}\tau^{-1}\sum_{\underline{n}\in\mathbb{Z}^2}\left[\frac{1}{P^2}\sum_{\underline{s}\in S}\psi(\underline{s})\,exp(2\pi i\underline{n}^t\underline{s}/P)\right]exp\left(\frac{2}{P}\pi i\underline{n}^t\underline{x} - \pi i\underline{n}^tA^{-1}\underline{n}/P^2\tau\right). \tag{5.9}$$

Proof. For a fixed τ write $f(\underline{x}) = \theta_Q(\tau;\underline{x},\psi)$. Then f is a periodic map from $\mathbb{R}^2$ to $\mathbb{C}$ of period P. We consider f as mapping the "square" $[0,P]^2 \subseteq \mathbb{R}^2$ into $\mathbb{C}$.

There is a standard orthogonal basis for the continuous functions on $[0,P]^2$, namely $\{f_{\underline{n}}(\underline{x}) := \exp(2\pi i\underline{n}^t\underline{x}/P) \mid \underline{n} \in \mathbb{Z}^2\}$. The standard Fourier theorem states that f may be written as $\sum_{\underline{n}\in\mathbb{Z}^2}a_{\underline{n}}f_{\underline{n}}$, where

$$a_{\underline{n}} = \frac{1}{P^2}\int_{[0,P]^2}f(\underline{x})f_{\underline{n}}(-\underline{x})d\underline{x}.$$

We will calculate the Fourier coefficients of the function $f(\underline{x})$ following the methods used in Ogg [29] pages VI-11 and VI-12.

$$a_{\underline{n}} = \frac{1}{P^2}\int_0^P\int_0^P \sum_{\underline{m}\in\mathbb{Z}^2} \psi(\underline{m})\exp(2\pi i\tau Q(\underline{m}+\underline{x}))\exp(-2\pi i\underline{n}^t\underline{x}/P)d\underline{x}.$$

We may swap the order of integration and summation so that the sum over $\underline{m}$ is on the outside. Now break the sum over $\underline{m}\in\mathbb{Z}^2$ up into P^2 parts by summing first over $\underline{s}\in S$ (where S is a set of representatives of $\mathbb{Z}^2/P\mathbb{Z}^2$) and then over $\underline{m}\equiv\underline{s}(\text{mod } P)$. We now have isolated the action of the function ψ. So we have

$$a_{\underline{n}} = \frac{1}{P^2}\sum_{\underline{s}\in S}\psi(\underline{s})\left[\sum_{\substack{\underline{m}\,\in\,\mathbb{Z}^2\\ \underline{m}\,\equiv\,(0,0)^t\ (\text{mod } P)}}\int_0^P\int_0^P \exp(2\pi i\tau Q(\underline{s}+\underline{m}+\underline{x}))\exp(-2\pi i\underline{n}^t\underline{x}/P)d\underline{x}\right].$$

Now substitute $\underline{y}=\underline{m}+\underline{x}$ (noting that we have $\exp(-2\pi i\underline{n}^t\underline{y}/P)=\exp(-2\pi i\underline{n}^t\underline{x}/P)$). The sum of the double integral may now easily be turned into a double infinite integral.

$$a_{\underline{n}} = \frac{1}{P^2}\sum_{\underline{s}\in S}\psi(\underline{s})\left[\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}\exp(2\pi i\tau Q(\underline{s}+\underline{y})-2\pi i\underline{n}^t\underline{y}/P)d\underline{y}\right]. \tag{5.10}$$

The next step is to "complete the square" on the inside of the exp in equation (5.10). For typesetting considerations write $\underline{w}:=\underline{s}+\underline{y}-\frac{1}{P}\tau^{-1}A^{-1}\underline{n}$. Note that $\tau\underline{w}^tA\underline{w}=\tau(\underline{s}+\underline{y})^tA(\underline{s}+\underline{y})-\frac{2}{P}\underline{n}^t\underline{y}-\frac{2}{P}\underline{n}^t\underline{s}+\frac{1}{P^2}\underline{n}^tA^{-1}\underline{n}/\tau$. Hence the term in square brackets of (5.10) may be written as

$$\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}\exp\left(\pi i\tau\underline{w}^tA\underline{w}\right)\exp\bigl(2\pi i\underline{n}^t\underline{s}/P-\pi i\underline{n}^tA^{-1}\underline{n}/P^2\tau\bigr)\,d\underline{y}.$$

The second exponential has no dependence on $\underline{y}$, so it may be carried to the front as a constant. The remaining integral may be evaluated using exactly the same techniques as used in Ogg ([29] pages VI-11 and VI-12), and this gives a value of $D^{-1/2}i\tau^{-1}$.

Hence we have

$$a_{\underline{n}} = \left[\frac{1}{P^2}\sum_{\underline{s}\in S}\psi(\underline{s})\exp(2\pi i\underline{n}^t\underline{s}/P)\right]D^{-1/2}i\tau^{-1}\exp\bigl(-\pi i\underline{n}^tA^{-1}\underline{n}/P^2\tau\bigr)$$

and the statement of the proposition follows from this. □

We should note that these generalised theta series with functions of period P need not actually be modular forms. However, if the function ψ of period P satisfies certain relations, then the theta series will be a modular form. We do not go into detail about this point, as the definition of the hemi-canonical map will not actually use this general notion of theta series. The functions of period P arise, in practice, when trying to analyse the behaviour of the theta series under certain Atkin-Lehner involutions (see Section 5.6). The previous proposition gives all the information required to understand the action of the involutions and therefore we give no further analysis.

It is possible to generalise the definition of theta series in other ways. One may use spherical functions to create more theta series of a given level. This changes the weight of the corresponding modular form. We could use this to generate equations but, if we start with forms of different weight, the equations will not be homogeneous. We do not explore that option in this thesis.

We finally note one further result which will be useful in later work. Notice that this result applies to the discriminant, D, of the form rather than the level N.

Theorem 4 *([29] Corollary page VI-12) If Q is a quadratic form of discriminant D arising from a matrix A and if DA^{-1} is equivalent to A then*

$$\theta_Q(\tau)\left|\begin{pmatrix} 0 & -1 \\ D & 0 \end{pmatrix}\right. = -i\theta_Q(\tau).$$

5.6 Involutions on Theta Series

It will be important to understand how the theta series behave under the involutions W_n. This is actually quite complicated.

Theorem 4 of the previous section explains the behaviour of $\theta(\tau)$ under W_N when $N = D$. However we will sometimes consider theta series of composite level. Thus we must understand the action of the involutions W_q where $q|N$. It seems that the eigenvalues of W_n depend quite subtly on the arithmetic properties of the quadratic forms associated with the theta series.

We give a full analysis of the case $D = 76 = 2^2 19$ and we let the reader wallow in the agony with us.

There are 3 strong equivalence classes of quadratic forms with discriminant 76. Namely

$$A_1 = \begin{pmatrix} 2 & 0 \\ 0 & 38 \end{pmatrix} \qquad A_2 = \begin{pmatrix} 4 & 2 \\ 2 & 20 \end{pmatrix} \qquad A_3 = \begin{pmatrix} 8 & 2 \\ 2 & 10 \end{pmatrix}.$$

Note that A_1 and A_3 have level 76 while A_2 has level 38 (i.e., A_2 corresponds to an imprimitive form). The order having discriminant $2^2 19$ is $\mathcal{O} = \langle 1, \sqrt{-19}\rangle$ in $\mathbb{Q}(\sqrt{-19})$. As there are two weak equivalence classes of matrices which are strongly equivalent to A_3 we see that the order $\mathcal{O}$ has class number 3.

Define the theta series $\theta_j(\tau) := \theta_{Q_j}(\tau)$, where Q_j is the quadratic form associated with the matrix A_j. For all $\gamma \in \Gamma_0(76)$ we have

$$\theta_j(\tau)\,|\gamma = \chi(d)\theta_j(\tau), \tag{5.11}$$

where $\chi(d) = \left(\frac{-76}{p}\right)$ for any prime $p \equiv d \pmod{N}$. It is an important point that the character here depends on the discriminant and not the level. Therefore the theta series using A_2 will have the same character as the theta series associated to A_1 and A_3. On the other hand, we cannot include the theta series associated to $\frac{1}{2}A_2$ (which has level 38), as it will have a different character.

We now study the behaviour of these the Atkin-Lehner involution W_{19}. Note that, in general, the theta series we consider will not be eigenforms with respect to W_n. This is not a problem for the application, because the hemi-canonical map is a map into projective space, therefore all that is required is that $\theta(\tau)|W_n = \mu(\tau)\theta(\tau)$ where $\mu(\tau)$ is the same for all the theta series under consideration. It is usual to call $\mu(\tau)$ the multiplier. We stress that the multiplier need not be a constant, it may be a complicated function of τ. The issue is to know, for which W_n, all the theta series of a given discriminant have the same multiplier with respect to W_n. If this occurs then the hemi-canonical map will factor through the quotient.

The rest of this section is dedicated to proving that $\theta_j(\tau)|W_{19} = -i\theta_j(\tau)$ for $j = 1, 2, 3$. In this case the theta series are actually eigenforms. The arguments in this section are elementary but detailed. It is necessary to handle the case θ_2 separately from the other two cases.

We first analyse $\theta_2(\tau)|W_{19}$. On $\Gamma_0(38)$, the involution W_{19} may be chosen to be

$$W_{19} = \begin{pmatrix} 19 & -10 \\ 38 & -19 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Q}).$$

Writing $\omega = 38\tau - 19$, we have

$$\theta_2(\tau)|W_{19} = \sqrt{19}\omega^{-1}\theta_2\left(\frac{19\tau - 10}{\omega}\right) = \sqrt{19}\omega^{-1}\theta_2\left(\frac{1}{2}\left(1 - \frac{1}{\omega}\right)\right)$$
$$= \sqrt{19}\omega^{-1}\sum_{\underline{n}\in\mathbb{Z}^2}\exp\left(2\pi i Q_2(\underline{n})/2\right)\exp\left(-2\pi i Q_2(\underline{n})/2\omega\right).$$

Now observe that $Q_2(\underline{n}) \equiv 0(\mathrm{mod}\ 2)$ and so the first exp term is identically 1. Apply equation (5.7) (equivalently (5.9) with $P = 1$) by substituting $-1/2\omega$ for τ and setting $\underline{x} = \underline{0}$. The previous expression becomes

$$= \sqrt{19}\omega^{-1}i(-2\omega)D^{-1/2}\sum_{\underline{n}\in\mathbb{Z}^2}\exp\left(\pi i\underline{n}^t A_2^{-1}\underline{n}2\omega\right) \qquad (5.12)$$

where $D = 76$. We now use the fact that $2\omega = D\left(\tau - \frac{1}{2}\right)$ and that DA_2^{-1} gives the same quadratic form (by swapping n_1 and n_2) as A_2. Thus equation (5.12) becomes

$$-i\sum_{\underline{n}\in\mathbb{Z}^2}\exp\left(2\pi i Q_2(\underline{n})\left(\tau - \frac{1}{2}\right)\right) = -i\theta_2(\tau).$$

So we have shown that $\theta_2(\tau)|W_{19} = -i\theta_2(\tau)$.

Now consider the level 76 forms θ_1 and θ_3. We repeat a similar argument but in this case we collect some functions of period 2 along the way. We handle both cases together until the last step, when the difference between the quadratic forms becomes important.

For level 76 a choice of W_{19} is

$$W_{19} = \begin{pmatrix} 19 & -5 \\ 76 & -19 \end{pmatrix}.$$

Writing $\omega = 76\tau - 19$ we find, as before,

$$\theta(\tau)|W_{19} = \sqrt{19}\omega^{-1}\theta\left(\frac{1}{4}\left(1 - \frac{1}{\omega}\right)\right) = \sqrt{19}\omega^{-1}\sum_{\underline{n}\in\mathbb{Z}^2}\exp\left(2\pi i Q(\underline{n})/4\right)\exp\left(-2\pi i Q(\underline{n})/4\omega\right). \qquad (5.13)$$

Observe that $\exp\left(2\pi i Q(\underline{n})/4\right)$ is a function of period $P = 2$ which depends on the behaviour of $Q(\underline{n})$. We will simply call this $\psi(\underline{n})$ and return to it later. Also observe that $4\omega = D\omega'$ where $\omega' = 4\tau - 1$.

As in the level 38 example we must now apply a transformation formula. In this case we need (5.9) as we are dealing with functions of period P. Again we substitute $-1/4\omega$ for τ in (5.9) and set $\underline{x} = \underline{0}$. We find that equation (5.13) becomes

$$= -2i\sum_{\underline{n}\in\mathbb{Z}^2}\left[\frac{1}{4}\sum_{\underline{s}}\psi(\underline{s})\exp\left(2\pi i\underline{n}^t\underline{s}/2\right)\right]\exp\left(\pi i\underline{n}^t A^{-1}\underline{n}4\omega/4\right). \qquad (5.14)$$

Now use the fact that $4\omega = D\omega'$ and that DA^{-1} is equivalent to A. But we must be careful, because in the equivalence of DA^{-1} and A we switch the components of $\underline{n}$. Therefore we change the first exp term within the square brackets. We write X for the obvious equivalence matrix and write $\underline{m} = X\underline{n}$ (so, equivalently, $\underline{n} = X\underline{m}$).

Equation (5.14) therefore becomes

$$= -2i\sum_{\underline{m}\in\mathbb{Z}^2}\left[\frac{1}{4}\sum_{\underline{s}}\psi(\underline{s})\exp\left(2\pi i(X\underline{m})^t\underline{s}/2\right)\right]\exp(2\pi i Q(\underline{m})(4\tau - 1)/4). \qquad (5.15)$$

In order to show that these theta series have eigenvalue $-i$ with respect to W_{19} it will therefore suffice to show that

$$\frac{1}{2}\left[\sum_{\underline{s}}\psi(\underline{s})\exp\left(2\pi i(X\underline{m})^t\underline{s}/2\right)\right]\exp(-2\pi iQ(\underline{m})/4)=1 \tag{5.16}$$

for each $\underline{m}\in\mathbb{Z}/2\mathbb{Z}$.

At this stage it is necessary to treat the two cases differently. For $\theta_1(\tau)$ we note that $Q(x,y)=x^2+19y^2$. We see that $Q(0,0)=0, Q(1,0)\equiv 1(\text{mod } 4)$, $Q(0,1)\equiv -1(\text{mod } 4)$ and finally that $Q(1,1)\equiv 0(\text{mod } 4)$. Recall that $\psi(u,v)=$exp$(2\pi iQ(u,v)/4)$. Therefore, if we write $\underline{m}=(x,y)^t$, the term

$$\sum_{\underline{s}}\psi(\underline{s})\exp\left(2\pi i(X\underline{m})^t\underline{s}/2\right)=\left(1+i(-1)^y-i(-1)^x+(-1)^{x+y}\right). \tag{5.17}$$

Now we may try the four possibilities for $\underline{m}$ in (5.17) and we see that the result follows.

Finally, consider the case of $\theta_3(\tau)$. Here $Q(x,y)=4x^2+2xy+5y^2$. We find that the analogous equation to (5.17) is

$$\left(1+(-1)^y+i(-1)^x-i(-1)^{x+y}\right).$$

Again, by trying the four possibilities for $\underline{m}\in\mathbb{Z}^2/2\mathbb{Z}^2$ the result follows.

Note that $\theta_1(\tau)$ and $\theta_3(\tau)$ have the same behaviour under $W_N=W_D$. With θ_2, since $N\neq D$, one cannot analyse $\theta_2(\tau)|W_N$ in such a direct manner. Instead, write $W=\begin{pmatrix}0 & -1\\ 76 & 0\end{pmatrix}$ and note that

$$W_{38}=W\gamma \qquad \text{where} \qquad \gamma=\begin{pmatrix}1/2 & 0\\ 0 & 1\end{pmatrix}.$$

Therefore $\theta_2(\tau)|W_{38}=\theta_2(\tau)|W|\gamma=\frac{-i}{\sqrt{2}}\theta_2(\tau/2)$, and this is seen to be not equal to $i\theta_2(\tau)$ by considering the q-expansions. Hence the theta series do not all behave the same under W_N. This therefore tells us that they do not all have the same eigenvalues under W_2 (since $W_2=W_NW_{19}$). In fact, as we will see later, these three forms give an equation for $X_0(76)/W_{19}$.

As one can see, the process of understanding the Atkin-Lehner involutions on theta series comes down to the arithmetic of the quadratic forms themselves. In general one finds that different theta series of discriminant D tend to have the same behaviour with respect to W_p (where $p^\alpha\|D$) only when D/p^α is small (e.g., 2, 3, 4). We conclude that general formulae for the behaviour in this situation will be complicated to write down. In the applications, we are usually more interested in finding equations for $X_0(N)$ or $X_0^+(N)$ where N is not highly composite, so the complexities discussed in this section do not tend to arise. Hence we spare the reader and leave this topic behind.

5.7 The Hemi-Canonical Map

We now emulate the theory of the canonical embedding and that of the projective embeddings of Mumford and Igusa, using the theta series introduced in earlier sections.

Suppose we are interested in obtaining a projective equation for the modular curve $X_0(N)$, where $N\equiv 0,-1(\text{mod } 4)$. We have seen that there are theta series, which are modular forms of weight 1 and level N, coming from integral binary quadratic forms of discriminant N. Suppose there are at least 3 such theta series, and write them as $\{\theta_1, \dots, \theta_n\}$. We may then define the map

$$\begin{aligned} \phi : X_0(N) &\rightarrow \mathbb{P}^{n-1} \\ \tau &\mapsto [\theta_1(\tau) : \cdots : \theta_n(\tau)]. \end{aligned} \tag{5.18}$$

We will call this the **hemi-canonical map** (the name was chosen by Bryan Birch). That the map does not depend on which representative, in the $\Gamma_0(N)$-orbit, of τ follows from the modularity of the $\theta(\tau)$ combined with the fact that they all have the same character.

Obviously this map is not defined if all the θ_j vanish identically at a point. However, as long as this only occurs at finitely many points, we still get a rational map of curves and this is good enough for our purposes.

The more important problem is to understand when this map is an injection. Certainly, as we have seen, all the theta series behave the same under W_D. Thus (when all the theta series have $N = D$) the hemi-canonical map factors through $X_0(N)/W_N$.

Note that the image corresponds, as in the case of the canonical map, to the curve defined by some polynomials Φ. These polynomials are found by considering relations between the θ_j which give the zero modular form. Such relations may be found using linear algebra on the q-expansions in the same manner as that used in Chapters 3 and 4.

Also note that theta series naturally have small q-expansion coefficients, and indeed their coefficients are quite sparse (meaning that zero appears quite often). This makes us optimistic that theta series could yield projective equations for modular curves which have quite small coefficients.

5.8 Examples

In this section we give some detailed examples of the hemi-canonical map. We analyse the projective curves obtained as the image of this map. This gives both a demonstration of the method in action and also an illustration of some of the difficulties inherent in this method.

5.8.1 Level 103

We find a total of three quadratic forms of determinant 103. They come from the matrices

$$\begin{pmatrix} 2 & 1 \\ 1 & 52 \end{pmatrix}, \begin{pmatrix} 4 & 1 \\ 1 & 26 \end{pmatrix} \text{ and } \begin{pmatrix} 8 & 3 \\ 3 & 14 \end{pmatrix}.$$

Notice that for each of these we have $N = D = 103$.

Write x, y and z for the theta series corresponding to these three quadratic forms. These theta series satisfy the relation

$$\begin{gathered} 2x^4 + x^3y - 5x^3z - 3x^2y^2 - 3x^2yz + 10x^2z^2 - 2xy^3 \\ +6xy^2z + xyz^2 - 9xz^3 + 6y^3z - 15y^2z^2 + 5yz^3 + 6z^4 = 0. \end{gathered}$$

This curve has only one singularity, and it is at $[1 : -2 : -1]$. We set $y = u - 2x, z = v - x$ and then make the curve affine by setting $v = 1$. This results in a curve in $\mathbb{A}^2$ which has a singular point at infinity. The form of this curve is

$$p_2(u)x^2 + p_3(u)x + p_3'(u) = 0$$

where $p_j(u)$ represents a polynomial of degree j in u. Multiplying by $p_2(u)$ and then making the (birational) change of variable $w = p_2(u)x$, gives the obvious hyperelliptic genus 2 curve

$$w^2 + p_3(u)w = -p_2(u)p_3'(u).$$

Explicitly this is

$$w^2 + (-8u^3 + 46u - 43)w = -144u^5 + 732u^4 - 1296u^3 + 781u^2 + 167u - 246.$$

This equation is a model for the genus 2 curve $X_0^+(103)$.

5.8.2 Level 76

As we have seen in Section 5.6, there are 3 quadratic forms of discriminant $76 = 2^2 19$, namely

$$A_1 = \begin{pmatrix} 2 & 0 \\ 0 & 38 \end{pmatrix} \qquad A_2 = \begin{pmatrix} 4 & 2 \\ 2 & 20 \end{pmatrix} \qquad A_3 = \begin{pmatrix} 8 & 2 \\ 2 & 10 \end{pmatrix}.$$

Set, as before, $Q_j(\underline{n}) = \frac{1}{2}\underline{n}A_j\underline{n}^t$ and $\theta_j(\tau) = \theta_{Q_j}(\tau)$. We find (using linear algebra on the q-expansions) the following relation between the three theta series.

$$-3\theta_1^5 + 13\theta_1^4\theta_2 - 24\theta_1^3\theta_2^2 + 22\theta_1^2\theta_2^3 - 9\theta_1\theta_2^4 + \theta_2^5 + 10\theta_1^3\theta_3^2 - 20\theta_1^2\theta_2\theta_3^2 + 18\theta_1\theta_2^2\theta_3^2 - 8\theta_1\theta_3^4 = 0$$

This gives a projective curve with one singularity at the point [1:1:0].

If we take functions $x(\tau) = \theta_2(\tau)/\theta_1(\tau)$ and $y = \theta_3(\tau)/\theta_1(\tau)$ we see that they satisfy the relation

$$(x-1)^2(x^3 - 7x^2 + 7x - 3) = 2y^2(4y^2 - 9x^2 + 10x - 5).$$

We know that x and y are modular functions on $\Gamma_0(76)$ and that they are both preserved under W_{19}.

By the birational change of variables $t := y/(x-1)$ we may remove the singularity at $(x, y) = (1, 0)$ and obtain the non-singular equation

$$C : x^3 - 7x^2 + 7x - 3 = t^2(8(x-1)^2t^2 - 2(9x^2 - 10x + 5)).$$

The map $(x, t) \mapsto (x, v)$ (where $v = t^2$) therefore makes C a double covering of the curve $D : x^3 - 7x^2 + 7x - 3 = v(8(x-1)^2v - 2(9x^2 - 10x + 5))$. This cover is ramified over 4 points. The curve D can be shown to be elliptic by the birational change of variables $w = 8x, u = 8(v - 9x^2 + 10x - 5)/(x + 1)$ which yields

$$E : u^2 = w^3 - 7w^2 + 16w + 64.$$

This is an elliptic curve with j-invariant $-1/2^5 19$ and we see from Cremona's tables [8] that it has conductor 38.

The Riemann-Hurwitz formula therefore shows that the genus of C is 3. The curve $X_0(76)$ is expected to split into curves of genus 1,3,2,2 (these are the $++, +-, -+, --$ parts under the involutions W_2 and W_{19}). We expect our curve C to be a subvariety of $X_0(76)/W_{19}$. Since both curves have genus 3 we conclude that we have found a model for $X_0(76)/W_{19}$ using the hemi-canonical map.

5.9 Discussion

Because the coefficients of the theta series we are considering are both small and sparse, we had high hopes that the hemi-canonical map would give good projective models for $X_0(N)$.

Indeed, the coefficients of theta series may be rigorously bounded and it was hoped that such bounds could be used to obtain a bound on the size of coefficients in models for $X_0(N)$.

Unfortunately these hopes were doomed to disappointment. The hemi-canonical map seems to be much less successful than the canonical map.

One of the main problems with the hemi-canonical map is that the number of theta series is related to the class number of $\mathbb{Q}(\sqrt{D})$. Admittedly, the image of the canonical embedding sits in space of dimension $g-1$. Nevertheless, the class number seems to grow much faster than the genus. In these cases the image of the hemi-canonical map is described by the intersection of a large number of equations. This is sometimes not a very useful form.

Often there are not enough theta series to even get started. In these cases it may be fruitful to generalise the definition of theta series (for instance, by using suitable functions of period 2). In this way we obtain more forms, but the drawback is that these forms tend to be of higher level (e.g., $4N$).

Finally, even when we are lucky enough to get a sensible number of theta series to start with, the equation relating them tends to be singular. This is not necessarily a major drawback, though it does mean that the equation is not as simple as it could be.

The root of the trouble is that there is very little control over the degree of the image of the hemi-canonical map, or the dimension of the projective space it lies in. In the case of the canonical embedding, since the weight 2 cusp forms correspond to well-understood geometric objects (the holomorphic differentials), we knew we would obtain a canonical curve of degree $2g-2$ in $\mathbb{P}^{g-1}$. In the case of the hemi-canonical map, there doesn't seem to be any concrete link between the theta series and an easily understood geometric object. Correspondingly, it is less easy to understand the geometry of the equations which arise. The dimension of the projective space comes from the weak class number which can be understood from an arithmetic viewpoint. However, one cannot predict the degree of the image curve.

Our original motivation for using theta series was that they have small q-expansion coefficients and so it was hoped they would give models with small coefficients. In this respect the method has some value as the coefficients arising are quite nice. On the other hand one does not obtain strikingly small coefficients (as we sometimes did with the canonical embedding).

5.10 Tables of Results

We list the results of some computations of equations using theta series. We only give equations for curves having genus at least one (except for $X_0^+(71)$, which is included because its coefficients are nice). Since theta series tend to all have the same eigenvalues under W_n it follows that many of the curves found do actually have small genus. The variables correspond (in alphabetical order) to the given ordering of the matrices.

Table 5. The Image of the Hemi-canonical Map

$X_0(44)/W_{44}$ $g=1$	$\begin{pmatrix} 2 & 0 \\ 0 & 22 \end{pmatrix} \begin{pmatrix} 4 & 2 \\ 2 & 12 \end{pmatrix} \begin{pmatrix} 6 & 2 \\ 2 & 8 \end{pmatrix}$ $x^3 - 2xy^2 - x^2z + xz^2 + z^3 = 0$
$X_0(63)/W_{63}$ $g=1$	$\begin{pmatrix} 2 & 1 \\ 1 & 32 \end{pmatrix} \begin{pmatrix} 4 & 1 \\ 1 & 16 \end{pmatrix} \begin{pmatrix} 8 & 1 \\ 1 & 8 \end{pmatrix}$ $2x^4 - x^3y - 2x^2y^2 + y^4 - 5x^3z + x^2yz + 2xy^2z$ $+7x^2z^2 + xyz^2 - 2y^2z^2 - 5xz^3 - yz^3 + 2z^4 = 0$ Singular at $[x:y:z] = [1:1:1]$ and $[1:-1:1]$
$X_0(68)/W_{68}$ $g=2$	$\begin{pmatrix} 2 & 0 \\ 0 & 34 \end{pmatrix} \begin{pmatrix} 4 & 2 \\ 2 & 18 \end{pmatrix} \begin{pmatrix} 6 & 2 \\ 2 & 12 \end{pmatrix}$ $x^2y^2 - xy^3 + x^2z^2 - 3xyz^2 + 2z^4 = 0$ Singular at $[x:y:z] = [1:0:0]$
$X_0^+(71)$ $g=0$	$\begin{pmatrix} 2 & 1 \\ 1 & 36 \end{pmatrix} \begin{pmatrix} 4 & 1 \\ 1 & 18 \end{pmatrix} \begin{pmatrix} 6 & 1 \\ 1 & 12 \end{pmatrix} \begin{pmatrix} 8 & 3 \\ 3 & 10 \end{pmatrix}$ $w^2 - wx - xy + y^2 - wz + yz = 0$ $wx - x^2 - y^2 - wz + xz + z^2 = 0$ $wx - wy - xy - y^2 + 2yz = 0$
$X_0(75)/W_{75}$ $g=1$	$\begin{pmatrix} 2 & 1 \\ 1 & 38 \end{pmatrix} \begin{pmatrix} 6 & 3 \\ 3 & 14 \end{pmatrix} \begin{pmatrix} 10 & 5 \\ 5 & 10 \end{pmatrix}$ $2x^4 - 7x^3y + 7x^2y^2 - 7xy^3 + 2y^4 + x^3z + x^2yz - xy^2z - y^3z$ $-2x^2z^2 + 6xyz^2 - 2y^2z^2 + z^4 = 0$ Singular at [1:-1:z] where $z^2 = 5$.
$X_0^+(79)$ $g=1$	$\begin{pmatrix} 2 & 1 \\ 1 & 40 \end{pmatrix} \begin{pmatrix} 4 & 1 \\ 1 & 20 \end{pmatrix} \begin{pmatrix} 8 & 3 \\ 3 & 10 \end{pmatrix}$ $x^3 - 2xy^2 + y^3 - x^2z + 2xyz - 3y^2z - xz^2 + yz^2 + 2z^3 = 0$

$X_0(84)/W_{84}$ $g = 4$	$\begin{pmatrix}2 & 0\\ 0 & 42\end{pmatrix}\begin{pmatrix}6 & 0\\ 0 & 14\end{pmatrix}\begin{pmatrix}4 & 2\\ 2 & 22\end{pmatrix}\begin{pmatrix}10 & 4\\ 4 & 10\end{pmatrix}$ $w^3 + wx^2 - 2wy^2 - w^2z + x^2z = 0$ $w^2x + x^3 - w^2y + x^2y - 2xz^2 = 0$ $w^2xy - x^2y^2 - xy^3 - wx^2z - w^2z^2 + 2y^2z^2 + wz^3 = 0$ $-w^2xy + w^2y^2 - xy^3 + wx^2z - 4wxyz + 2wy^2z$ $+x^2z^2 - 2xyz^2 + 2y^2z^2 + wz^3 = 0$ Singular model which is not a complete intersection.
$X_0(92)/W_{23}$ $g = 1$	$\begin{pmatrix}2 & 0\\ 0 & 26\end{pmatrix}\begin{pmatrix}4 & 2\\ 2 & 24\end{pmatrix}\begin{pmatrix}8 & 2\\ 2 & 12\end{pmatrix}$ $2x^3 - 2xy^2 - y^3 - 4x^2z + 3y^2z + 4xz^2 - 3yz^2 + z^3 = 0$
$X_0(99)/W_{99}$ $g = 3$	$\begin{pmatrix}2 & 1\\ 1 & 50\end{pmatrix}\begin{pmatrix}10 & 1\\ 1 & 10\end{pmatrix}\begin{pmatrix}6 & 3\\ 3 & 18\end{pmatrix}$ $x^5 - x^4y + x^3y^2 + x^2y^3 - xy^4 + y^5 - 2x^4z - 2x^2y^2z$ $-2y^4z + x^3z^2 + 5x^2yz^2 + 5xy^2z^2 + y^3z^2 - 2x^2z^3 - 8xyz^3$ $-2y^2z^3 + xz^4 + yz^4 + 2z^5 = 0$ Singular at [1:1:1] and $[1{:}(1 \pm \sqrt{-3})/2{:}0]$
$X_0(100)/\langle W_2, W_5\rangle$ $g = 1$	$\begin{pmatrix}2 & 0\\ 0 & 50\end{pmatrix}\begin{pmatrix}10 & 0\\ 0 & 10\end{pmatrix}\begin{pmatrix}4 & 2\\ 2 & 26\end{pmatrix}$ $x^3 - 3x^2y + xy^2 + y^3 + 2x^2z + 2xyz - 4xz^2 = 0$

$X_0^+(103)$	$\begin{pmatrix} 2 & 1 \\ 1 & 52 \end{pmatrix} \begin{pmatrix} 4 & 1 \\ 1 & 26 \end{pmatrix} \begin{pmatrix} 8 & 3 \\ 3 & 14 \end{pmatrix}$
$g = 2$	$2x^4 + x^3y - 5x^3z - 3x^2y^2 - 3x^2yz + 10x^2z^2 - 2xy^3 + 6xy^2z + xyz^2 - 9xz^3$
	$+6y^3z - 15y^2z^2 + 5yz^3 + 6z^4 = 0$
	Singular at [−1:2:1]
$X_0^+(127)$	$\begin{pmatrix} 2 & 1 \\ 1 & 64 \end{pmatrix} \begin{pmatrix} 4 & 1 \\ 1 & 32 \end{pmatrix} \begin{pmatrix} 8 & 1 \\ 1 & 16 \end{pmatrix}$
$g = 3$	$4x^5 + 4x^4y - 20x^4z - 5x^3y^2 - 24x^3yz + 45x^3z^2 - 5x^2y^3 + 10x^2y^2z$
	$+53x^2yz^2 - 58x^2z^3 + xy^4 + 18xy^3z - 7xy^2z^2 - 58xyz^3 + 42xz^4 + 2y^5 + y^4z$
	$-13y^3z^2 + 2y^2z^3 + 23yz^4 - 15z^5 = 0$
	Singular at [−1:4:2] and [1:−1:1]
$X_0^+(131)$	$\begin{pmatrix} 2 & 1 \\ 1 & 66 \end{pmatrix} \begin{pmatrix} 6 & 1 \\ 1 & 22 \end{pmatrix} \begin{pmatrix} 10 & 3 \\ 3 & 14 \end{pmatrix}$
$g = 1$	$x^3 - x^2y + xy^2 - 2y^3 - 2x^2z - y^2z + 2xz^2 + 3yz^2 - z^3 = 0$
$X_0^+(151)$	$\begin{pmatrix} 2 & 1 \\ 1 & 72 \end{pmatrix} \begin{pmatrix} 4 & 1 \\ 1 & 38 \end{pmatrix} \begin{pmatrix} 8 & 3 \\ 3 & 20 \end{pmatrix}$
$g = 3$	$-x^6 - 6x^5y + 10x^5z - 4x^4y^2 + 44x^4yz - 41x^4z^2 + 13x^3y^3 - 3x^3y^2z$
	$-113x^3yz^2 + 95x^3z^3 + 12x^2y^4 - 87x^2y^3z + 81x^2y^2z^2 + 135x^2yz^3$
	$-136x^2z^4 - 8xy^5 - 4xy^4z + 123xy^3z^2 - 149xy^2z^3 - 73xyz^4 + 115xz^5$
	$-8y^6 + 48y^5z - 64z^2y^4 - 49z^3y^3 + 115z^4y^2 + 5yz^5 - 50z^6 = 0$
	Must have many singularities

$X_0^+(179)$ $g = 3$	$\begin{pmatrix} 2 & 1 \\ 1 & 90 \end{pmatrix} \begin{pmatrix} 6 & 1 \\ 1 & 30 \end{pmatrix} \begin{pmatrix} 10 & 1 \\ 1 & 18 \end{pmatrix}$ $x^5 - x^4y + 2x^3y^2 - x^2y^3 + xy^4 + 2y^5 - 4x^3yz - x^2y^2z - 8xy^3z$ $-7y^4z + 3x^2yz^2 + 4xy^2z^2 + 5y^3z^2 + x^2z^3 + 4xyz^3 - y^2z^3 = 0$ Singular at [0:0:1] and [−1:1:1]
$X_0(188)/\langle W_2, W_{47}\rangle$ $g = 1$	$\begin{pmatrix} 2 & 0 \\ 0 & 94 \end{pmatrix} \begin{pmatrix} 6 & 2 \\ 2 & 32 \end{pmatrix} \begin{pmatrix} 14 & 6 \\ 6 & 16 \end{pmatrix}$ $-x^3y^2 - x^3z^2 + 2x^2y^3 - 2x^2y^2z + 4x^2yz^2 + 2x^2z^3 - 2xy^4 + 4xy^3z$ $-3xy^2z^2 - 4xyz^3 - xz^4 + 2y^5 = 0$ Singular at [1:0:0], [1:0:1] and [1:1:−1]
$X_0^+(223)$ $g = 6$	$\begin{pmatrix} 2 & 1 \\ 1 & 112 \end{pmatrix} \begin{pmatrix} 4 & 1 \\ 1 & 56 \end{pmatrix} \begin{pmatrix} 8 & 1 \\ 1 & 28 \end{pmatrix} \begin{pmatrix} 14 & 1 \\ 1 & 16 \end{pmatrix}$ $w^4 + 2w^3x + 2w^2x^2 + wx^3 - 2x^4 - 2w^3y - 7w^2xy - 5wx^2y + 2w^2y^2$ $+7wxy^2 + 6x^2y^2 - wy^3 - 4xy^3 - w^3z - 3w^2xz - 5wx^2z + 5x^3z + 4w^2yz$ $+wxyz - x^2yz - 6wy^2z - 7xy^2z + 5y^3z + w^2z^2 + 9wxz^2 - 3x^2z^2 + 3wyz^2$ $-4y^2z^2 - 3wz^3 + 3yz^3 + 2z^4 = 0$ And three more equations like this first one !
$X_0^+(251)$ $g = 4$	$\begin{pmatrix} 2 & 1 \\ 1 & 126 \end{pmatrix} \begin{pmatrix} 6 & 1 \\ 1 & 42 \end{pmatrix} \begin{pmatrix} 14 & 1 \\ 1 & 18 \end{pmatrix} \begin{pmatrix} 10 & 3 \\ 3 & 26 \end{pmatrix}$ $w^2x - wx^2 - w^2y + x^2y + wy^2 + xy^2 - 2xz^2 = 0$ $w^3 - w^2x + 2wx^2 - x^3 - 2wxy + x^2y + 3wy^2 - 2xy^2 - 2y^3 - 2w^2z$ $-2x^2z + 3y^2z + 2xz^2 - yz^2 + z^3 = 0$ Note that this is an intersection of two cubics, rather than an intersection of a cubic and a quadric, therefore it must be singular.

We should make a few comments about how to check that the equations are what they claim to be.

In almost all cases $N = D$ and therefore the theta series all behave the same under W_N. There is the possibility that the theta series could have the same behaviour under other involutions W_n. Also one cannot rule out the chance that there are other ways for injectivity of the hemi-canonical map to fail. Thus we expect the equations to describe some quotient of $X_0(N)$ and usually this will be contained in $X_0(N)/W_N$.

By the Hurwitz formula, for genus at least 2, taking quotients reduces the genus. Thus we have been able to check the correctness of our claims by calculating the genus of each of the curves listed. The Plücker formulae given in Griffiths and Harris [17] are useful for this task.

We briefly discuss the calculation for $X_0(84)/W_{84}$, as it is the hardest case included in the tables.

The second equation listed allows us to solve birationally for y, and thus obtain the plane curve

$$w^6 - 3w^4x^2 + 8w^2x^2z^2 + 8wx^2z^3 - 5w^2x^4 - 8wx^4z - x^6. \tag{5.19}$$

This is singular at [1:1:−1], [−1:1:1] and [0:0:1]. The first two singularities are double points or cusps. The third singularity has multiplicity 3. We will show that it may be removed by blowing-up twice.

To blow-up [0:0:1] first set $z = 1$ to make the equation affine, with a singularity of multiplicity 3 at $(0, 0)$. Then set $x = \lambda w$ and divide by w^3 to get the equation

$$-w^3\lambda^6 - 5w^3\lambda^4 - 8w^2\lambda^4 - 3w^3\lambda^2 + 8w\lambda^2 + 8\lambda^2 + w^3.$$

The singularity at $(0, 0)$ now has multiplicity one. Blowing up again by setting $\lambda = \mu w$ and dividing by w^2 gives an equation which is non-singular at $(0, 0)$.

Therefore the genus of the singular plane curve (5.19) is given by

$$\frac{(6-1)(6-2)}{2} - \frac{3(3-1)}{2} - 1 - 1 - 1 = 4.$$

as expected.

Chapter 6

Heights of Modular Curves

In earlier chapters we have given explicit equations for projective embeddings of modular curves. Some of these equations have very small coefficients. The theory of heights is a way to study coefficient size in a precise mathematical manner. In this chapter we discuss the relationships between different notions of height of (rather than "on") curves. We are looking for clues which would enable us to show why modular curves seem to have a model with small coefficients. Also it would be interesting to know if our models with small coefficients can give any information about the heights of abelian varieties such as $J_0(N)$.

We will show how these heights relate to some conjectures in number theory. We discuss some problems which could be considered as steps towards the proof of these conjectures. Using the examples of previous chapters and by examining some of the heights in detail we illustrate the subtlety and difficulty of some of these problems. It is hoped that this chapter has value as a companion to the more theoretical literature on this topic.

This chapter is more speculative and concerns deeper theories than the rest of the thesis. Correspondingly we will be more terse with the description and details. The first section contains a brief summary of some of the motivating ideas and tools.

6.1 Heights and Arakelov Theory

The guiding star in this chapter, upon which the reader's eyes should be fixed, is the classical logarithmic height of a point in projective space over a number field. For a point $P \in \mathbb{P}^N(K)$ fix a representative $(P_0, \dots, P_N) \in K^{N+1}$. For all finite places ν of K set $n_\nu = 1$ and define $\|P\|_\nu = \max\{|P_j|_\nu\}$, where $|.|_\nu$ denotes the usual (normalised) ν-adic absolute value. For each infinite place ν of K define $\|P\|_\nu = \left(\sum_j |P_j|_\nu^2\right)^{1/2}$ and set $n_\nu = 1$ if ν is a real place, or $n_\nu = 2$ if ν is complex. Then the logarithmic height of P is defined to be

$$h(P) = \frac{1}{[K:\mathbb{Q}]} \sum_\nu n_\nu \log \|P\|_\nu .$$

A key point is that this notion of height does not depend on the particular representative of P chosen in K^{N+1}. The reason for this is the well-known product formula.

Generalisations of the classical height have many applications. For instance the analysis of the heights of rational points on elliptic curves is a major ingredient of the proof of the Mordell-Weil theorem. A computational analysis of the heights may be used to actually compute generators of the Mordell-Weil group.

The classical height associates a real number to a point in some space. In this chapter we are more interested in heights which associate a real number to some geometric object (for instance a curve or an abelian variety).

It was observed that the classical height on projective space may be interpreted in the language of Arakelov Theory (this interpretation is described in Faltings and Wüstholz [11] II.1). Arakelov Theory is also a useful language for the construction of heights on other objects. We aim to keep the description as simple as possible and so we refer to [39], [40] for details on Arakelov theory in general.

In the Arakelovian approach, one of the basic objects is the metrized line bundle. It will be necessary to mention such objects in a few places in this Chapter, so we give some discussion about them here. A good reference for this theory is Silverman [37]. Let X be a variety defined over a field K. We will think of X as a scheme over Spec K, with sheaf of functions $\mathcal{O}_X$. Let $\mathcal{L}$ be a line bundle on X. For each point P of X, the stalk $\mathcal{L}_P$ is an $\mathcal{O}_P$-module. Since X is a scheme over $\mathrm{Spec}(K)$, the stalk $\mathcal{O}_P$ is a K-algebra. Therefore, $\mathcal{L}_P$ is a K-vector space. For each infinite place ν of K one may consider the K_ν-vector space $\mathcal{L}_P \otimes K_\nu$, where K_ν is the completion of K with respect to the valuation ν. We call $\mathcal{L}$ a **metrized line bundle** if there are metrics on each $\mathcal{L}_P \otimes K_\nu$, which are chosen so that they "vary continuously" over P in X (see Silverman [37]).

6.2 Heights of Abelian Varieties

One of the ideas introduced by Faltings (see, for instance, [11] or [12]) in order to prove the Mordell conjecture is the notion of a height of an abelian variety. This is a number associated to an abelian variety which measures, in some sense, its arithmetic complexity. Suppose A is an abelian variety defined over a number field K. Let $\mathcal{A}$ be the connected component of zero in the Néron Model of A over $\mathrm{Spec}(\mathcal{O}_K)$. The canonical bundle $\omega_{\mathcal{A}/\mathcal{O}_K}$ may be given the structure of a metrized line bundle (i.e., we give a canonical Hermitian metric on the bundle over each infinite place, see Silverman [37] and [38] for details). The height of the abelian variety A is defined to be

$$h(A) = \frac{1}{[K:\mathbb{Q}]}\deg\left(\omega_{\mathcal{A}/\mathcal{O}_K}\right)$$

where deg denotes the usual degree function (see Silverman [37]) for a metrized line bundle over $\mathrm{Spec}(\mathcal{O}_K)$.

Let $\mathcal{M}_g$ be the moduli space of principally polarised abelian varieties of dimension g. Assume we have some projective embedding of $\mathcal{M}_g$. The height of such an abelian variety A is closely related to the height of the point $P \in \mathcal{M}_g$ which corresponds to A.

Information about heights of abelian varieties gives vast amounts of arithmetic information. The following few sections will start to describe some of the theory necessary to provide a theory of heights of projective varieties.

6.3 Heights of Polynomials

Heights also arise in the theory of transcendental numbers. Working in this area Philippon [31] (following Mahler and others) introduced the height of a polynomial. The height is defined to be a sum of local terms, in the same way as the classical height on projective space.

Suppose $P(\underline{x})$ is a polynomial in $K[x_0, \ldots, x_N]$ (where K is a number field). Let ν be a finite place of K. The local component, at ν, of the height of the polynomial P is defined to be

$$M_\nu(P) := log\, max\{|P_J|_\nu\} \tag{6.1}$$

where P_J runs through all the coefficients of the polynomial P.

For an infinite place ν of K we define a "local height" using the Mahler measure. The classical Mahler measure of a polynomial P is

$$M(P) = \int_0^1 \dots \int_0^1 \log |P(\exp(2\pi i u_0), \dots, \exp(2\pi i u_N))| \, du_0 \dots du_N .$$

We will use the following variation of the Mahler measure (see Soulé [39] or [3]). For homogeneous polynomials in $N+1$ variables, define a set $\mathbb{S} = \{z \in \mathbb{C}^{N+1} \mid \sum_{i=0}^{N} |z_i|^2 = 1\}$. This is a sphere in $\mathbb{C}^{N+1}$. Let $d\mu$ be the unique $U(N+1)$-invariant probability measure on $\mathbb{S}$. Each infinite place, ν, corresponds to a pair of conjugate embeddings $K \overset{\sigma_\nu}{\hookrightarrow} \mathbb{C}$. The absolute value $|\alpha|_\nu$ on K, associated to ν, is $|\sigma_\nu(\alpha)|$, where $|.|$ is the usual absolute value on $\mathbb{C}$. Therefore, for an infinite place ν of K, fix a corresponding embedding $\sigma : K \hookrightarrow \mathbb{C}$ and then consider the polynomial $\sigma P(z)$ as a polynomial with coefficients in $\mathbb{C}$. Define the local height of the polynomial P at the infinite place ν to be

$$M_\nu(P) := \int_{\mathbb{S}} log|\sigma P(z)| d\mu. \tag{6.2}$$

Some authors discuss the Fubini-Study metric on $\mathbb{P}^N(\mathbb{C})$ but the definition we have given is less complicated and is sufficient for what we need.

To combine these local heights (6.1) and (6.2) into a height of a polynomial we set, as before, $n_\nu = 1$ for finite or real places, and $n_\nu = 2$ for complex places. The height of the polynomial P is defined to be

$$h(P) = \frac{1}{[K : \mathbb{Q}]} \sum_\nu n_\nu M_\nu(P).$$

By the product formula we see that $h(\lambda P) = h(P)$ for any $\lambda \in K^\times$.

6.4 The Chow Form

To define the height of a projective variety we will need to associate a particular polynomial to the variety. There is a standard method in algebraic geometry which associates a hypersurface to a variety. The idea (see for instance Harris [19], Lecture 21) is to give a parameterised collection of hyperplanes such that their intersection describes the variety.

To be precise, let X be a variety of degree d and dimension k in $\mathbb{P}^N$. A hyperplane $U_j \subset \mathbb{P}^N$ may be identified with an element of $\mathbb{P}^N$ (i.e., the equation of U_j is $u_{0,j}x_0 + \dots + u_{N,j}x_N$ so we identify U_j with $[u_{0,j} : \dots : u_{N,j}]$). Consider the set $\Gamma = \{(p, U_1, \dots, U_{k+1}) \mid p \in X, p \in U_j \forall j\}$. This set projects, in the obvious manner, to the set of all hyperplanes whose intersection meets X. Indeed (see Harris [19]) it is possible to map Γ birationally to $\mathbb{P}^N \times \dots \times \mathbb{P}^N$ ($k+1$ times) and a dimensions argument shows that the variety obtained is a hypersurface (i.e., it is defined by a single polynomial). Any such choice of polynomial is called a **Chow form** (or Chow point) of the variety X. Note that the Chow form is unique, up to a scalar multiple, once a choice of embedding of X in $\mathbb{P}^N$ is given. The Chow form is multihomogeneous of degree $(d, \dots, d)$ in the $k+1$ sets $\underline{u}_j$ of $N+1$ variables $\underline{u}_j = \{u_{0,j}, \dots, u_{N,j}\}$.

A slightly more concrete description of the Chow form, in the case where X is an irreducible curve, is given in Philippon [31] (he calls the Chow form a "forme éliminante" in this case). Suppose the dimension k variety, X, is given by the zero locus of a $\mathbb{C}[\underline{x}]$-ideal $\mathcal{I}$. Let $\underline{u}$ be the set of variables $u_{i,j}$ where $0 \le i \le N$ and $1 \le j \le k+1$. Write, as before, $U_j = u_{0,j}x_0 + \dots + u_{N,j}x_N$. Now define the $\mathbb{C}[\underline{u}]$-ideal

$$\mathcal{C}(\mathcal{I}) = \{f \in \mathbb{C}[\underline{u}] \mid f.(x_0, \dots, x_N)^m \subseteq (\mathcal{I}, U_1, \dots, U_{k+1}) \text{ for some } m\}.$$

Note here that the ideal $(\mathcal{I}, U_1, \dots, U_{k+1})$ is a $\mathbb{C}[\underline{x}, \underline{u}]$-ideal. The ideal $\mathcal{C}(\mathcal{I})$ can be shown to be principal. Any generator of it is a Chow form.

Let us come down to earth and consider the case of a curve $X \subset \mathbb{P}^2$ described by a single polynomial $g(x_0, x_1, x_2)$. Here $k = 1$ so we have $U_1 = u_{0,1}x_0 + u_{1,1}x_1 + u_{2,1}u_2$ and similarly for U_2. We have the following relations

$$\begin{aligned} v_1 &:= u_{2,2}U_1 - u_{2,1}U_2 &= (u_{2,2}u_{0,1} - u_{0,2}u_{2,1})x_0 + (u_{2,2}u_{1,1} - u_{1,2}u_{2,1})x_1 \\ v_2 &:= u_{1,2}U_1 - u_{1,1}U_2 &= (u_{1,2}u_{0,1} - u_{1,1}u_{0,2})x_0 + (u_{1,2}u_{2,1} - u_{1,1}u_{2,2})x_2. \end{aligned} \tag{6.3}$$

Thus it is possible to "replace" all occurrences of the variables x_1 and x_2 in g by x_0, while all the time working in the ideal $(g, U_1, \ldots, U_{k+1})$.

We give an example. Let $X = X_0(64)$, so that $g(x_0, x_1, x_2) = x_0^4 + 6x_0^2x_1^2 + x_1^4 - 8x_2^4$. To remove the term x_2^4, for instance, we use the second relation in (6.3). It is clear that

$$(u_{1,2}u_{2,1} - u_{1,1}u_{2,2})^4 g(x_0, x_1, x_2) + 8v_2^4$$

will have no x_2^4 terms. Note that we have added terms such as $x_0x_2^3$ in the process, but these have lower degree in x_2. Thus the process may be repeated until only x_0 remains (and it will necessarily have degree 4). The calculation is quite horrible. The following combination eliminates all x_1 and x_2.

$$\begin{aligned} &g(x_0, x_1, x_2)(u_{1,1}u_{2,2} - u_{1,2}u_{2,1})^4 + 8v_2^4 - v_1^4 - 32x_0v_2^3(u_{1,2}u_{0,1} - u_{0,2}u_{1,1}) \\ &-4x_0v_1^3(u_{0,2}u_{2,1} - u_{2,2}u_{0,1}) + 48x_0^2v_2^2(u_{0,1}u_{1,2} - u_{0,2}u_{1,1})^2 \\ &-6x_0^2v_1^2((u_{2,2}u_{0,1} - u_{0,2}u_{2,1})^2 + (u_{1,1}u_{2,2} - u_{2,1}u_{1,2})^2) - 32x_0^3v_2(u_{1,2}u_{0,1} - u_{0,2}u_{1,1})^3 \\ &+4x_0^3v_1((u_{2,2}u_{0,1} - u_{2,1}u_{0,2})^3 + 3(u_{2,2}u_{0,1} - u_{2,1}u_{0,2})(u_{1,1}u_{2,2} - u_{1,2}u_{2,1})^2) \end{aligned}$$

The result of this is x_0^4 multiplied by the polynomial $f[\underline{u}] \in \mathbb{C}[\underline{u}]$ which has multihomogeneous degree $(4, 4)$.

$$\begin{aligned} f[\underline{u}] = {} & u_{2,2}^4u_{0,1}^4 - 8u_{1,2}^4u_{0,1}^4 + 32u_{1,2}^3u_{0,2}u_{1,1}u_{0,1}^3 - 4u_{2,2}^3u_{0,2}u_{2,1}u_{0,1}^3 \\ &-48u_{1,2}^2u_{0,2}^2u_{1,1}^2u_{0,1}^2 + 6u_{2,2}^4u_{1,1}^2u_{0,1}^2 - 12u_{2,2}^3u_{1,2}u_{2,1}u_{1,1}u_{0,1}^2 + 6u_{2,2}^2u_{0,2}^2u_{2,1}^2u_{0,1}^2 \\ &+6u_{2,2}^2u_{1,2}^2u_{2,1}^2u_{0,1}^2 + 32u_{1,2}u_{0,2}^3u_{1,1}^3u_{0,1} - 12u_{2,2}^3u_{0,2}u_{2,1}u_{1,1}^2u_{0,1} \\ &+24u_{2,2}^2u_{1,2}u_{0,2}u_{2,1}^2u_{1,1}u_{0,1} - 4u_{2,2}u_{0,2}^3u_{2,1}^3u_{0,1} - 12u_{2,2}u_{1,2}^2u_{0,2}u_{2,1}^3u_{0,1} - 8u_{0,2}^4u_{1,1}^4 \\ &+u_{2,2}^4u_{1,1}^4 - 4u_{2,2}^3u_{1,2}u_{2,1}u_{1,1}^3 + 6u_{2,2}^2u_{0,2}^2u_{2,1}^2u_{1,1}^2 + 6u_{2,2}^2u_{1,2}^2u_{2,1}^2u_{1,1}^2 \\ &-12u_{2,2}u_{1,2}u_{0,2}^2u_{2,1}^3u_{1,1} - 4u_{2,2}u_{1,2}^3u_{2,1}^3u_{1,1} + u_{0,2}^4u_{2,1}^4 + 6u_{1,2}^2u_{0,2}^2u_{2,1}^4 + u_{1,2}^4u_{2,1}^4. \end{aligned}$$

One important observation to make is that the coefficients of the Chow form $f[\underline{u}]$ are at worst 4 or 6 times those of $g(x_0, x_1, x_2)$. The reason for this is given by the following lemma.

Lemma 11 *Suppose $X \subset \mathbb{P}^2$ is a curve of degree 4 defined by $g(x_0, x_1, x_2)$. Let g_p and f_p be the maximum of the p-adic norms of the coefficients of g and the Chow form f of g respectively. Then $f_2 \leq 4g_2$, $f_3 \leq 3g_3$ and $f_p = g_p$ for all primes $p > 3$.*

Proof. The polynomial g may be written as

$$\sum_{i+j+k=4} a_{i,j,k}x_0^ix_1^jx_2^k$$

where $i, j, k \geq 0$. To eliminate the variables x_1 and x_2, one uses the elements v_1 and v_2 (see equation (6.3)) which lie in the ideal. Write these as $v_1 = \alpha x_0 + \beta x_1$ and $v_2 = \gamma x_0 - \beta x_2$, where

$\alpha = u_{2,2}u_{0,1} - u_{0,2}u_{2,1}$, $\beta = u_{2,2}u_{1,1} - u_{1,2}u_{2,1}$ and $\gamma = u_{1,2}u_{0,1} - u_{0,2}u_{1,1}$. The polynomial $\beta^4 g(x_0, x_1, x_2)$ is equal (in the quotient ring $\mathbb{C}[x_0, x_1, x_2, \underline{u}]/(g, U_1, \dots, U_{k+1})$) to

$$\sum_{i+j+k=4} a_{i,j,k}\beta^i(-\alpha)^j\gamma^k x_0^4. \tag{6.4}$$

The term $\beta^i\alpha^j\gamma^k$ contains terms

$$u_{0,1}^{j_1+k_1}u_{2,2}^{i_1+j_1}u_{0,2}^{j_2+k_2}u_{2,1}^{i_2+j_2}u_{1,2}^{i_2+k_1}u_{1,1}^{i_1+k_2} \tag{6.5}$$

where $i = i_1 + i_2$, $j = j_1 + j_2$ and $k = k_1 + k_2$. We want to know when there can be two different sets of powers $i_1, i_2, j_1, j_2, k_1, k_2$ which give the same monomial in (6.5). Fix such a choice of monomial and write it as $u_{0,1}^a u_{2,2}^b u_{0,2}^c u_{2,1}^d u_{1,2}^e u_{1,1}^f$ so that $a = j_1 + k_1$ etc. Suppose there two different ways of obtaining this monomial in the form (6.5), and write the corresponding powers as $i_1, \dots, k_2$ and $i'_1, \dots, k'_2$. It follows that $j_1 \neq j'_1$ and $j_2 \neq j'_2$ (and, indeed, all the other pairs are non-equal too). It is easy to obtain the following relations (and more).

$$j_1 = a - k_1 \qquad i_1 = b - a + k_1 \qquad j_2 = c - k_2$$

$$i_2 = d - c + k_2 \qquad i_1 = f - k_2 \qquad i_2 = e - k_1.$$

From these relations one sees that, to get a non-unique solution to (6.5), one would need $1 \leq a, b, c, d, e, f$. Furthermore, it is clear that $a + b + c + d + e + f = 8$. Suppose one of these variables, say a, is at least 3. Then one of j_1 and k_1 is at least 2, and thus b or e is at least 2, but this would give a sum larger than 8. Therefore, if a monomial arises in a non-unique way, then $1 \leq a, b, c, d, e, f \leq 2$. From the above relations one may also deduce that $i = i_1 + i_2 = b + e - a$, $j = a + d - e$ and $k = a + f - b$. and, therefore, a monomial can arise in a non-unique way only for a single choice of i, j and k.

When taking monomials of an arbitrary form using (6.4), the coefficients will grow from taking powers. Since $0 \leq i, j, k \leq 4$ the powers can introduce only extra factors of 2,3,4 or 6. From the discussion in the first part of the proof, if there is non-uniqueness in the calculation of the monomial then it only occurs within a particular choice of i, j, k, and the extra multiples introduced by taking powers are at most 2. Therefore combining such terms does not change the coefficients by more than a factor of 2 or 4. In particular, different $a_{i,j,k}$ do not get combined by this process. Therefore the coefficients of the Chow form are simply multiples (by 1,2,3,4 or 6) of the coefficients of the original model. □

This lemma may be viewed as a low-dimensional coincidence. For curves in $\mathbb{P}^n$ (where $n > 2$), which are defined as intersections of higher dimensional varieties, then there will not, in general, be such a strong correlation between the coefficients of the Chow form and those of the original equations. This difficulty will become relevant in later sections when we try to use the Philippon height as a framework for the analysis of the coefficient size of models for curves.

6.5 Heights of Projective Varieties

It is now possible to associate a height to a projective variety. The method discussed in this section is to take the Philippon height of the Chow form of the variety. This was developed in [31], though we follow the presentation in Soulé [39].

There is another method of defining a height on projective varieties which was introduced by Faltings [12]. It is modelled on the definition of the degree of a projective variety. One of the ways to compute the degree of a projective variety is to use intersection theory (see Fulton [16] page 42). Faltings adapted this definition by using Arakelov intersection theory. We will not give details about the definition of the Faltings height. In the next section we will discuss the relationship between these two different notions of height.

Let X be an irreducible variety of degree d and dimension n in $\mathbb{P}^N_K$. Let F be the Chow form of X. As we have seen this is a homogeneous polynomial of multidegree $(d, \ldots, d)$ in the variables $U_j = \{u_{0,j} \ldots u_{N,j}\}$ where $j = 1, \ldots, n+1$. Take $\mathbb{S} = \{z \in \mathbb{C}^{N+1} | \sum_i |z_i|^2 = 1\}$ with measure $d\mu$.

For the infinite places $\sigma : K \hookrightarrow \mathbb{C}$ we consider

$$\int_{\mathbb{S}^{n+1}} log|\sigma F| d\mu.$$

For the finite places ν we consider the maximum of the ν-adic norm of the coefficients of the Chow form F.

Definition 12 *The* **Philippon height** *of X is defined to be*

$$h_P(X) = \sum_{\nu \nmid \infty} log\, max_J |F_J|_\nu + \sum_{\sigma : K \hookrightarrow \mathbb{C}} \int_{\mathbb{S}^{n+1}} log|\sigma F| d\mu$$

where J indexes all the coefficients of the Chow form F of X.

From the statement of Lemma 11, and from the equations for $X_0(N)$ calculated in Chapter 3, one can give bounds for the height of some of the curves $X_0(N)$ (and $X_0(N)/W_n$). The accuracy of these estimates depends mainly on the estimation of the integral (i.e., the component at the infinite places). We have not explored the subject of estimating integrals in this chapter as there is no obvious reason, at this stage, why estimates of $h(X_0(N))$ for known curves would be useful. Instead we concern ourselves with trying to link heights of projective varieties with other parts of arithmetic geometry.

6.6 Comparing Heights

We have been very vague about the Faltings height of projective varieties. Philippon [31] and Soulé [39] have been able to explicitly relate the Faltings height with the Philippon height. Such a situation was already alluded to by Faltings in Corollary 2.12 of [11]. In this section we write down the relation between these two heights. For the purposes of this thesis, one may as well define the Faltings height to be the right hand side of equation (6.6) below.

The Philippon height is suitable for practical use as it has a very explicit description. The Faltings height is a more theoretical notion, and it is useful as one may apply geometric techniques to prove statements about it. An important intuition to keep in mind is that heights of projective varieties behave in a similar way to degrees. This is quite clear from the definition of the Faltings height of a projective variety.

Theorem 5 *(See Soulé [39] Theorem 3). Let $X \subset \mathbb{P}^N_K$ be an irreducible variety of dimension n and degree d. Then*

$$h_F(X) = h_P(X) + \frac{1}{2}(n+1)\left(\sum_{j=1}^{N} \frac{1}{j}\right)[K : \mathbb{Q}]deg(X). \tag{6.6}$$

We emphasise that, although both these heights are related by (6.6), they both also depend on the choice of embedding of X in $\mathbb{P}^N$.

It would be very nice to have some relation between these heights and a more intrinsic height associated to the curve X. In particular it would be very useful to have a relation between the height of the projective variety X and the height (as an abelian variety) of its Jacobian variety $Jac(X)$.

In the next section we will discuss the case of elliptic curves. We know that the Philippon height $h_P(E)$ depends on the coefficients of the projective model for the curve E. In the next section we will prove (Corollary 1) that, for a certain special class of elliptic curves E, the height of $Jac(E) \cong E$ as an abelian variety depends only on the particular τ corresponding to E. There does not seem to be an obvious connection between the size of τ and the size of the coefficients of E. This leads us to suspect that a relation between $h_P(E)$ and $h(E)$ may be rather difficult to understand.

6.7 Computation of a Height for Elliptic Curves

The article of Silverman [38] gives a concrete illustration of the theory of heights of abelian varieties by stating all the results in the context of elliptic curves. Our intention in this section is to provide a companion discussion, this time giving an illustration for the theory of heights of projective varieties.

In this section we will also specialise the discussion to the case where we are working over $K = \mathbb{Q}$. There is no real theoretical saving compared to working over a general number field but this restriction will allow us to recognise some expressions more easily.

We begin by recapitulating some of the results about the height of an elliptic curve E when it is considered as an abelian variety.

6.7.1 Elliptic Curves as Abelian Varieties

Silverman's paper [38] gives an explicit analysis of the height of an elliptic curve E. The primary result ([38] Proposition 1.1) is that, for an elliptic curve $E/\mathbb{Q}$ with minimal discriminant Δ_E,

$$h(E) = \frac{1}{12}\left[log|\Delta_E| - log\left(|\Delta(\tau)|(Im\,\tau)^6\right)\right] \tag{6.7}$$

where $\tau \in \mathcal{H}$ is such that $E \cong E_\tau$ and where $\Delta(\tau)$ is the usual modular form of weight 12.

At first glance this supports the idea that the height depends on the coefficients of a small model (i.e., the model having minimal discriminant Δ_E). We have found a corollary to (6.7) which demonstrates that the height of E actually depends more on the modular interpretation.

Corollary 1 *Suppose $E/\mathbb{Q}$ has a mimimal integral model of the form $E : y^2 = x^3 + Ax + B$. Suppose $\tau_0 \in \mathcal{H}$ is the specific τ which corresponds to this model for E (via the usual complex analytic map from $\tau \in \mathcal{H}$ to plane elliptic curves). Then*

$$h(E) = \frac{-1}{2} log(Im\,\tau_0).$$

Proof. The formulae in Silverman [35] Section III.1.3 and Chapter VI show how E and τ are related. The elliptic curve E is isomorphic to one of the form $(2y)^2 = 4x^3 + 4Ax + 4B$ and it is known that there is some $\tau_0 \in \mathcal{H}$ such that $g_2(\tau_0) = -4A, g_3(\tau_0) = -4B$ where g_2, g_3 are the usual modular forms (see Silverman [35] VI.3). It follows that $\Delta(\tau_0) = \Delta_E$. Substituting $\tau = \tau_0$ in equation (6.7) gives

$$h(E) = \frac{1}{12}\left[log|\Delta_E| - log\left(|\Delta_E|(Im\,\tau_0)^6\right)\right] = \frac{1}{12} log\left|\frac{\Delta_E}{\Delta_E(Im\,\tau_0)^6}\right|$$

and the result follows. □

Note that the hypothesis in this corollary (that the minimal model for E is of the simplest form) is quite a restriction as it implies $\Delta_E = -16(4A^3 + 27B^2)$ and, therefore, that E has bad reduction at the prime 2.

Silverman gives several other approximations for $h(E)$. He demonstrates the expected relation, between the height of an abelian variety and the height of the corresponding point in the moduli space, in the formula $|h(j(E)) - 12h(E)| \leq 6log(1 + h(j(E))) + C$ where $h(j(E))$ is the usual height of a rational number.

For modular elliptic curves, Proposition 3.1 of Silverman [38] gives the well-known relation between the height of E and the degree of its modular parameterisation $\phi : X_0(N) \to E$. This relation is

$$\frac{1}{2} log\, deg(\phi) = h(E) + log\|f_E\| + log|c_E| \tag{6.8}$$

where f_E is the modular form associated to E, $\|f_E\|$ is its Petersson norm and where c_E is the Manin constant which is conjectured to be simply ± 1. This formula has been used by Cremona [9] to compute tables of the degrees of the modular parameterisations for a large number of modular elliptic curves.

Cremona [9] gives a comprehensive table of results. A glance through his tables quickly reveals the following pattern: If the model for E has large coefficients then the covering map must have high degree. Note that the tables of Cremona use the convention of writing elliptic curves as $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ where $a_1, a_3 \in \{0, 1\}$ and $a_2 \in \{0, \pm 1\}$. Indeed Silverman [38], Proposition 3.4 shows that, for each $\epsilon > 0$, there is some constant C_ϵ such that

$$deg\, \phi \geq C_\epsilon max\{|c_4|^{1/4}, |c_6|^{1/6}\}^{2-\epsilon}. \tag{6.9}$$

Here c_4 and c_6 are the usual quantities associated to a model for the elliptic curve E. To be precise, suppose $E : y^2 + a_1yx + a_3y = x^3 + a_2x^2 + a_4x + a_6$. Then $c_4 = a_1^4 + 8a_1^2a_2 - 24a_1a_3 + 16a_2^2 - 48a_4$ and $c_6 = -a_1^6 - 12a_1^4a_2 + 36a_1^3a_3 - 48a_1^2a_2^2 + 72a_1^2a_4 + 144a_1a_2a_3 - 64a_2^3 + 288a_2a_4 - 216a_3^2 - 864a_6$. Note that when $a_1 = a_2 = a_3 = 0$ these formulae collapse to $c_4 = -48a_4$ and $c_6 = -864a_6$. Equation (6.9) clearly justifies the pattern observed in Cremona's tables.

A relationship between the height of E and the degree of the modular parameterisation is already conjectured in the "degree conjecture" (see Frey [14]). This conjecture is related to the height conjecture and both conjectures imply the A-B-C conjecture (and thus Fermat's last theorem). We discuss the height conjecture (see Frey [14]) in more detail. In our case (restricting to elliptic curves over $\mathbb{Q}$) it becomes the following.

Height Conjecture. There are numbers $c, d \in \mathbb{R}$ such that, for all elliptic curves $E/\mathbb{Q}$, one has $h(E) \leq c + dlog(N_E)$ (here N_E is the conductor of E).

This conjecture may also be generalised to abelian varieties of higher dimension. Frey goes on to prove the result for elliptic curves over function fields.

6.7.2 Elliptic Curves as Projective Varieties

Suppose we have a model $y^2 = x^3 + ax + b$ for an elliptic curve E with coefficients in $\mathbb{Z}$. Certainly this may be viewed as a quasiprojective variety over $\mathbb{Q}$.

In this section we estimate the Philippon height of E. Certainly the component of the height at the finite places just depends on which primes divide a and b.

For the component of the height at the infinite places we consider the Chow form of the elliptic curve E. This may be calculated to be

$$\begin{aligned}
&-bu_{0,1}^3u_{1,2}^3 + u_{0,1}^3u_{2,2}^2u_{1,2} + 3bu_{0,1}^2u_{1,1}u_{0,2}u_{1,2}^2 - u_{0,1}^2u_{1,1}u_{2,2}^2u_{0,2} - au_{0,1}^2u_{1,1}u_{2,2}u_{1,2}^2 \\
&-2u_{0,1}^2u_{1,2}u_{2,1}u_{2,2}u_{0,2} + au_{0,1}^2u_{2,1}u_{1,2}^3 - 3bu_{0,1}u_{0,2}^2u_{1,2}u_{1,1}^2 + 2au_{0,1}u_{1,1}^2u_{0,2}u_{1,2}u_{2,2} \\
&+2u_{0,1}u_{0,2}^2u_{1,1}u_{2,1}u_{2,2} - 2au_{0,1}u_{1,1}u_{2,1}u_{1,2}^2u_{0,2} + u_{0,1}u_{0,2}^2u_{1,2}u_{2,1}^2 + bu_{0,2}^3u_{1,1}^3 \\
&-au_{0,2}^2u_{1,1}^3u_{2,2} - u_{1,1}^3u_{2,2}^3 + au_{1,1}^2u_{1,2}u_{0,2}^2u_{2,1} + 3u_{1,1}^2u_{1,2}u_{2,1}u_{2,2}^2 - u_{0,2}^3u_{1,1}u_{2,1}^2 \\
&-3u_{1,1}u_{1,2}^2u_{2,1}^2u_{2,2} + u_{1,2}^3u_{2,1}^3.
\end{aligned} \tag{6.10}$$

From this we estimate the integral $\int_{\mathbb{S}^2} log|F|d\mu$. Let $M = max\{|3b|, |2a|, |3|, |2|\}$ and note that there are 20 terms in the Chow form (6.10). For points $\underline{u} \in \mathbb{S}^{n+1}$ it is clear that all $|u_{i,j}| \leq 1$. A very crude estimate of the integral is therefore $\int_{\mathbb{S}^2} log|F|d\mu \leq log(20M)$.

For the finite places, the contribution to the height is

$$max\{2, |2a|_2, |b|_2\} + max\{3, |a|_3, |3b|_3\} + \sum_{p>3} max\{|a|_p, |b|_p\}.$$

If a and b are integers such that $ab \neq 0$ then we obtain

$$h_P(E) \leq log(6|ab|) + log(20M) \leq log\left(20(6ab)^2\right). \tag{6.11}$$

One knows that $N_E|\Delta_E$ and that $\Delta_E = 4a^3 + 27b^2$. In order to be able to apply the theory of the Philippon height to the height conjecture there are two difficulties to be overcome. The first, which we have already mentioned, would be to relate the height of E as a projective variety to its height as an abelian variety. The second obstacle is to relate the coefficients of the model for the elliptic curve to the conductor N_E. This second problem is probably insurmountable. Although the discriminant depends precisely on the coefficients of the elliptic curve in an explicit way, the size of the discriminant cannot usually be inferred from the size of the coefficients. For instance, the elliptic curve $E : y^2 + y = x^3 - x^2 - 7820x - 263580$ has level 11 and discriminant -11. Also, the level N_E may differ from Δ_E by a large amount. The difference between the size of N_E and the size of Δ_E may at least be bounded by the conjecture of Szpiro [42]. This conjecture (when restricted to the case of elliptic curves over $\mathbb{Q}$) states the following. For each $\epsilon > 0$, there is some constant C such that, for all elliptic curves $E/\mathbb{Q}$,

$$\Delta_E \leq C.N_E^{6+\epsilon}. \tag{6.12}$$

It seems that the study of heights of elliptic curves as projective varieties is probably not a suitable angle from which to attack the height conjecture for elliptic curves.

6.8 Rational Maps Between Varieties

In several places we have come across maps from the modular curve $X_0(N)$ to curves of smaller genus. An important example is the modular parameterisation of a rational elliptic curve E. Another example which has arisen in this thesis is the canonical quotient $X_0(p) \to X_0^+(p)$. It would be interesting to be able to understand how the heights of curves change across such rational maps.

Consider, for instance, the relationship given in equation (6.9) between $h(E)$ and the degree of the modular parameterisation $\phi : X_0(N) \to E$. If it were possible to infer the height $h(X_0(N))$ from $h(E)$ and $deg\,\phi$, then we could have a theoretical way to get bounds on $h(X_0(N))$.

In this section we consider the following slightly more general questions. Let f be a rational map of degree d between two projective curves X and Y. Given $h(X)$ and $deg(f)$ what can one say about $h(Y)$? Given $h(Y)$ and $deg(f)$ what can one say about $h(X)$?

Faltings [12] mentions the behaviour of the height under the operation of projection of a variety $X \subset \mathbb{P}^n$ from a point down to a variety in $\mathbb{P}^{n-1}$. To be precise, choose a point $x \in \mathbb{P}^n - X$ and let π be the projection of X from x to $\mathbb{P}^{n-1}$. Faltings calls π a "good projection" if it satisfies certain properties which, essentially, exclude projections which will allow the height to grow. Faltings then proves that ([12] Proposition 2.10)

$$h(\pi(X))deg\,\pi \leq h(X) + c \tag{6.13}$$

where c is a constant depending only on the degree of the variety X. This result suggests that heights should become smaller across rational maps. However the good projections studied by Faltings are not sufficiently general for our application.

For the more general case, the most promising angle of attack is the following. Suppose $X \subset \mathbb{P}^n_{\mathbb{Z}}$, $Y \subset \mathbb{P}^m_{\mathbb{Z}}$ and suppose that $f : X \to Y$ extends to a morphism $f : \mathbb{P}^n_{\mathbb{Z}} \to \mathbb{P}^m_{\mathbb{Z}}$. The heights of the projective varieties X and Y are computed using an analysis of metrized line bundles of the form $\overline{\mathcal{O}(1)}$. The precise definition involves expressions of the form $h(X) = deg\left(\hat{c}_1\left(\overline{\mathcal{O}(1)}\right).\hat{X}\right)$. It is known ([40] Theorem III.3 (iii) and Theorem IV.3 (i)) that $f_*\left(\hat{c}_1\left(f^*\overline{\mathcal{O}(1)}\right).\hat{X}\right) = \hat{c}_1\left(\overline{\mathcal{O}(1)}\right).f_*\hat{X}$. Also the pushforward $f_*\hat{X}$ is well-understood (see [40] Theorem III.3 (ii)). Therefore one hopes to be able to compute a relation between $h(X)$ and $h(Y)$ using a careful analysis of the pushforwards and pullbacks, of certain metrized line bundles, along f.

The key is to understand $f^*\overline{\mathcal{O}(1)}$ where $\overline{\mathcal{O}(1)}$ is the canonical metrized line bundle on $\mathbb{P}^m_{\mathbb{Z}}$. The behaviour at the metrics over the infinite place is not the real problem here. The main challenge is to understand the geometry. It is known (Hartshorne [20] Theorem II.7.1) that $f^*(\mathcal{O}(1))$ is a line bundle on $\mathbb{P}^n_{\mathbb{Z}}$ which is generated by $m+1$ global sections (namely the inverse images of the $m+1$ global sections which generate $\mathcal{O}(1)$ on $\mathbb{P}^m_{\mathbb{Z}}$). In the applications we will have $n > m$ so this shows that $f^*\mathcal{O}(1)$ cannot be equal to $\mathcal{O}(1)$. What, then, is this pullback? No progress was made with understanding these questions.

The hope would be that, despite the fact that $f^*(\mathcal{O}_{\mathbb{P}^m}(1)) \neq \mathcal{O}_{\mathbb{P}^n}(1)$, there is a way to manipulate the line bundles in a suitably controlled way, so that one may still understand the relation between $h(X)$ and $h(Y)$.

The parallelism between heights and degrees suggests we consider the behaviour of the degrees of projective varieties under rational maps. There does not seem to be any simple relation in this case. The most obvious example of such a relation is the Hurwitz formula which relates the genus of projective curves X and Y to the degree of the map $f : X \to Y$ between them. The genus is related to the degree but, again, the precise relation is quite complicated. It seems that what we are looking for is some kind of "arithmetic" analogue of the Hurwitz formula. One would expect this to be quite difficult to analyse.

It seems that there are no further techniques available to easily relate $h(X)$ with $h(Y)$. Indeed this question seems harder than it might appear. We suffice to examine a few examples.

One noteworthy example is the case of the genus 4 curve $X_0(61)$. The canonical model for $X_0(61)$ given in Chapter 3 is the following.

$$w^2 - x^2 + 2xy - 6xz + 3y^2 + 6zy - 5z^2 = 0 \tag{6.14}$$

$$x^2z + xy^2 + xyz + 5xz^2 + 4y^2z + 5yz^2 + 6z^3 = 0 \tag{6.15}$$

It can be shown that $X_0^+(61)$ is an elliptic curve, and it is given by simply equation (6.15). The quotient map from the canonical curve $X_0(61) \subset \mathbb{P}^3$ to $\mathbb{P}^2$ simply "forgets" the variable w and equation (6.14). Let us compare the Philippon heights of the two curves. The Chow form for $X_0(61)$ will be extremely complicated. I have not been able to calculate explicit expressions for any Chow forms of varieties in $\mathbb{P}^3$, as the presence of extra variables makes the calculation vastly more tedious. The Chow form will have multidegree $(6, 6)$ in the two sets of 4 variables. The relationship between the coefficients of the model for $X_0(61)$ and the coefficients of its Chow form is also less transparent in this case. The Chow form of the canonical curve $X_0^+(61)$ will be much less horrible but, nevertheless, related to that of $X_0(61)$. The coefficients of (6.15) are larger at the finite places than those of (6.14), so one might expect that the Chow forms will have the same valuation at the finite places (at the primes 2, 3 and 5 the valuation may be larger on $X_0(61)$ as there is a 6th power compared with the powers of 3 for the $X_0^+(61)$ case). The difference in the heights will then come down to the difference between the integrals of the two Chow forms. The relationship between the integrals of the Chow forms is not clear.

This example shows a difficulty in the use of the Philippon height. When looking at equations (6.14) and (6.15) one is tempted to say that the heights of both $X_0(61)$ and $X_0^+(61)$ are the same (as they have the same "worst" coefficients). However their Chow forms are very different and it is not clear how the integrals of the Chow forms are related.

In many cases we have been able to compute a model for $X_0^+(p)$ when the whole curve $X_0(p)$ is out of reach. Does the fact that the model for $X_0^+(p)$ has small height reflect on the model for $X_0(p)$?

In earlier sections we noted how the coefficient size of a rational elliptic curve E depends on the degree of its modular parameterisation $\phi : X_0(N) \to E$. This fact suggests that the coefficient size should grow, in general, across rational maps. This is the opposite of Faltings' statement (6.13) about good projections. It is evident that there are some subtleties in this problem.

As mentioned earlier, it would be useful to have a better theory about the behaviour of the heights of projective varieties across rational maps. Also it would be useful to have a better understanding about how the heights at the infinite places behave.

Chapter 7

Rational Points on Modular Curves

The study of rational points on curves is central to number theory. For modular curves, since their points have an interpretation as interesting objects in their own right, the study is even more important. For instance, Mazur [24] classified the possible torsion groups of elliptic curves over the rationals by a study of which curves $X_1(N)$ have non-cuspidal rational points.

7.1 Rational Points on $X_0(N)$

The modular curve $X_0(N)$ will always have some rational points coming from cusps. If the genus of $X_0(N)$ is zero then there will be an infinite number of rational points on $X_0(N)$. Mazur [24] classified all the non-cuspidal rational points of $X_0(p)$. This programme was continued by Kenku and others. When the dust settled the conclusion was that $X_0(N)$ has both genus $g \geq 1$ and a number $n_N \geq 1$ of non-cuspidal rational points for precisely those N listed in the following table (see Kenku [23]).

Table 6. Number of points on $Y_0(N)(\mathbb{Q})$

N	11	14	15	17	19	21	27	37	43	67	163
n_N	3	2	4	2	1	4	1	2	1	1	1

The explanation for these rational points is the following. The cases $N = 11, 19, 27, 43, 67$ and 163 correspond to modular curves with Heegner points over $\mathbb{Q}$. These Heegner points arise from elliptic curves with complex multiplication by the orders in $\mathbb{Q}(\sqrt{-N})$ of class number one. Note that the class number one discriminants $D = -3, -4, -7, -8, -12, -16$ correspond to genus zero modular curves. There is one further class number 1 discriminant, namely $D = -28$. However, there are no points on $X_0(28)$ arising from Heegner points with complex multiplication by the order of discriminant -28, because the equation $B^2 - 112C = -28$ is insoluble subject to $(28, B, C) = 1$. In later sections we will introduce Heegner points and show why this equation is important.

The curves $X_0(N)$ where $N = 11, 14, 15, 17, 21, 37$ are well-known for having exceptional rational isogenies. For instance, the curve $X_0(37)$ has 2 rational cusps and it is hyperelliptic. The hyperelliptic involution is defined over $\mathbb{Q}$, but it does not come from the action of an element of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathcal{H}$. The images of the cusps under the hyperelliptic involution must be distinct rational points, and it turns out that neither of these rational points are cusps.

Therefore one obtains two exceptional rational points on $X_0(37)$.

Three of these examples ($N \in \{37, 43, 67\}$) have been calculated in earlier chapters. In the remainder of this section we will exhibit the rational points on our models of these curves.

For $X_0(37)$ we give all the details of the calculation. From the tables of weight 2 cusp forms we find two eigenforms of level 37, namely $h_1 = q - 2q^2 - 3q^3 + \cdots$ and $h_2 = q + q^3 + \cdots$. We note that $h_1|W_{37} = h_1$ and $h_2|W_{37} = -h_2$. Setting $f = h_1$, $g = (h_2 - h_1)/2 = q^2 + 2q^3 + \cdots$, $X = f$, $Y = (gdf - fdg)/g^2 = q^{-1} + 7q + \cdots$ and $Z = g$ yields the following equation for $X_0(37)$.

$$Y^2Z^4 = X^6 + 20X^5Z + 120X^4Z^2 + 348X^3Z^3 + 544X^2Z^4 + 444XZ^5 + 148Z^6$$

Note that the change of variable $X = U - 1$ gives the equation listed in Table 3 of Chapter 4.

To compute the image of the cusp at infinity under this projective mapping we consider $[X : Y : Z] = [q + \cdots : q^{-1} + \cdots : q^2 + \cdots]$. Multiplying by q and evaluating at $\tau = i\infty$ (i.e., $q = 0$) gives the point [0:1:0].

To compute the image of the cusp zero we must act on the functions X, Y and Z by W_{37}. Note that $X|W_{37} = X$, $Z|W_{37} = -X - Z$ and $Y|W_{37} = -YZ^2/(X + Z)^2 = -q + \cdots$. Thus $[X|W_{37} : Y|W_{37} : Z|W_{37}] = [q + \cdots : -q + \cdots : -q + \cdots]$. Dividing by q and evaluating at $\tau = i\infty$ gives the point [1:$-$1:$-$1].

There are also two non-cuspidal points on $X_0(37)$. These are the images of the cusps under the hyperelliptic involution (which just maps the Y coordinate to $-Y$). For the point [$-$1:1:1] the image under the hyperelliptic involution is [1:1:$-$1]. For the point [0:1:0] the image under the hyperelliptic involution is the same point [0:1:0]. The reason why there are two points at infinity is the following. The curve $X_0(37)$ is a smooth projective curve of genus 2 and thus it does not have a non-singular projective model in $\mathbb{P}^2$. The model we are calling an "equation for $X_0(37)$" is actually the projection of a good model down to $\mathbb{P}^2$, and this projection cannot be an isomorphism. Indeed it maps a pair of points to the singular point [0:1:0] (see Section 2.6). We stick to the convention of not worrying about the fact that our models are singular, although it will be necessary later in this chapter to remember that there are two rational points [0:1:0] on genus two curves in general.

For $X_0(43)$ it is fairly easy to show that we have the point [1:1:0] corresponding to the cusp at infinity and the point [1:$-$1:0] corresponding to the cusp zero. One may then find the point [0:4:$-$3] corresponding to the non-cuspidal point by a simple brute-force search.

For $X_0(67)$ the point [1:0:1:1:0] corresponds to the cusp infinity, the point [$-$1:0:1:1:0] corresponds to the cusp zero and the point [0:0:-7:12:2] is the extra one. Under the covering $X_0(67) \to X_0^+(67)$, given explicitly in Table 1 of Chapter 3, the extra point [0:0:$-$7:12:2] maps to the point $(-2, -7)$ on the affine hyperelliptic model. We will see later that the point [0:0:$-$7:12:2] must be a Heegner point which is fixed by W_{67}.

As the study of rational points on $X_0(N)$ is already fully understood we turn to the case of rational points on $X_0^+(p)$. This is a particularly interesting case as it is the one not studied by Momose [25], [26]. It is no more work to introduce the ideas for $X_0^+(N) = X_0(N)/W_N$ so we work with the greater generality.

7.2 Points of $X_0^+(N)$

The standard moduli interpretation of $Y_0(N)$ is that a point $\tau \in \Gamma_0(N)\backslash\mathcal{H}$ corresponds to the elliptic curve $E_\tau = \mathbb{C}/\langle 1, \tau\rangle$ (where $\langle 1, \tau\rangle = \mathbb{Z} + \mathbb{Z}\tau$) together with the fixed cyclic N-element subgroup $C_\tau = \left\langle \frac{1}{N}, \tau \right\rangle$. It is a fact that, for every elliptic curve E and every cyclic N-element subgroup C of E, there is some τ (unique up to $\Gamma_0(N)$) such that $E \cong E_\tau$ and such that C is mapped to C_τ under this isomorphism.

Equivalently we may interpret the pair (E, C) as a pair (E, E') where there is a given isogeny $\pi : E \to E'$ such that $\ker \pi = C$. Note that E' is determined, up to isomorphism, by E and C (see Silverman [35] Proposition III.4.12). Sometimes E and E' do not uniquely determine C, so it is necessary to always keep the particular isogeny π in mind. Note that $E_\tau / C_\tau = \mathbb{C}/\langle 1, \tau\rangle / \left\langle \frac{1}{N}, \tau \right\rangle = \mathbb{C}/\left\langle \frac{1}{N}, \tau \right\rangle \cong \mathbb{C}/\langle 1, N\tau\rangle$.

The involution W_N acts on $Y_0(N)$ by mapping τ to $-1/N\tau$. Therefore E_τ is mapped to $\mathbb{C}/\left\langle 1, \frac{-1}{N\tau}\right\rangle \cong \mathbb{C}/\langle 1, N\tau\rangle$ and C_τ is mapped to $\left\langle \frac{1}{N}, \frac{-1}{N\tau}\right\rangle \cong \langle 1, \tau\rangle$. Thus a point of $Y_0^+(N)$ may be interpreted as an unordered pair $\{E, E'\}$ of elliptic curves with specified cyclic N-isogenies $E \xrightarrow{\pi} E' \xrightarrow{\pi'} E$. We will often lazily write simply $E \xrightarrow{\pi} E'$ to represent a Heegner point since the dual isogeny is uniquely determined. We remark that $Y_0^+(N)$ is $\Gamma_0^*(N)\backslash\mathcal{H}$, where $\Gamma_0^*(N) = \Gamma_0(N) \cup W_N\Gamma_0(N)$.

Note that $X_0^+(N)$ will always have one particular rational point, namely the cusp at infinity. Since the cusps correspond to generalised elliptic curves they will not arise in the constructions given in the following sections.

7.3 Heegner Points

A **Heegner Point** of $Y_0(N)$ is a pair (E, E') of elliptic curves together with a cyclic N-isogeny $E \xrightarrow{\pi} E'$, such that both E and E' have complex multiplication by the same order $\mathcal{O}$.

We assume much of the theory of complex multiplication here. For future reference we quote a few key results.

Theorem 6 *(See Silverman [36] Theorem II.4.3 on page 122) Let E_τ be an elliptic curve with complex multiplication by $\mathcal{O}$ then $[K(j(\tau)) : K] = [\mathbb{Q}(j(\tau)) : \mathbb{Q}] = h_{\mathcal{O}}$ the class number of the order.*

For a given $\tau \in \mathcal{H}$, all the elliptic curves $E_{\gamma(\tau)}$, where $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, are isomorphic to E_τ over $\mathbb{C}$. There is a particular choice of elliptic curve, in the $\mathbb{C}$-isomorphism class, which is defined over $\mathbb{Q}(j(\tau))$. For instance, if $j \neq 0, 1728$, consider the model $E : y^2 + xy = x^3 - \frac{36}{j-1728}x - \frac{1}{j-1728}$ (see Silverman [35] Section III.1). Therefore we will always assume that the elliptic curves in question are defined over $\mathbb{Q}(j(\tau))$.

Also note that there are precisely $h_{\mathcal{O}}$ isomorphism classes of elliptic curves E having complex multiplication by $\mathcal{O}$. This correspondence may be seen by taking, for each ideal class $[\mathfrak{a}]$ of $\mathcal{O}$, the elliptic curve $E = \mathbb{C}/\mathfrak{a}$. We sometimes use this notation of ideals and write $j(\mathfrak{a})$ instead of $j(E)$.

We emphasise the above results in the class number 1 and 2 situations.

Corollary 2 *Suppose $\mathcal{O}$ has class number one. Then there is a unique elliptic curve E (up to isomorphism over $\mathbb{C}$) having complex multiplication by $\mathcal{O}$. For this elliptic curve E we have $j(E) \in \mathbb{Q}$ so we may consider E as being defined over $\mathbb{Q}$.*

Corollary 3 *Suppose $\mathcal{O}$ has class number two. Then there are two non-isomorphic elliptic curves, E_1 and E_2, each having complex multiplication by $\mathcal{O}$. Suppose K is the quadratic imaginary field associated to $\mathcal{O}$. Then $j(E_1), j(E_2) \notin K$ and if $\sigma \in Gal\,(K(j(E_1))/K)\backslash\{1\}$ then $j(E_1)^\sigma = j(E_2)$.*

We will use the notation of Gross [18]. Suppose $\mathcal{O}$ is an order in a quadratic imaginary field K and let its discriminant be $D < 0$. The **conductor** of the order is the number f such that D/f^2 is the discriminant of the full ring of integers of K. Equivalently, f is the largest integer such that $D/f^2 \equiv 0, 1 (\text{mod } 4)$. Then $K = \mathbb{Q}\left(\sqrt{D}\right) = \mathbb{Q}\left(\sqrt{D/f^2}\right)$. Let $\mathfrak{a}$ be a fractional ideal of $\mathcal{O}$ (we will write $[\mathfrak{a}]$ for the class of $\mathfrak{a}$ in $Pic(\mathcal{O})$, the ideal class group of $\mathcal{O}$). Then $E = \mathbb{C}/\mathfrak{a}$ is an elliptic curve with complex multiplication by $\mathcal{O}$.

In this Chapter we will be concerned with N-isogenies of curves such as E. We say that N **factors** in K if (N) may be written as a product of two ideals $(N) = \mathfrak{n}\mathfrak{n}'$ in K, such that both $\mathfrak{n}$ and $\mathfrak{n}'$ have norm equal to N and such that $\mathcal{O}/\mathfrak{n} \cong \mathbb{Z}/N\mathbb{Z}$. That N factors in K implies that all the rational primes dividing the square-free part of N either split or ramify in K. Later, in the case where N is prime, it will be necessary to distinguish between the split and ramified situations. Suppose N factors as $\mathfrak{n}\mathfrak{n}'$ in $\mathcal{O}$. Then the identity map on $\mathbb{C}$ induces an isogeny $\mathbb{C}/\mathfrak{a} \to \mathbb{C}/\mathfrak{a}\mathfrak{n}^{-1}$ which has cyclic N-element kernel $\mathfrak{a}\mathfrak{n}^{-1}/\mathfrak{a} \cong \mathcal{O}/\mathfrak{n} \cong \mathbb{Z}/N\mathbb{Z}$. We write $y = (\mathcal{O}, \mathfrak{n}, [\mathfrak{a}])$ to represent the Heegner point $E = \mathbb{C}/\mathfrak{a}$ which has complex multiplication by $\mathcal{O}$ and which has an isogeny with kernel $\mathfrak{n}$. We define $j(\mathfrak{a}) = j(E)$.

The Heegner point $y = (\mathcal{O}, \mathfrak{n}, [\mathfrak{a}])$ must correspond to some $\tau \in \mathcal{H}$. Indeed, write the $\mathbb{Z}$-module $\mathfrak{a}$ as $\langle \omega_1, \omega_2 \rangle$ where the ω_j are chosen so that the kernel of the isogeny is $\langle \omega_1/N, \omega_2 \rangle$. Then $\tau = \omega_2/\omega_1$ lies in K. Let A, B, C be coprime integers such that $A\tau^2 + B\tau + C = 0$. It can be shown that $B^2 - 4AC = D$. Furthermore, since $E' \cong E_{N\tau}$, it follows that $N\tau$ must also be quadratic imaginary of discriminant D. But $N\tau$ satisfies $A(N\tau)^2 + NB(N\tau) + N^2C = 0$ and this has discriminant N^2D, so it must be possible to factor out N. This means that $N|A$, i.e., $A = NA'$. So $N\tau$ is a root of $A'x^2 + Bx + NC = 0$ and $(A', B, NC) = 1$. Furthermore, any A', B, C such that $D = B^2 - 4NA'C$ and $(NA', B, C) = (A', B, NC) = 1$ will give rise to a Heegner point of $X_0(N)$.

Our main interest is in Heegner points on $X_0(N)/W_N$, and we will need to discuss the field of definition of them. It is also possible to understand the field of definition of Heegner points on $X_0(N)$ using the same ideas. This will not be needed in later work. We merely comment that every Heegner point which comes from a class number 1 order in a quadratic imaginary field K gives a point of $X_0(N)$ defined over K.

7.4 Heegner Points on $X_0^+(N)$

Suppose N factors in K. For each order, $\mathcal{O}$, of K we have $(N) = \mathfrak{n}\mathfrak{n}'$, where both $\mathfrak{n}$ and $\mathfrak{n}'$ have norm N. Suppose $y = (\mathcal{O}, \mathfrak{n}, [\mathfrak{a}])$ is a Heegner point of $X_0(N)$ with complex multiplication by $\mathcal{O}$. Write $E = \mathbb{C}/\mathfrak{a}$ and $E' = \mathbb{C}/\mathfrak{a}\mathfrak{n}^{-1}$ and recall that $j(\mathfrak{a}) = j(E)$ and $j(\mathfrak{a}\mathfrak{n}^{-1}) = j(E')$. Then the Atkin-Lehner involution W_N takes y to $(\mathcal{O}, \mathfrak{n}', [\mathfrak{a}\mathfrak{n}^{-1}])$. The pair $\{y, W_p(y)\}$ is a point on $X_0^+(N)$.

In this section the goal is to ascertain when such a Heegner point gives a rational point of $X_0^+(N)$. A point of $X_0^+(N)$ is rational if it is fixed by $Gal\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$. In this situation, it is clear that the Heegner point will be fixed by $Gal\left(\overline{\mathbb{Q}}/K(j(E))\right)$. Note that $K(j(E))/\mathbb{Q}$ is a Galois extension since, by the theory of complex multiplication, $K(j(E))$ is Galois over K (it is the ring class field of the order $\mathcal{O}$), and $K/\mathbb{Q}$ is a degree 2 extension. The purpose of this section is to examine, in detail, the action of $Gal\,(K(j(E))/\mathbb{Q})$ on these Heegner points.

Let σ be any non-trivial element of $Gal(K(j(E))/K)$, if there is one, and let ρ be the non-trivial element of $Gal(K/\mathbb{Q})$. Consider the action of these Galois conjugations on the Heegner point $y = (\mathcal{O}, \mathfrak{n}, [\mathfrak{a}])$. Following Gross [18] we see that

$$(\mathcal{O}, \mathfrak{n}, [\mathfrak{a}])^\rho = (\mathcal{O}, \mathfrak{n}', [\mathfrak{a}^\rho]).$$

Note that $\mathfrak{a}^\rho$ is a principal ideal if and only if $\mathfrak{a}$ is.

To understand the action of σ on y it is necessary to recall the Artin map. We restrict attention to the case where $\mathcal{O}$ has class number 1 or 2. Recall that $K(j(E))/K$ is the Hilbert class field (or ring class field, when $\mathcal{O}$ is not maximal) of K (i.e., it is the maximal extension of K which is unramified everywhere). In this case the Artin map is the only possible group isomorphism $\sigma[.] : Pic(\mathcal{O}) \to Gal(K(j(E))/K)$. Note that $\sigma \in Gal(K(j(E))/K)$ doesn't act on $\mathfrak{a} \subset K$ itself, this is why one must use the Artin map. For a more thorough picture of what is going on see Shimura [33] Chapter 5. The action of $Gal(K(j(E))/K)$ is given by

$$(\mathcal{O}, \mathfrak{n}, [\mathfrak{a}])^{\sigma[\mathfrak{b}]} = (\mathcal{O}, \mathfrak{n}, [\mathfrak{a}\mathfrak{b}^{-1}]).$$

If $\{y, W_N(y)\}$ is to give a rational point on $X_0^+(N)$ then it follows that both of the above expressions must be either $(\mathcal{O}, \mathfrak{n}, [\mathfrak{a}])$ or $(\mathcal{O}, \mathfrak{n}', [\mathfrak{a}\mathfrak{n}^{-1}])$.

In the class number 1 situation, σ is trivial, $j(\mathfrak{a}) = j(\mathfrak{a}\mathfrak{n}^{-1})$, and both elliptic curves are defined over $\mathbb{Q}$. Thus ρ switches the two expressions. Therefore the Heegner point will give a rational point of $X_0^+(N)$. Furthermore it follows that the points (or point) of $X_0(N)$ which lie above this Heegner point must be defined over K.

In the class number 2 situation, $j(\mathfrak{a})$ and $j(\mathfrak{a}\mathfrak{n}^{-1})$ are defined over $\mathbb{Q}(j(E))$. If $E \cong E'$ (i.e., $\mathfrak{n}$ is a principal ideal) then σ maps the Heegner point to a completely different one, while ρ swaps the two expressions around. Hence we obtain a point on $X_0^+(N)$ which is defined over a quadratic field.

If $E \ncong E'$ (i.e., the ideal $\mathfrak{n}$ of K is not principal) then E and E' are Galois conjugate and σ swaps the curves (though it does not necessarily swap the isogenies in the correct manner). There are now two cases. Firstly, if N ramifies as $\mathfrak{n}^2$ in K then ρ acts trivially and σ switches the Heegner points, and so we get a rational point of $X_0^+(N)$. If N does not ramify in K then ρ maps $(\mathcal{O}, \mathfrak{n}, [\mathfrak{a}])$ to $(\mathcal{O}, \mathfrak{n}', [\mathfrak{a}^\rho])$ which is a different Heegner point. Similarly, σ maps y to $(\mathcal{O}, \mathfrak{n}, [\mathfrak{a}\mathfrak{n}^{-1}])$ which is the companion of y^ρ. In this case we obtain a point of $X_0^+(N)$ which is defined over a quadratic extension.

The case where one obtains a rational point from a Heegner point of class number 2 is very rare. We now restrict to the case where $N = p$ is a prime. For p to ramify in an order $\mathcal{O}$ we need $p|D$ where D is the discriminant of the order $\mathcal{O}$. Stark has proved that there are precisely 18 quadratic imaginary fields having class number 2. There are 29 orders with class number two and their discriminants are $\{-15, -20, -24, -32, -35, -36, -40, -48, -51, -52, -60, -64, -72, -75, -88, -91, -99, -100, -112, -115, -123, -147, -148, -187, -232, -235, -267, -403, -427\}$. From this list it is seen that the only primes p which ramify are $2, 3, 5, 7, 11, 13, 17, 23, 29, 31, 37, 41, 47, 61, 89$. In all of these cases the genus of $X_0^+(p)$ is 0 or 1. Therefore we have proved the following theorem.

Theorem 7 *Let p be a prime such that $X_0^+(p)$ has genus at least 2. Then Heegner points corresponding to orders of class number 2 are never rational points of $X_0^+(p)$.*

We end this section by giving an example which shows a rational point on the genus one curve $X_0^+(61)$ which comes from a Heegner point of class number 2.

First note that $p = 61$ ramifies in the order $\mathcal{O}$ of discriminant $-427 = -7.61$ (this order is the full ring of integers of $\mathbb{Q}(\sqrt{-427})$). The point $\tau \in \mathcal{H}$ which is a root of $61\tau^2 + 61\tau + 17$ corresponds to the Heegner point of discriminant -427. Evaluating the weight 2 cusp forms x, y and z (see the tables in Chapter 3) at τ gives the point $[-30{:}8{:}3]$ on the model

$$x^2z + xy^2 + xyz + 5xz^2 + 4y^2z + 5yz^2 + 6z^3 = 0$$

for $X_0^+(61)$. This point corresponds to the two points $[\pm 3\sqrt{61}{:}-30{:}8{:}3]$ on $X_0(61)$ and we see that these points are defined over $K = \mathbb{Q}\left(\sqrt{-427}\right)$ as expected.

7.5 Rational Points from Heegner Points

We now combine the results of this Chapter with the explicit equations for modular curves found in Chapters 2 and 3. The aim is to produce a list of rational points, coming from Heegner points, on the curves $X_0^+(p)$ of genus at least 2.

Following the ideas of the previous section we have a method for finding explicit rational points on the embedding of $X_0^+(p)$ into $\mathbb{P}^n$. Namely, for each class number 1 discriminant $D < 0$ we find (as long as D is a square modulo $4p$) integers A, B, C (here A is what we called A' before) such that $B^2 - 4pAC = D$. Then evaluate the modular functions which give the embedding of $X_0^+(p)$ into $\mathbb{P}^n(\mathbb{C})$ at the value of $\tau \in \mathcal{H}$ such that $Ap\tau^2 + B\tau + C = 0$. We see that there is a single rational point for each of these τ.

Theorem 8 *Suppose D is the discriminant of a class number 1 quadratic order and suppose D is a square modulo $4p$. Then there is precisely one rational point on $X_0^+(p)$ corresponding to the Heegner point of discriminant D.*

So one gets a single Heegner point for each class number 1 quadratic order in which p factors. The corresponding elliptic curve E is defined over $\mathbb{Q}$ and is a fixed point of W_p on $X_0(p)$. Note that it doesn't correspond to a rational point of $X_0(p)$ as the cyclic p-element subgroup (the kernel of the p-isogeny) will not in general be defined over $\mathbb{Q}$. The corresponding points of $X_0(p)$ will be defined over $\mathbb{Q}\left(\sqrt{D}\right)$.

In the case of class number 2 discriminants, we saw that it was necessary for E and E' to be Galois conjugates. Therefore we would still only get one rational point for each discriminant. We will only consider the case where the genus of $X_0^+(p)$ is at least 2 and hence the class number 2 case does not occur.

Note that, by a result of Mazur ([24] Corollary 1.5 on page 143), $J_0^+(p)$ is torsion-free. Hence the rational points we find will yield points of inifinite order on the Jacobian of the genus 2 curve. It would be interesting to know if these points could be used to yield a set of generators for the Mordell-Weil group of the Jacobian.

7.6 Other Rational Points

We have seen that on $X_0^+(p)$ there is a rational cusp and also some rational points coming from Heegner points of class number 1. In a few cases we also get rational points coming from a Heegner point of class number 2. It is impossible to obtain rational points which are Heegner points of class number larger than 2. This is because such points will have at least 3 distinct Galois conjugates, and therefore a pair of them cannot be Galois invariant.

We may now ask if there are any other rational points on $X_0^+(p)$ and, if so, where they come from.

The first step is the following proposition.

Proposition 9 *Suppose $E \xrightarrow{\pi} E'$ corresponds to a rational point on $X_0^+(p)$ which is neither a cusp nor a Heegner point nor rational point of $X_0(p)$. Then E and E' do not have complex multiplication and neither E nor E' are defined over $\mathbb{Q}$.*

Proof. Since the point is not a cusp we know that E and E' are genuine elliptic curves. To be a rational point of $X_0^+(p)$ it follows that, for every $\sigma \in Gal\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$, we must have $E^\sigma \xrightarrow{\pi^\sigma} E'^\sigma$ equal to either $E \xrightarrow{\pi} E'$ or $E' \xrightarrow{\pi'} E$. Therefore either $E^\sigma \cong E$ and $\pi^\sigma \cong \pi$, or $E^\sigma \cong E'$ and $\pi^\sigma \cong \pi'$.

Suppose first that E is defined over $\mathbb{Q}$. If $j(E') \notin \mathbb{Q}$ then choose some $\sigma \in Gal\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$ which acts non-trivially on E'. The conjugate of $E \xrightarrow{\pi} E'$ by σ is $E \xrightarrow{\pi^\sigma} E'^\sigma$. Since $E'^\sigma \not\cong E'$ this contradicts the assumption that we have a rational point. Therefore E' is defined over $\mathbb{Q}$. An element $\sigma \in Gal\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$ takes $E \xrightarrow{\pi} E'$ to $E \xrightarrow{\pi^\sigma} E'$. If $\pi^\sigma = \pi$ for all σ then $\ker \pi$ is defined over $\mathbb{Q}$ and therefore we actually have a rational point on $X_0(p)$. Otherwise we must have $\pi^\sigma = \pi'$ for some σ and, therefore, $E \cong E'$. In this case $\pi \in \mathrm{End}(E)$ and so E has complex multiplication and is a Heegner point.

Now suppose $j(E) \notin \mathbb{Q}$. Then E must be defined over some quadratic field $L/\mathbb{Q}$ and E' must be E^σ for the non-trivial element $\sigma \in Gal(L/\mathbb{Q})$. The endomorphism ring of E is the same as the endomorphism ring of E^σ. Therefore, if E has complex multiplication by $\mathcal{O}$, then so does E' and this completes the proof. □

The only cases where the genus of $X_0^+(p)$ is at least 2 and where $X_0(p)$ has non-cuspidal rational points are for $p = 67$ or 163. In both these cases there is only one such point on $X_0(p)$. Therefore that point must be fixed by the involution W_p (since the action of this involution is defined over $\mathbb{Q}$). Thus the corresponding rational point on $X_0^+(p)$ is actually a Heegner point after all.

If $X_0^+(p)$ has genus zero then there are an infinite number of rational points. Slightly more interesting is the genus one case. If $X_0^+(p)$ has genus 1 then it isomorphic to $J_0^+(p)$ and Mazur has shown that this abelian variety is torsion free and has positive rank. Therefore there are an infinite number of rational points on it. In both these cases it must be that there are points which do not come from elliptic curves having complex multiplication.

If $X_0^+(p)$ has genus at least 2 then we know that it has only finitely many rational points. Momose [25], [26] has studied the cases of composite level N and has shown that, in certain cases, there are no rational points on $X_0(N)/W_N$ other than the expected cusps and complex multiplication points. We quote the statement of his theorem from [26].

Theorem 9 *([26] Theorem 0.1). Let N be a composite number. If N has a prime divisor p which satisfies both conditions (i) and (ii) below then $X_0(N)/W_N$ has no rational points other than cusps and complex multiplication points.*

(i) $p \geq 11$ *and* $p \neq 13, 37$.

(ii) $\#J_0^-(p)(\mathbb{Q})$ *finite.*

According to Momose, all primes $17 \leq p \leq 300$ satisfy the condition $\#J_0^-(p)(\mathbb{Q})$ finite except for possibly $p \in \{151, 199, 227, 277\}$. The justification for this is given in Mazur [24], on page (coincidently?) 151.

As a result of our calculations we will exhibit, for some primes p, points on $X_0^+(p)$ which are neither cusps nor Heegner points.

One wonders if there is an arithmetic interpretation of these exceptional rational points. It seems a peculiar state of affairs that, when the genus of $X_0^+(p)$ is 0 or 1, one gets an infinite number of such points but when the genus is at least 2 one gets almost none of them.

7.7 Tables for Genus 2 Curves

In this section we present the results of some computations of rational points on genus 2 curves arising from Heegner points. The cusp infinity will always be associated to one of the points [0:1:0], though we write the equations in affine form in the tables. The hyperelliptic involution is always $[x : y : z] \mapsto [x : -y : z]$, which is clearly defined over $\mathbb{Q}$. For the curves $X_0^+(p)$, the hyperelliptic involution does not come from the action of $\mathrm{SL}_2(\mathbb{Z})$ (this is unlike the $X_0(N)$ case, where Ogg [30] showed that $X_0(37)$ is the only example of a hyperelliptic modular curve whose hyperelliptic involution does not come from an element of $\mathrm{SL}_2(\mathbb{Z})$).

We list the discriminants D of suitable orders $\mathcal{O}$ (i.e., so that D is a square modulo p). The computation of suitable τ is elementary. The evaluation of the given modular forms at τ is, however, more involved, as the q-expansions do not usually have very good convergence. In general one finds that a q-expansion of about 80 terms will suffice in order to obtain a recognisable form for most of the Heegner points. Sometimes, though, the convergence is very bad. Even using 300 term q-expansions and optimising the choice of τ using the action of $\Gamma_0^*(p)$ does not allow us to calculate these points to even crude accuracy. In these cases we mark the Heegner point with a question mark. Note that since the modular functions should evaluate to a rational number we may get a feel for the error in our calculation by looking at the size of the imaginary part.

The model for the curve is that used in Chapter 4. Thus we have modular forms f and g with $X = f/g$ and $Y = dX/g$. The projective model $Y^2Z^4 = p_6(X, Z)$ corresponds to $X = f, Z = g$ and $Y = (gdf - fdg)/g^2$. Thus a point τ corresponds to $\infty = [0{:}1{:}0]$ if $X(\tau) = f(\tau)$ and $Z(\tau) = g(\tau)$ are very small compared with $Y(\tau)$. Care must be taken here as it is easy to mistakenly identify ∞ in this way. Set $d = gdf - fdg = -q^3 + \cdots$. It therefore follows that $d/f^3 = -1 + \cdots$. Thus, at the cusp $i\infty$, the function d/f^3 must take the value -1. For the "other" point which falls at ∞, the modular forms must behave in the same way. Therefore we recognise points at ∞ by checking to see that $d/f^3 = -1$. We use this criterion to confirm that our candidate τ does give the point ∞.

We have performed a search for all points $[X{:}Y{:}Z]$ on the projective model of the curve such that $X, Y, Z \in \mathbb{Z}$ and $|X|, |Y|, |Z| < 300$. Note that, in the genus 2 case, we tend to represent the points in affine form as (x, y) or as ∞. One suspects there will be no other rational points on these curves but I do not have the tools to show this. We list all the points found in the search which are not already listed as Heegner points.

One confidently expects that the question marks in the list of Heegner points may be filled with a suitable choice from among the points found by the brute-force search. Indeed, the correspondence may be deduced, in many cases, by lifting the rational points from $X_0^+(p)$ to $X_0(p)$ and then examining their field of definition.

An interesting case arises when there are points "left over". In these cases we genuinely have rational points which do not arise as Heegner points. It is clear from our computations that these points are very rare. Unfortunately we cannot "invert" our modular forms so we cannot find which τ correspond to these stray points. As a result we have no clues to the arithmetic interpretation of these points.

Table 7. Rational Points on Genus 2 $X_0^+(p)$

$X_0^+(67)$	$y^2 = x^6 + 2x^5 + x^4 - 2x^3 + 2x^2 - 4x + 1$			
	$D = -3$	$(-1,1)$	$D = -7$	$(0,1)$
	$D = -8$	$(0,-1)$	$D = -11$	∞
	$D = -12$	$(1,1)$	$D = -27$	$(-1,-3)$
	$D = -28$	$(-2,-7)$	$D = -43$	$(1,-1)$
	$D = -67$	$(-2,7)$ (from $X_0(67)(\mathbb{Q})$)		
$X_0^+(73)$	$y^2 = x^6 + 2x^5 + x^4 + 6x^3 + 2x^2 - 4x + 1$			
	$D = -3$	$(\frac{1}{2},\frac{5}{8})$	$D = -4$	$(-1,-1)$
	$D = -8$	$(0,-1)$	$D = -12$	∞
	$D = -16$	$(1,-3)$	$D = -19$	$(0,1)$
	$D = -27$	$(-1,1)$	$D = -67$	$(1,3)$
	$(\frac{1}{2},-\frac{5}{8})$			
$X_0^+(103)$	$y^2 = x^6 + 6x^5 + 5x^4 + 2x^3 + 2x^2 + 1$			
	$D = -3$	$(2,-19)$	$D = -11$	$(0,1)$
	$D = -12$	$(0,-1)$	$D = -27$	$(-1,1)$
	$D = -43$	$(-1,-1)$	$D = -67$	∞
	$(2,19)$			
$X_0^+(107)$	$y^2 = x^6 + 2x^5 + 5x^4 + 2x^3 - 2x^2 - 4x - 3$			
	$D = -7$	$(1,-1)$	$D = -8$	∞
	$D = -28$	$(-1,1)$	$D = -43$	$(1,1)$
	$D = -67$	$(-1,-1)$		
$X_0^+(167)$	$y^2 = x^6 - 4x^5 + 2x^4 - 2x^3 - 3x^2 + 2x - 3$			
	$D = -43$	∞	$D = -67$	$(-1,-1)$
	$D = -163$	$(-1,1)$		
$X_0^+(191)$	$y^2 = x^6 + 2x^4 + 2x^3 + 5x^2 - 6x + 1$			
	$D = -7$	$(0,1)$	$D = -11$	$(0,-1)$
	$D = -19$	∞	$D = -28$	$(2,11)$
	$(2,-11)$			

So $X_0^+(73)$, $X_0^+(103)$ and $X_0^+(191)$ each have an extra rational point and, as we have shown, this cannot come from a Heegner point or a complex multiplication point. In the case of $X_0^+(73)$

we may trace (from the tables in Chapter 3) the point $(\frac{1}{2}, \frac{-5}{8})$ back to $[\sqrt{-127}{:}-2\sqrt{-127}{:}-3{:}19{:}2]$ on $X_0(73)$ and so it follows that this point is the non-Heegner point as it isn't defined over any of the fields having class number one discriminant.

7.8 Tables for Higher Genus Curves

We now perform a similar analysis for curves $X_0^+(p)$ of genus $3 \leq g \leq 5$. In all cases the points given lie on the model (using eigenforms) listed in Chapter 2.

First we consider genus 3 curves $X_0^+(p)$. Once again we have occasional trouble with convergence of the q-expansions. Nevertheless we compute points corresponding to most of the applicable discriminants and we perform a search over all integral points $[X : Y : Z]$ with $|X|, |Y|, |Z| < 300$. We assume, as before, that the points with bad convergence (marked with a "?") can be paired with the unmatched points found in the search. We find that all the rational points arise as either the cusp (in this case always [1:0:0]) or as a Heegner point. So there are no exceptional points in these cases.

Note that, in this case, our modular parameterisation really is projective. Therefore the modular forms do not evaluate to rational numbers themselves, but taking ratios yields easily recognised rational numbers. In theory we could use the PARI−GP function `algdep` to recognise these rational numbers, but in all our examples they have such small height that it is obvious by sight.

Table 8. Rational Points on Genus 3 $X_0^+(p)$

$X_0^+(97)$	cusp	[1:0:0]		
	$D = -3$	?	$D = -4$	?
	$D = -8$	[−1:0:1]	$D = -11$	[0:1:0]
	$D = -12$	[1:1:−1]	$D = -16$	[−2:0:1]
	$D = -27$	[−2:1:1]	$D = -43$	[1:1:0]
	$D = -163$	[−7:3:2]		
	[0:1:0]	[0:0:1]		
$X_0^+(109)$	cusp	[1:0:0]		
	$D = -3$	?	$D = -4$	?
	$D = -7$	[1:1:−1]	$D = -12$	[0:1:0]
	$D = -16$	[−1:0:1]	$D = -27$	[2:1:−1]
	$D = -28$	[−3:1:1]	$D = -43$	[0:−1:1]
	[−4:1:2]	[1:2:−1]		

$X_0^+(113)$	cusp	[1:0:0]		
	$D = -4$	[1:2:−1]	$D = -7$	[−1:1:0]
	$D = -8$	[1:1:−1]	$D = -11$	[0:1:0]
	$D = -16$	[−1:0:1]	$D = -28$	[1:1:−2]
	$D = -163$	[3:3:−1]		
$X_0^+(127)$	cusp	[1:0:0]		
	$D = -3$	?	$D = -7$	[2:1:−1]
	$D = -12$	[0:1:0]	$D = -27$	[−2:0:1]
	$D = -28$	[0:−1:1]	$D = -43$	[−1:1:0]
	$D = -67$	[3:2:−1]		
	[4:3:−2]			
$X_0^+(139)$	cusp	[1:0:0]		
	$D = -3$	?	$D = -8$	[1:1:−1]
	$D = -12$	[−1:0:1]	$D = -19$	[−2:0:1]
	$D = -27$	[2:1:−1]	$D = -43$	[0:−1:1]
	[−5:2:1]			

$X_0^+(149)$	cusp	[1:0:0]		
	$D=-4$	?	$D=-7$	[-1:0:1]
	$D=-16$	[2:1:-1]	$D=-19$	[1:1:-1]
	$D=-28$	[1:2:-1]	$D=-67$	[-3:1:1]
	[0:-1:1]			
$X_0^+(151)$	cusp	[1:0:0]		
	$D=-3$	?	$D=-7$	[-1:1:0]
	$D=-12$	[-2:0:1]	$D=-27$	[0:-1:1]
	$D=-28$	[1:1:-2]	$D=-67$	[1:-2:1]
	$D=-163$	[1:0:1]		
	[0:-4:1]			
$X_0^+(179)$	cusp	[1:0:0]		
	$D=-7$	[-1:0:1]	$D=-8$	[0:1:0]
	$D=-11$	[1:1:-1]	$D=-28$	[1:2:-1]
	$D=-163$	[3:3:-1]		
$X_0^+(239)$	cusp	[1:0:0]		
	$D=-7$	[-1:0:1]	$D=-19$	[-2:0:1]
	$D=-28$	[-1:2:1]	$D=-43$	[-2:1:1]

We now give a table for some genus 4 curves $X_0^+(p)$. In this case the brute-force search is over a smaller region, namely $w, x, y, z \in \mathbb{Z}$ such that $|w|, |x|, |y|, |z| \leq 60$. We find that $X_0^+(137)$ has an exceptional rational point.

Table 9. Rational Points on Genus 4 Curves $X_0^+(p)$

$X_0^+(137)$	cusp	[1:0:0:0]		
	$D = -4$	[2:−4:−3:2]	$D = -7$	[2:−1:−2:1]
	$D = -8$	[−1:1:0:0]	$D = -11$	[1:1:−1:0]
	$D = -16$	[2:0:−1:0]	$D = -19$	[1:−2:−1:1]
	$D = -28$	[0:1:2:−1]		
	[19:2:−16:4]			
$X_0^+(173)$	cusp	[1:0:0:0]		
	$D = -4$	[0:−4:0:1]	$D = -16$	[2:−2:−2:1]
	$D = -43$	[0:1:−1:0]	$D = -67$	[3:−3:−2:1]
	$D = -163$	[12:−9:−5:2]		

Now for genus 5 curves. Here the bound for the search for rational points is reduced to 45. No further exceptional rational points are found.

Table 10. Rational Points on Genus 5 Curves $X_0^+(p)$

$X_0^+(157)$	cusp	[1:0:0:0:0]		
	$D = -3$	[6:11:−13:−6:4] ?	$D = -4$	[0:0:2:1:−1] ?
	$D = -11$	[1:−2:−1:1:0]	$D = -12$	[2:1:−1:0:0]
	$D = -16$	[2:2:−4:−1:1]	$D = -19$	[1:2:−3:−1:1]
	$D = -27$	[3:−1:−4:0:1]	$D = -67$	[2:1:−5:0:1]
$X_0^+(181)$	cusp	[1:0:0:0:0]		
	$D = -3$	[13:9:−11:−3:2] ?	$D = -4$	[2:2:−7:−1:2] ?
	$D = -11$	[2:−3:−1:1:0]	$D = -12$	[1:−3:−1:1:0]
	$D = -16$	[2:−2:−1:1:0]	$D = -27$	[2:0:−4:0:1]
	$D = -43$	[3:1:−1:0:0]	$D = -67$	[2:6:−4:−2:1]

Chapter 8

Future Paths

We have accumulated some evidence about the size of coefficients occurring in models for $X_0(N)$. It is clear that these modular curves (and their quotient curves by Atkin-Lehner involutions) do have remarkably small coefficients. Our computations only give information for small values of N and for low genus curves. Therefore we find ourselves in a poor position to make inferences about the general case.

We have seen that the theory of heights is a language in which one may phrase statements about the coefficient size of equations. Using heights we may bring questions about coefficient size into more well-known areas of number theory. There is much potential for further research in this direction, although some of the questions are doubtless very difficult to answer.

Another problem which begs further analysis is to interpret the exceptional rational points on $X_0^+(p)$ in terms of elliptic curves. It would also be interesting to know if there are exceptional rational points on other modular curves (for instance $X_{split}(p) = X_0(p^2)/W_p$ and $X_{non-split}(p)$).

One interesting problem which has arisen during this research is the following. Suppose we have a genus 3 curve D given as a double cover of an elliptic curve E. Suppose further that the Jacobian of D is isogenous to the product of E with the Jacobian of some genus 2 curve C. Then, is it possible to find an equation for the curve C from the explicit equations for $D \to E$? For example, $X_0(43)$ has genus 3 and it is a double cover of the elliptic curve $X_0^+(43)$. It can be shown that $J_0(43) \simeq E \times Jac(C)$ for some genus 2 curve C. By studying the period lattice of $J_0(43)$ and using techniques such as those of Wang [44], it might be possible to obtain an equation for C. Is there a more simple and direct way to obtain equations in this case?

It is fascinating to witness the hidden depth in even the most simple equations. For instance, the rational points on our equations contain large amounts of arithmetic information. The equations themselves are constrained by the task of reflecting this (and more) information − and yet they find the freedom to assume such elegant forms. This small illustration of the beauty of mathematics is payment enough for all the hard and dirty work.

References

[1] A. O. L. Atkin, J. Lehner, *Hecke Operators on* $\Gamma_0(N)$, Math. Ann., **185**, (1970) p. 134−160

[2] B. J. Birch, W. Kuyk (editors), *Modular Functions of One Variable IV*, Springer-Verlag LNM 476 (1975)

[3] J.-B. Bost, H. Gillet, C. Soulé, *Heights of Projective Varieties and Positive Green Forms*, J. Am. Math. Soc, **7**, no. 4, (1994) p. 903−1027

[4] J. W. S. Cassels, *Rational Quadratic Forms*, Academic Press (1978)

[5] J. W. S. Cassels, E. V. Flynn, *Prolegomena to a Middlebrow Arithmetic of Genus 2*, Cambridge (1996)

[6] C. H. Clemens, *A Scrapbook of Complex Curve Theory*, Plenum Press (1980)

[7] H. Cohen, D. Zagier, *Tables of weight 2 cusp forms*, Privately circulated

[8] J. E. Cremona, *Algorithms for Modular Elliptic Curves*, Cambridge (1992)

[9] J. E. Cremona, *Computing The Degree of the Modular Parameterization of a Modular Elliptic Curve*, Math. Comp., **64**, no 211 (1995) p. 1235−1250

[10] F. Diamond, J. Im, *Modular Forms and Modular Curves*, Canadian Math. Soc. Conf. Proc., **17**, AMS (1995) p. 39−133

[11] G. Faltings, G. Wüstholz, *Rational Points*, Vieweg (1986)

[12] G. Faltings, *Diophantine Approximation on Abelian Varieties*, Annals of Math., **133**, (1991) p. 549−576

[13] H. M. Farkas, I. Kra, *Riemann Surfaces*, Springer-Verlag GTM 71 (1980)

[14] G. Frey, *Links Between Solutions of* $A - B = C$ *and Elliptic Curves*, in Number Theory, Ulm 1987, Springer LNM 1380 (1989) p. 31−62

[15] G. Frey, *Construction and Arithmetical Applications of Modular Forms of Low Weight*, in CRM Lecture Notes 4, AMS (1994)

[16] W. Fulton, *Intersection Theory*, Springer (1984)

[17] P. Griffiths, J. Harris, *Principles of Algebraic Geometry*, Wiley (1978)

[18] B. H. Gross, *Heegner Points on* $X_0(N)$, in Modular Forms, R. A. Rankin ed., Wiley (1984)

[19] J. Harris, *Algebraic Geometry, a first course*, Springer-Verlag GTM 133 (1992)

[20] R. Hartshorne, *Algebraic Geometry*, Springer GTM 52 (1977)

[21] J-i. Igusa, *Theta Functions*, Springer-Verlag (1972)

[22] S. Iitaka, *Algebraic Geometry*, Springer-Verlag GTM 76 (1982)

[23] M. A. Kenku, *On the Modular Curves* $X_0(125), X_0(25)$ *and* $X_0(49)$, J. London Math. Soc., **23** (1981) p. 415−427

[24] B. Mazur, *Modular Curves and the Eisenstein Ideal*, Pub. I.H.E.S, **47** (1977) p. 33−186

[25] F. Momose, *Rational Points on* $X_0^+(p^r)$, J. Faculty of Science University of Tokyo Section 1A Mathematics, **33** no.3 (1986) p. 441−466

[26] F. Momose, *Rational Points on the Modular Curves* $X_0^+(N)$, J. Math. Soc. Japan, **39**, no.2 (1987) p.269−285

[27] D. Mumford, *Tata Lectures on Theta*, Birkhauser Prog. in Math., **28** (1983)

[28] N. Murabayashi, *On Normal Forms of Modular Curves of Genus 2*, Osaka J. Math., **29** (1992) p. 405−418

[29] A. Ogg, *Modular Forms and Dirichlet Series*, Benjamin (1969)

[30] A. Ogg, *Hyperelliptic Modular Curves*, Bull. Soc. Math. France, **102**, (1974) p. 449−462

[31] P. Philippon, *Sur des Hauteurs Alternatives I*, Math. Ann., **289** (1991) p. 255−283

[32] B. Schoenenberg, *Elliptic Modular Functions*, Springer Grundlehren der Math. Wissenschaften **203** (1974)

[33] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*, Iwanami / Princeton (1971)

[34] G. Shimura, *On Modular Forms of Half Integral Weight*, Annals of Math. **97** (1973) p. 440−481

[35] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer GTM 106, (1986)

[36] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer GTM 151 (1994)

[37] J. H. Silverman, *The Theory of Height Functions*, in Arithmetic Geometry, G. Cornell and J. H. Silverman eds., Springer (1986)

[38] J. H. Silverman, *Heights and Elliptic Curves*, in Arithmetic Geometry, G. Cornell and J. H. Silverman eds., Springer (1986)

[39] C. Soulé, *Geometrie D'Arakelov et Theorie des Nombres Transcendants*, Asterisque 198−200, (1991) p. 355−371

[40] C. Soulé, D. Abramovich, J.-F. Burnol, J. Kramer, *Lectures on Arakelov Geometry*, Cambridge (1992)

[41] H. P. F. Swinnerton-Dyer, *Analytic Theory of Abelian Varieties*, Cambridge (1974)

[42] L. Szpiro, *Discriminant et Conducteur des Courbes Elliptiques*, Astérisque **183**, (1990) p. 7−18

[43] D. J. Tingley, *Elliptic Curves Parameterised by Modular Functions*, D. Phil Thesis, Oxford (1975)

[44] X. D. Wang, *2−Dimensional Simple Factors of* $J_0(N)$, Manuscripta Math., **87**, No. 2, (1995) p. 179−197