A Splitting Criterion for Galois Representations Associated to Exceptional Modular Forms

Ken McMurdy

September 20, 2001
Abstract

There is a well-known way to get a two dimensional global Galois representation $\rho_f$ from a newform $f$ of weight $k \pmod{p}$ for $\Gamma_1(N)$. There is a conjecture by Serre, proven in most cases, which says that the ramification of $\rho_f$ at $p$ is completely determined by whether $f$ has a companion form. Furthermore, the existence of a companion form is in most cases equivalent to the splitting of the restriction of $\rho_f$ to a decomposition group at $p$. However, there is an exceptional case in which the splitting of this restriction, $\rho_{f,p}$, is a more subtle issue. The goal of Part I of this thesis is to develop a criterion which determines the splitting of $\rho_{f,p}$ in the exceptional case. The goal of Part II is to show the computability of this splitting criterion by working out some explicit examples. In the process of showing computability, we also develop some methods for obtaining very good models for modular curves and the maps between them which have a variety of other applications.
## Contents

### I Splitting Criterion

1 Introduction ........................................... 6

2 Background ............................................ 8
   2.1 Constructing the Representation $\rho_f$ ............ 8
   2.2 The $p$-divisible Group $G$ Associated to $f$ ........ 9

3 Splitting Invariants ................................ 11
   3.1 Definition of the Invariants $q$ and $q_p$ .......... 11
   3.2 Computing $q_p$ from $q$ .......................... 13

4 Inner Product Formulas for $\log q$ and $d\log q$ .... 15
   4.1 Formula for $\log q$ .................................. 15
   4.2 Formula for $d\log q$ ................................ 16

5 The Main Theorem ................................... 18

### II Examples

6 What Is an Example? .................................. 22

7 Getting Models for Modular Curves ................. 24
   7.1 Introduction ....................................... 24
   7.2 Review of Divisors and Basic Theorems of Algebraic Curves ... 25
   7.3 Ligozat and Eta Products ........................... 28
   7.4 Application of Cusp Theory .......................... 29
   7.5 Models for $X_0(N)$ ................................. 33

8 Example 1 ............................................. 36
   8.1 A Weight 5 Newform on $X_1(4)$ ..................... 36
   8.2 A Good Model for $I_1(4)$ .......................... 37
   8.3 Differentials $v_f$ and $v_{f'}$ on $I_1(4)$ .......... 38
   8.4 Computing $<[f],[f']>_{I_1}$ on $I_1(4)$ ............... 39
   8.5 A Good Model for $X_1(20)$ ....................... 40
Part I

Splitting Criterion
Chapter 1

Introduction

Any discussion of this thesis must first begin with a famous conjecture by Serre. Given a newform \( f \) of type \((k, \epsilon)\) and level \( N \) defined over a finite field \( E \) of characteristic \( p \), there is a standard way to get a 2-dimensional global Galois representation.

\[
\rho_f : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(E)
\]

Serre has conjectured that the restriction \( \rho_{f,p} \) of this representation to a decomposition group at \( p \) is unramified \((k = p)\) or tamely ramified \((k \neq p)\) if and only if there exists a companion form for \( f \). This companion form \( g \) is by definition a cusp form of weight \( k' = p + 1 - k \) and character \( \epsilon \) which satisfies the equation \( \theta g = \theta^{k'} f \).

In [CV], Coleman and Voloch proved this conjecture in every case except \( p = 2 \). Using a different approach in [G], Gross had previously proved the conjecture in all cases except when \( \epsilon(p) = a_p^2 \) and \( k = p \), which is called the “exceptional case.” Furthermore, Gross showed that the existence of a companion form is equivalent to the representation being split, i.e. the sum of two characters. Again, this is only in the non-exceptional case. In the exceptional case, the splitting of \( \rho_{f,p} \) is a more subtle issue, and the goal of this thesis is to find a computable criterion for the splitting of \( \rho_{f,p} \) in that case.

Following the general approach of [CV] and [G], we will begin by defining a \( p \)-divisible subgroup \( G \) of \( J_1(Np) \). \( G \) is a natural \( H_m \)-module where \( H_m \) is the \( m \)-adic completion of the Hecke algebra at a maximal ideal determined by \( f \). Under the assumption that \( H_m = \mathbb{Z}_p \), the representation of \( G = \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \) on \( G[m] = G[p] \) is simply a twist of \( \rho_f \). Therefore the splitting of one is completely determined by the splitting of the other, in particular when we restrict to a decomposition group at \( p \). At this point we attach a splitting invariant \( q_p \) to \( G[p] \) which is trivial if and only if the representation of \( G_p = \text{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p) \) given by \( G[p] \) is split. We then show how to calculate \( q_p \) from the usual Serre-Tate invariant \( q : T_p G \times T_p G' \to 1 + \pi R \) where \( R \) is the ring of integers in the maximal unramified extension of \( \mathbb{Q}_p(\zeta_p) \).

The final step in the proof of the main theorem is to incorporate two formulas for \( \log q \) and \( d\log q \) provided in [C1] and [CV]. The first formula involves an
inner product denoted $(\ , \ )_\infty$ on a subspace of $H^0(\mathcal{X}_1(N\mathfrak{p}), \Omega)$ which includes the unique lifting $F$ of $f$ as well as $F|_{w_{\mathfrak{q}_p}}$. The second formula involves the usual cup product on $H^1_{\text{DR}}(I)$ where $I = I_1(N)$ is the Igusa curve of level $N$ in characteristic $p$. The two forms $f$ and $f' = \theta f$ both define classes $[f], [f'] \in H^1_{\text{DR}}(I)$ whose inner product can then be taken. Applying these two formulas to $q$ and then calculating $q_{\mathfrak{p}}$ from $q$ we are able to prove the following.

**Theorem 1.1.** In the exceptional case and under the assumption that $H_m = \mathbb{Z}_p$, $\rho_{f,\mathfrak{p}}$ is split if and only if $<[f], [f']>_I = 0$ and $(F, F|_{w_{\mathfrak{q}_p}})_\infty \equiv 0 \pmod{\pi p+1}$.

The second part of the thesis is an attempt to show that the criterion is practically computable by working out a couple of examples. Gross provides a formula for the inner product on $I_1(N)$ given expansions for the differentials $[f]$ and $[f']$ at each of the supersingular points. Coleman provides an analogous formula for the inner product on $\mathcal{X}_1(N\mathfrak{p})$ given expansions for the differentials corresponding to $F$ and $F|_{w_{\mathfrak{q}_p}}$ along the supersingular annuli. So all that is needed for computing the splitting criterion is a good model for each of these curves. So Part II begins with the development of some useful techniques for obtaining such models which are then applied to two specific examples.

In the first example, the exceptional form $f$ is of weight 5 on $\mathcal{X}_1(4)$. So we must find models for the Igusa curve $I_1(4)$ as well as the curve $\mathcal{X}_1(20)$. $\mathcal{X}_1(20)$ has genus 3, so this example is enlightening but not too complicated. The result is that both inner products are in fact trivial (enough) and so we know that $\rho_{f,\mathfrak{p}}$ is indeed split. In the second example, the exceptional form $f$ is of weight 7 on $\mathcal{X}_1(3)$. So we must find models for $I_1(3)$ and $\mathcal{X}_1(21)$. $\mathcal{X}_1(21)$ has genus 5 so this example is slightly more complicated and slightly more enlightening. It is particularly interesting to see concretely that $F$ pairs trivially with all forms other than $F|_{w_{\mathfrak{q}_p}}$, and so the only real issue is how these two forms pair with each other. As in the first example, the two inner products are again trivial (enough) and so $\rho_{f,\mathfrak{p}}$ is again split.

As of right now, the theorem has only been proven in the case where $H_m$ is simply $\mathbb{Z}_p$. However, it should be possible to generalize the proof with only minor modifications to the case where $H_m$ is an order in the ring of integers of a finite unramified extension of $\mathbb{Q}_p$. This is equivalent to the condition that the lifting $F$ of $f$ is unique. At this time it is unclear how the removal of this restriction will affect the proof of the theorem.
Chapter 2

Background

2.1 Constructing the Representation $\rho_f$

In this chapter we will recall how the newform $f$ gives rise to a Galois representation $\rho_f$ as well as a $p$-divisible group $G$. We will borrow heavily from [G] where one can find more detailed descriptions and all relevant proofs. As always we begin with an ordinary newform $f$ of type $(k, \epsilon)$ for $\Gamma_1(N)$ over a finite field $E$ of characteristic $p$ with $(N, p) = 1$. Furthermore, we assume $p > 2$. Then there is a lifting of $f$ to a newform $F$ of type $(2, \epsilon_F)$ for $\Gamma_1(Np)$ over the integral closure $R$ of $\mathbb{Z}_p$ in $\overline{\mathbb{Q}}_p$.

Note. If $F(q) = \sum A_n q^n$ and $f(q) = \sum a_n q^n$ this means that $A_n \equiv a_n$ (mod $m_R$). Also, if $\epsilon_F = \epsilon_N \cdot \epsilon_p$ we must have $\epsilon_N(d) \equiv \epsilon(d)$ (mod $m_R$). In fact, the guaranteed lifting also satisfies $\epsilon_p = \chi^{k-2}$, where $\chi$ is the Teichmüller character into $\mathbb{Z}^*_p$.

Now, let $K$ be the finite extension of $\mathbb{Q}_p$ over which $F$ is defined. Let $H$ be the commutative subring of $\text{End}(J_1(Np))$ generated by the Hecke operators $T_l$ for $l$ prime to $Np$ and $\langle d \rangle_{Np}$. Then the subspace $W$ of $T_p(J_1(Np)) \otimes K$ on which $H \otimes K$ acts via the character associated to $F$ is a 2-dimensional $K$-vector space. Therefore we have a representation

$$r_F : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(K)$$

We define $\rho_F = r_F \otimes \epsilon_F$ so that the characteristic polynomial of $\rho(\sigma_l)$ for $l$ prime to $Np$ is simply $x^2 - A_l x + \epsilon_F(l)$. Finally, since $\rho_F$ stabilizes an $\mathcal{O}_K$-lattice we may reduce modulo $m_K$ and define $\rho_f$ to be the semisimplification of this reduction. It is then easy to show that the characteristic polynomial of $\rho_f(\sigma_l)$ is $x^2 - a_l x + \epsilon(l)l^{k-1}$ for $l$ prime to $p$.

It is almost possible to construct the representation $\rho_f$ without first lifting $f$. Let $V_f$ be the subspace of $J_1(Np)[p]\otimes \overline{\mathbb{Q}} \otimes E$ on which $T_l$ acts like $a_l$ for $l$ prime to $Np$, $\langle d \rangle_N$ acts like $\epsilon(d)$, and $\langle d \rangle_p$ acts like $d^{k-2}$. Gross shows that when $\rho_f$ is irreducible, the semi-simplification of $V_f \otimes \epsilon \chi^{k-2}$ is isomorphic to a...
direct sum of copies of $\rho_f$, where this $\chi$ is induced by the Galois action on $\mu_p$ and the Teichmüller character (hence the abuse of notation).

### 2.2 The $p$-divisible Group $G$ Associated to $f$

For the definition of $G$ we start by enlarging $H$ to include also the operators $U_t$ for $t \mid N_p$. Following [G] there is a maximal ideal $m$ of $H$ with $H/m = E$ such that modulo $m$ we have

$$ T_t \cong a_t $$

$$ U_t \cong a_t $$

$$ < d >_N \equiv \epsilon(d) $$

$$ < d >_p \equiv d^{k-2} $$

Let $H_m$ and $H_p$ be the completions of $H$ at $m$ and $p$, and let $\epsilon_m$ be the idempotent of $H_p$ satisfying $H_m = \epsilon_m H_p$.

**Note.** We will be most interested in the case where $f$ has a unique lifting to $F$. In this case, $H_m$ is simply the order $\mathbb{Z}_p[A_n]$.

The Tate module of $J_1(Np)$ is a module for $H_p$ and the submodule $\epsilon_m T_p(J_1(Np))$ is both free over $\mathbb{Z}_p$ and stable under $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$. Therefore it defines a $p$-divisible group $G$ over $\mathbb{Q}$ with $T_p(G) = \epsilon_m T_p(J_1(Np))$ which is acted on by $H_m$. Studying this $p$-divisible group and its $m$-torsion will enable us to prove the main theorem about when the representation $\rho_{f,p}$ is split in the exceptional case.

At this point we will assume that we are in the case where $H_m$ is simply $\mathbb{Z}_p$. The following theorem tells us what the structures of $G$ and $G/m = G[p]$ are in that case.

**Theorem 2.1.** In the case where $H_m = \mathbb{Z}_p$, the $p$-divisible group $G$ satisfies the following:

1. $G$ has height 2 and good reduction over $\mathbb{Z}_p[\zeta_p]$.
2. We have an exact sequence $0 \to G^0 \to G \to G^e \to 0$ over $\mathbb{Z}_p[\zeta_p]$ where $G^0$ and $G^e$ both have height 1.
3. From 2 we have an exact sequence of $\mathbb{Z}_p[\mathbb{G}_m]$-modules, $0 \to T_p G^0 \to T_p G \to T_p G^e \to 0$. $G_t = Gal(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ acts on $T_p G^0$ via the character $\lambda(U_p^{-1}) \cdot \chi_p$, where $\chi_p$ is the character given by the Galois action on $\mu_p$, and on $T_p G^e$ via the character $\lambda(U_p, p^{-1}) \cdot \chi^{2-k}$.
4. We have an exact sequence of $\mathbb{F}_p$-vector space schemes $0 \to G^0[p] \to G \to G^e[p] \to 0$ over $\mathbb{Q}_p$ with flat extensions to $\mathbb{Z}_p[\zeta_p]$.
5. $G^0[p]$ and $G^e[p]$ are 1-dimensional and the action of $G_p$ is given by the characters $\lambda(1/a_p) \cdot \chi$ and $\lambda(a_p/\epsilon(p)) \cdot \chi^{2-k}$.

Gross proves that $G$ has good reduction over $\mathbb{Z}_p[\zeta_p]$. It then follows from the theory of $p$-divisible groups that we have the exact sequences in 2 and 4. He also proves that the action of Galois is as given, that the height of $G$ is 2,
and that the dimension of $G^c[p]$ is 1. Now, by Nakayama’s Lemma and the fact that $T_pG$ is free of rank 2 over $H_m = \mathbb{Z}_p$, $T_pG/pT_pG$ must be a 2-dimensional $\mathbb{F}_p$-vector space. But this means $G^0[p]$ must also be dimension 1. By applying Nakayama’s Lemma again in the other direction, we see that $G^0$ and $G^c$ must then have height 1.

**Note.** Gross arrives at the same heights and dimensions without the assumption that $H_m = \mathbb{Z}_p$. However, he needed to use the fact that when $k = p$ we have $\epsilon(p) \neq a_p^2$. The additional assumption about $H_m$ was necessary because we will be working in the exceptional case.

We want to relate the splitting of $\rho_{f,p}$ to the extension class of the exact sequence involving $G[p]$. First we need to relate the representation given by $G[p]$ with $\rho_f$. Now, $G[p]$ is precisely the $\mathbb{F}_p$-subspace of $J_1(Np)[p]$ on which Hecke acts according to the eigenvalues and character of $f$. Indeed, this was the action which defined the maximal ideal $m$. This was how we also defined the subspace $V_f$ so one might expect that the two representations are the same. However, we had enlarged Hecke slightly. Therefore, $G[p]$ is in fact a 2-dimensional subspace of $V_f$ fixed by Galois. Now, assume $\rho_f$ is irreducible so that the semisimplification of $V_f \otimes \epsilon \chi^{k-2}$ is the direct sum of copies of $\rho_f$. Then we must have that $G[p]$ is also irreducible and furthermore that the representation on $G[p]$ is simply $\rho_f \otimes (\epsilon \chi^{k-2})^{-1}$. This leads us to the following theorem relating the splitting of $\rho_{f,p}$ and the splitting of the exact sequence involving $G[p]$.

**Theorem 2.2.** Suppose $H_m = \mathbb{Z}_p$ and that we are in the exceptional case. Then the following are equivalent:

1) $\rho_{f,p}$ is split and $\text{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ acts on the representation space via the scalar $\lambda(a_p)$

2) The exact sequence involving $G[p]$ is split so that $\text{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ acts on $G[p]$ via the scalar $\lambda(1/a_p) \cdot \chi$.

Since $k = p$ in the exceptional case, and $p-1$ kills $\chi$, we must have $\chi^{2-k} = \chi$. Similarly, $\epsilon(p) = a_p^2$ implies that $a_p/\epsilon(p) = 1/a_p$. Therefore the representation of $G[p]$ and the representation $\rho_{f,p}$ are split if and only if they are the scalars $\lambda(1/a_p) \cdot \chi$ and $\lambda(a_p)$ respectively, by Theorem 2.1. If this is the case, any exact sequence involving $G[p]$ would have to be split. Therefore the theorem is proved.
Chapter 3

Splitting Invariants

3.1 Definition of the Invariants $q$ and $q_p$

$G^0[p]$ is a connected one dimensional $\mathbb{F}_p$-vector space scheme and $G^e[p]$ an étale one dimensional $\mathbb{F}_p$-vector space scheme. Therefore by Theorem 2.1 they are simply twists of $\mu_p$ and $\mathbb{Z}/p\mathbb{Z}$ by the characters $\lambda(1/a_p)$ and $\lambda(1/a_p) \cdot \chi$ respectively. If we base extend up to a suitable field, this twisting becomes trivial and we can characterize the splitting of the exact sequence by looking at the invariant of the sequence in the group $Ext^1(\mathbb{Z}/p\mathbb{Z}, \mu_p)$. We must choose the extension field to be large enough to trivialize the twisting and yet hopefully small enough so that the splitting status does not change. Fortunately there is such a field $L_0$ which we will now describe.

Let $n$ be the order of $a_p$ in $\mathbb{F}_p^*$ and consider the following homomorphisms of groups:

$$\text{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p(\zeta_p)) \rightarrow \text{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p) \rightarrow \mathbb{Z}/n\mathbb{Z}$$

The first map is the usual reduction map and the second is simply modding out by $\phi^n$ where $\phi$ is the Frobenius automorphism. Let $\Delta_n$ be the kernel of the composition and define $L_0$ to be the fixed field of $\Delta_n$. Since $\Delta_n$ is a normal subgroup, $L_0$ is a normal extension of $\mathbb{Q}_p(\zeta_p)$ and we have $\text{Gal}(L_0/\mathbb{Q}_p(\zeta_p)) \cong \mathbb{Z}/n\mathbb{Z}$. Also, since $\Delta_n$ contains the kernel of reduction, $L_0/\mathbb{Q}_p(\zeta_p)$ is unramified. Finally, while $\chi$ becomes trivial upon extending up to $\mathbb{Q}_p(\zeta_p)$, the unramified character $\lambda(1/a_p)$ becomes trivial upon extending up to $L_0$ since it maps $\phi^n \rightarrow a_p^n = 1$. Now, we want to show that the splitting of the exact sequence remains invariant under this base extension, ie. the following theorem.

**Theorem 3.1.** The exact sequence of vector space schemes is split over $\mathbb{Q}_p$ iff it is split over $L_0$.

To prove this we first note that $L_0/\mathbb{Q}_p$ is a finite Galois extension of degree $n(p-1)$. Therefore for any element $\gamma \in \text{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$, $\gamma^{n(p-1)}$ must fix $L_0$. Now
suppose the sequence is split over $L_0$ and that $\gamma$ acts on $G[p]$ via the matrix

$$\begin{bmatrix} a & b \\ 0 & a \end{bmatrix}$$

with respect to any basis compatible with the exact sequence of vector space schemes. Recall that the characters of $G^0[p]$ and $G^e[p]$ were equal in the exceptional case, so $\gamma$ must act via such a matrix. Then $\gamma^{n(p-1)}$ must act via the matrix:

$$\begin{bmatrix} a^{n(p-1)} & n(p-1)a^{n(p-1)-1}b \\ 0 & a^{n(p-1)} \end{bmatrix}$$

But this matrix must be diagonal since $\gamma^{n(p-1)}$ fixes $L_0$ over which the sequence is split (and the representation is a scalar). Since $n(p-1)$ is prime to $p$ this implies $b = 0$ and the theorem is proved.

Since $\chi$ and $\lambda(1/a_p)$ are both trivial over $L_0$, we have isomorphisms $\lambda : G^0[p] \to \mu_p$ and $\beta : \mathbb{Z}/p\mathbb{Z} \to G^e[p]$ over $L_0$. Therefore via $\alpha$ and $\beta$ the exact sequence of vector space schemes defines a class in $Ext^1_{L_0}(\mathbb{Z}/p\mathbb{Z}, \mu_p) = L_0^*/L_0^p$. But the vector space schemes actually had flat extensions over $\mathbb{Z}_p(\zeta_p)$. Therefore if we let $R_0 \subset L_0$ be the ring of integers, we can extend $\alpha$ and $\beta$ to $R_0$. This gives us a class $q_p(\alpha, \beta) \in Ext^1_{R_0}(\mathbb{Z}/p\mathbb{Z}, \mu_p) = R_0^*/R_0^p$. Since any element of $R_0$ which is a $p$th power in $L_0$ must be a $p$th power in $R_0$, we see that we could add a third equivalent condition to the theorem.

**Theorem 3.2.** The following are equivalent:

1) The exact sequence is split over $\mathbb{Q}_p$
2) The exact sequence is split over $L_0$
3) The exact sequence is split over $R_0$
4) $q_p(\alpha, \beta)$ is trivial

It is interesting and useful to note what values in particular are possible for $q_p$. To do this we first consider how $Gal(L_0/\mathbb{Q}_p)$ acts on the various vector space schemes. On $G^0[p]$ and $G^e[p]$ the action is given by $\lambda(1/a_p) \cdot \chi$, and on $\mu_p$ and $\mathbb{Z}/p\mathbb{Z}$ the action is given by $\chi$ and the identity. Therefore on $\alpha$ and $\beta$ the actions are $\lambda(a_p)$ and $\lambda(1/a_p) \cdot \chi$. Since push-out and pull-back commute with scalar multiplication, Galois acts on the class $q_p \in Ext^1_{R_0}(\mathbb{Z}/p\mathbb{Z}, \mu_p)$ via the product $\lambda(a_p)\lambda(1/a_p) \cdot \chi = \chi$. In other words, the values of $q_p$ must lie in the $\chi$-eigenspace. This gives us a very useful starting point when we attempt to calculate $q_p$ and prove the main theorem.

So far the focus has been on the exact sequence of vector space schemes. It is possible to do the analogous construction with the exact sequence of $p$-divisible groups. In particular, $G^0$ and $G^e$ become simply $\mu_{p^\infty}$ and $\mathbb{Q}_p/\mathbb{Z}_p$ upon base extension to the maximal unramified extension of $\mathbb{Q}_p(\zeta_p)$. Let $L$ denote this field, and $R$ its ring of integers. Then for any isomorphisms $\alpha : G^0 \to \mu_{p^\infty}$ and $\beta : \mathbb{Q}_p/\mathbb{Z}_p \to G^e$ we get a class $q \in Ext^1_{R}(\mathbb{Q}_p/\mathbb{Z}_p, \mu_{p^\infty}) = 1 + \pi R$, where we choose $\pi$ to be the uniformizer $1 - \zeta_p$. If we mod out by $(1 + \pi R)^p$ we simply get $q_p$ after extending up to $R$. Therefore by the same argument this class must still be in the $\chi$-eigenspace. However, calculating $q_p$ over $R$ would not tell us
about the splitting of the exact sequence of vector space schemes over $R_0$. It is possible, though, to calculate $q_p$ over $R_0$ from $q$, using a result of Coleman. This will be a key element in the proof of the main theorem as will be a couple of useful formulas for calculating $q$.

### 3.2 Computing $q_p$ from $q$

It is natural to ask what relationship exists between the splitting invariants $q$ and $q_p$ attached to the $p$-divisible group $G$. Since $L$ is an extension of $L_0$ it is clear that the images of $q$ and $q_p$ are equal in $R^*/R^{*p}$ under the obvious maps. But $R^*_0/R^{*p}_0 \to R^*/R^{*p}$ is far from an injection. So it would be impossible to determine $q_p$ from $q$ using this fact alone. However, the two invariants are much more closely related, and in fact we can calculate $q_p$ from $q$. The following theorem does exactly that. Although originally proven by Coleman, here we follow the general line of reasoning of a proof by De Shalit.

**Theorem 3.3.** Let $\gamma : \text{Gal}(L/L_0) \to \mathbb{Z}_p^*$ be the character $\lambda(U_p^2/\langle \bar{y} \rangle_N)$. Choose $w \in R^*$ satisfying $w^{\sigma - 1} = q^{(\sigma - 1)/p}$ $\forall \sigma \in \text{Gal}(L/L_0)$. Then $q/w^p$ is in $R_0^*$ and $q_p \equiv q/w^p$ in $R_0^*/R^{*p}_0$.

Before proving the theorem we should first note why there is such a $w$. From Gross we know that $q^\tau = q^{\gamma(\tau)}$, and we know that $p|\gamma(\tau) - 1$ because $\epsilon(p) = a_p^2$ in the exceptional case. Therefore we have the equation

$$q^{(\gamma(\tau) - 1)/p} \left( q^{(\gamma(\tau) - 1)/p} \right)^\sigma = q^{(\gamma(\tau) - 1)/p} q^{(\gamma(\tau) - 1)/p} = q^{(\gamma(\tau) - 1)/p}$$

This shows that $q^{(\gamma(\tau) - 1)/p}$ is a cocycle of $\text{Gal}(L/L_0)$ acting on $L^*$. Therefore it must be a coboundary, which implies that $w$ exists and can in fact be taken to be a unit. Furthermore, raising $w^{\sigma}/w$ to the $p$th power we see that

$$\left( \frac{w^{\sigma}}{w} \right)^p = \left( q^{(\gamma(\tau) - 1)/p} \right)^p \Rightarrow \left( \frac{w^{p^{\sigma}}}{w^p} \right) = q^{\sigma} = \left( \frac{q}{w^p} \right)^\sigma = \frac{q}{w^p}$$

But this means $q/w^p$ is in $L_0$ and hence in $R_0^*$. Now we will show that $q/w^p$ does in fact reduce to $q_p$ in $R_0^*/R^{*p}_0$.

Recall that we have an exact sequence of $p$-divisible groups over $R_0$, namely

$$0 \to G^0 \to G \to G^e \to 0$$

which gives us via $\alpha$ and $\beta$ a class in $\text{Ext}^1_{R_0}(\mathbb{Q}_p/\mathbb{Z}_p(\lambda(U_p^2/\langle \bar{y} \rangle_N)), \mu_p \vee (\lambda(U_p^{-1})))$. By base extending to $R$ we obtain the class $q$ and by restricting to the $p$-torsion we obtain the class $q_p$. Twisting everything by the character $\lambda((\bar{y})_N/U_p)$ of $\text{Gal}(L/L_0)$ changes neither the $p$-torsion (by choice of $L_0$) nor the base extension. A small advantage of doing this is that $\lambda(U_p^{-1}) \lambda((\bar{y})_N/U_p) = \gamma^{-1}$. However, there is also the greater advantage that $\text{Ext}^1_{R_0}(\mathbb{Q}_p/\mathbb{Z}_p, \mu_p \vee \gamma^{-1}) = H^1(R_0, \mu_p \vee \gamma^{-1})$, so we may now phrase the problem in the language of cohomology. We have a class $\eta = \eta_q \in H^1(R_0, \mu_p \vee \gamma^{-1})$ which becomes (by $\text{res}$) $q$. 

in $H^1(R, \mu_{p^\infty}) = 1 + \pi R$ and reduces to $q_p$ in $H^1(R_0, \mu_p) = R_0^*/R_0^{*p}$. Because $\mu_{p^\infty}(L)$ is finite, $res$ is an injection. Therefore, all we need to do is find a class which restricts to $q$ (which must be $\eta$) and show that it reduces to $q/w^p$.

To define $\eta$ we first pick a compatible system of roots of $q$ in $\overline{\mathbb{Q}}_p$. By compatible, we simply mean that

$$\left(q^{1/p^{k+1}}\right)^p = q^{1/p^k}$$

In $H^1(R_0, \mu_{p^\infty}\gamma^{-1})$ we define

$$\eta_k(\sigma) = \frac{\left(q^{1/p^k}\right)^{\sigma\gamma^{-1}(\sigma)}}{q^{1/p^k}}$$

Since $q$ is fixed by $\sigma\gamma^{-1}(\sigma)$, we know $\eta_k$ must be a $p^k$th root of unity. To show $\eta_k$ is a cocycle (of $\mu_p\gamma^{-1}$) we simply calculate

$$\eta_k(\sigma)\eta_k(\tau) = \frac{\left(q^{1/p^k}\right)^{\sigma\gamma^{-1}(\sigma)}}{q^{1/p^k}} \cdot \frac{\left(q^{1/p^k}\right)^{\sigma\gamma^{-1}(\sigma)\tau\gamma^{-1}(\tau)}}{\left(q^{1/p^k}\right)^{\sigma\gamma^{-1}(\sigma)}} = \frac{\left(q^{1/p^k}\right)^{\sigma\tau\gamma^{-1}(\sigma\tau)}}{q^{1/p^k}} = \eta_k(\sigma\tau)$$

By the compatibility condition, the map $H^1(R_0, \mu_{p^{k+1}}\gamma^{-1}) \to H^1(R_0, \mu_{p^k}\gamma^{-1})$ takes $\eta_{k+1}$ to $\eta_k$. Therefore by taking the inverse limit we obtain a class $\eta \in H^1(R_0, \mu_{p^\infty}\gamma^{-1})$. It is important to note that a different compatible family of roots of $q$ would define a different cocycle $\eta'$ but that $\eta/\eta'$ is actually a coboundary determined by a compatible system of roots of unity. Therefore the class of $\eta$ is uniquely determined.

The only task remaining is to calculate the image of $\eta$ in $H^1(R, \mu_{p^\infty})$ under $res$ and the class of $\eta_1$ in $H^1(R_0, \mu_p)$. Since $\gamma$ is trivial over $L$, we have

$$res(\eta)(\sigma) = \lim \left(\frac{q^{1/p^k}}{q^{1/p^k}}\right)^\sigma$$

But this is precisely the class corresponding to $q$ in $1 + \pi R$. On the other hand, since $\eta_1(\sigma)$ is a $p$th root of unity and hence is fixed by $\gamma$, in $H^1(R_0, \mu_p)$ we have

$$\eta_1(\sigma) = \frac{(q^{1/p})^{\sigma\gamma^{-1}(\sigma)}}{q^{1/p}} = \frac{(q^{1/p})^\sigma}{(q^{1/p})^{\gamma(\sigma)}} = \frac{(q^{1/p})^\sigma}{q^{1/p}} \cdot q^{(1-\gamma(\sigma))/p} = \frac{(q^{1/p})\sigma}{q^{1/p}} \cdot \frac{w}{w^\sigma} = \frac{(w^{q/w^{1/p}})^\sigma}{(w^{q/w^{1/p}})^\sigma}$$

But this is precisely the class corresponding to $q/w^p$ in $H^1(R_0, \mu_p) = R_0^*/R_0^{*p}$. Therefore we have proved the theorem.
Chapter 4

Inner Product Formulas for $\log q$ and $d \log q$

At this point we know that we could (in theory) determine whether $\rho_{f,p}$ is split by choosing isomorphisms $\alpha$ and $\beta$ and then determining the splitting invariant $q(\alpha, \beta) \in 1 + \pi R$. We still do not have a practical criterion, however, which can be checked by straightforward calculations. In this chapter we will introduce two formulas for $\log q$ and $d \log q$ which can be evaluated by straightforward calculations. The formulas will involve two inner products, one on a subspace of $H^0(X_1(Np), \Omega)$ and the other on $H^1_{DR}(I)$ where $I = I_1(N)$ is the Igusa curve of level $N$ in characteristic $p$. The main theorem will then be a statement of how the splitting of $\rho_{f,p}$ is precisely related to the triviality of these inner products.

The first step to understanding the formulas is to give a different but equivalent interpretation of $\alpha$ and $\beta$. The choice of any homomorphism from $\mathbb{Q}_p/\mathbb{Z}_p$ to $G^c$ is equivalent to choosing an element of $T_p G^c = T_p G$. When $H_m = \mathbb{Z}_p$, this is a free $\mathbb{Z}_p$-module of rank 1. Therefore, $\beta$ corresponds to a generator of $T_p G$. Similarly, a choice of homomorphism from $G^0$ to $\mu_{p^\infty}$ is equivalent to choosing an element of $T_p G'$. Again, since this is a free $\mathbb{Z}_p$-module of rank 1, an isomorphism $\alpha$ corresponds to a generator of $T_p G'$.

With this interpretation of $\alpha$ and $\beta$, $q(\alpha, \beta)$ is just the usual Serre-Tate invariant given by:

$$q : T_p \bar{G} \times T_p \bar{G}' \rightarrow 1 + \pi R$$

4.1 Formula for $\log q$

Any element $\beta \in T_p G$ gives us a homomorphism from $G'$ to $G_m$ by which we can pull back $dt/t$ to obtain a differential $\omega_\beta \in \Omega_{G'}$. Using the canonical isomorphism of $G''$ with $G$ we can also construct from $\alpha \in T_p G'$ a differential $\omega_\alpha \in \Omega_G$. The resulting maps factor through $T_p \bar{G}$ and $T_p \bar{G}'$ so that we have the following:

$$T_p G \rightarrow T_p \bar{G} \rightarrow \Omega_{G'}$$
CHAPTER 4. INNER PRODUCT FORMULAS FOR LOG Q AND D LOG Q

$T_p G' \to T_p G' \to \Omega_G$

In [CV], Coleman shows that the second maps are actually isomorphisms. One must be careful, however, when applying Hecke here. While $H$ acts on $T_p G$ and $\Omega_G$, $\text{ros}(H)$ acts on $T_p G'$ and $\Omega_{G'}$. The isomorphisms do respect the action, though, in the sense that we have the formulas: $h\beta = \text{ros}(h)\omega_\beta$ and $\text{ros}(h)\alpha = h\omega_\alpha$.

Now, $G$ is the $p$-divisible subgroup of $J_1(Np)$ cut out by $\epsilon_m$ and $G'$ is isomorphic to the subgroup cut out by $\epsilon_{m'}$ where $m' = \text{ros}(m) \subseteq \text{ros}(H) \subseteq \text{End}(J_1(Np))$. Therefore $\Omega_G$ and $\Omega_{G'}$ are submodules of $H^0(X, \Omega)$ where $X$ is the canonical model for $X_1(Np)$ over $\mathbb{Z}_p[\zeta_p]$ given by Deligne-Rappaport. When $H_m = \mathbb{Z}_p$ we know from Gross that $\Omega_G$ is generated by the regular differential coming from the newform $F$, and $\Omega_{G'}$ is generated by the regular differential coming from the cusp form $F'|w_{\zeta_p}$. We should remark that $F'|w_{\zeta_p}$ is actually a constant multiple of another newform $F'$ where the constant has $\pi$-adic valuation 1 in the exceptional case.

In [C1], Coleman introduces an inner product on a subspace of $H^0(X_1(Np), \Omega)$ which contains both $\Omega_G$ and $\Omega_{G'}$, denoted $(\omega_1, \omega_2)_\infty$. He also provides a very practical formula for computing the inner product using expansions for the differentials along the supersingular annuli. Furthermore, if the inner product is applied to $T_p G \times T_p G'$ we have the following useful result:

$$\log q(\alpha, \beta) = (\omega_\beta, \omega_\alpha)_\infty$$

This is the first of the two formulas which we will need for the proof of the main theorem in the next chapter.

4.2 Formula for $d \log q$

The formula for $d \log q$ involves the usual inner product on $H^1_{DR}(I)$ where $I$ is the Igusa curve $I_1(N)$. Recall that $X$ reduces (mod $\pi$) to the union of two curves $I$ and $I'$ with only simple intersections at the supersingular points. Therefore any regular differential on $X$ reduces to a holomorphic differential on $I$ which then defines a class in $H^1_{DR}(I)$. There is also the class $[f']$, described by Gross, where $f' = \theta f$ in the exceptional case. It is not the reduction of any regular differential on $X$, and it is not holomorphic, although it has at most poles of order 2 at the supersingular points in the exceptional case.

From [CV] we have the following theorem which tells us how to compute the first term in the expansion for $d \log q = dq/q$.

**Theorem 4.1.** If $\beta \in T_p G$, $\alpha \in T_p G'$, and $\omega_\alpha|_I = \omega_f$, then

$$d \log q(\alpha, \beta) = a_p < w_{\zeta_p}^* \omega_\beta|_I, [f']>_I d\pi + \cdots$$

Although the choice of $\pi$ was different for this theorem, the following corollary is all we need and is independent of that choice.
Corollary 4.1.1. If \( \omega_\alpha|_I = \omega_f \) then \( d \log q \) is trivial (mod \( \pi d \pi \)) iff \( \omega_\beta|_I, [f'] >_I = 0 \).

For the proof of the main theorem, we will take \( \omega_\beta \) to be in fact \( \omega_F|_{w_\zeta p} \). Therefore we will actually be concerned with the triviality of \( < [f], [f'] >_I \). In the Part II, when actual examples are worked out, the formula for \( < [f], [f'] >_I \) will be taken from the formula of Gross involving explicit expansions for the two forms at the supersingular points.
Chapter 5

The Main Theorem

Theorem 5.1. Suppose \( H_m = \mathbb{Z}_p \) and we are in the exceptional case. Then \( \rho_{f,p} \) is split iff \( \left( \omega_F, \omega_F|\omega_{\xi_p} \right)_\infty \equiv 0 \pmod{\pi^{p+1}} \) and \( <[f],[f']> = 0 \).

As alluded to earlier we begin the proof by making the most obvious choice for \( \beta \in T_p \bar{G} = \Omega'G \) and \( \alpha \in T_p \bar{G'} = \Omega G' \). In particular we take \( \alpha \) to be the regular differential corresponding to the newform \( F \) and \( \beta \) to be the regular differential corresponding to the weight 2 cusp form \( F|\omega_{\xi_p} \). Again, since \( H_m = \mathbb{Z}_p \), \( \alpha \) and \( \beta \) are generators and hence correspond to isomorphisms of \( G_0 \) and \( G_\varepsilon \) with twists of \( \mu_{p^\infty} \) and \( \mathbb{Q}_p/\mathbb{Z}_p \) respectively. So from Theorems 2.2 and 3.2 we know \( \rho_{f,p} \) is split iff \( q_p(\alpha, \beta) = 0 \).

Now, since we want to ultimately calculate \( q_p \) from \( q_\ell \), we need a starting point. So we use the fact that \( q_\ell \) must be in the \( \chi \)-eigenspace of the Galois module

\[
\frac{R^*}{R^*p} = \frac{(1 + \pi R)/(1 + \pi R)^p = (1 + \pi R)/(1 + \pi^p R)}
\]

This last equality of course follows from the fact that \( R \) is the ring of integers in the maximal unramified extension of \( \mathbb{Q}_p(\xi_p) \). Using the triviality of Frobenius and solving for the \( \pi \)-coefficients iteratively one can show that the \( \chi \)-eigenspace is precisely the \( p \)th roots of unity. Therefore we must have \( q = \zeta^s(1 + r \pi^p) \) for \( s \in \mathbb{Z}/p\mathbb{Z} \) and \( r \in R \).

We can in fact be more precise, though, about the \( r \). \( q \) is in the \( \lambda(A^2_p/\epsilon(p)) \cdot \chi \)-eigenspace of the Galois module \( 1 + \pi R \), and \( A^2_p/\epsilon(p) \equiv 1 \). So acting on \( q \) by a Frobenius automorphism \( \phi \) we have

\[
q^\phi = q \cdot (q^p)^{(A^2_p/\epsilon(p)-1)/p}
\]

Plugging in \( \zeta^s(1 + r \pi^p) \) for \( q \) we get

\[
\zeta^s(1 + r^\phi \pi^p) = \zeta^s(1 + r \pi^p) \left( \left( \zeta^s(1 + r \pi^p) \right)^p \right)^{(A^2_p/\epsilon(p)-1)/p}
\]

Of course \( \zeta^{sp} = 1 \) and \( (1 + r \pi^p)^p \in 1 + \pi^{p+1}R \). So modulo \( \pi^{p+1} \) we have the congruence

\[
\zeta^s(1 + r^p \pi^p) \equiv \zeta^s(1 + r \pi^p)
\]
But this means that in $R/\pi$, $r$ is actually in $\mathbb{F}_p$. So we may actually start with the congruence

$$q \equiv \zeta^s (1 + \pi^p)^t \pmod{\pi^{p+1}}$$

with $s$ and $t$ in $\mathbb{Z}/p\mathbb{Z}$.

To calculate $q_p$ from $q$ we need to find $w \in R^*$ satisfying $w^{\sigma-1} = q^{(\gamma(\sigma)-1)/p}$ for all $\sigma \in \text{Gal}(L/L_0)$. Since this Galois group is generated by a power of $\phi$, it suffices to find $w$ such that $w^{\phi-1} = q^{(A_p^\phi/\epsilon(p)-1)/p}$. The map $\phi - 1$ from $1 + \pi R$ to itself is surjective, so we can do this by choosing $u,v \in 1 + \pi R$ satisfying

$$u^{\phi-1} = \zeta = 1 - \pi v^{\phi-1} = 1 + \pi^p$$

and then taking $w = (u^sv^t)^{(A_p^\phi/\epsilon(p)-1)/p}$. We see immediately that $u = 1 + r\pi$ with $r^p \equiv r - 1 \pmod{\pi}$ and $v = 1 + r\pi$ with $r^p \equiv r \pmod{\pi}$. Since $(1 + r\pi)^p \equiv 1 + (r^p - r) \pi^p \pmod{\pi^{p+1}}$ we must have $u^p \equiv (1 - \pi^p) \equiv (1 + \pi^p)^{-1} \pmod{\pi^{p+1}}$. Similarly we find that $v \equiv 1 \pmod{\pi^{p+1}}$. Therefore $u^p \equiv (1 + \pi^p)^{-s(A_p^\phi/\epsilon(p)-1)/p}$ which implies

$$q_p \equiv \zeta^s (1 + \pi^p)^{t+s(A_p^\phi/\epsilon(p)-1)/p}$$

**Lemma 5.1.** $\rho_{f,p}$ is split iff $s = t = 0$.

If $s = t = 0$, $q_p$ is in $1 + \pi^{p+1} R$ and is therefore a $p$th power. By Theorems 2.2 and 3.2 this means $\rho_{f,p}$ is split. Conversely, we know that $(1 + \pi R)^p \subset (1 + \pi^p R)$, so if $q_p$ is a $p$th power it follows immediately that $s = 0$. Furthermore, it is easily shown that a $p$th root of $1 + t\pi^2 + \cdots$ for $t \in \mathbb{Z}/p\mathbb{Z}$ generates a degree $p$ extension of $\mathbb{Q}_p(\zeta_p)$ unless $t = 0$. But the degree of $L_0/\mathbb{Q}_p(\zeta_p)$ was prime to $p$. Therefore, once $s = 0$, it is clear that $t$ must also be 0.

To complete the proof of the main theorem we first observe that $d\log q \equiv (-s/\zeta)d\pi \pmod{\pi d\pi}$. Therefore

$$s = 0 \iff d\log q \equiv 0 \pmod{\pi d\pi} \iff <[f],[f']>_{I_1} = 0$$

On the other hand, if $s = 0$, $\log q \equiv t\pi^p \pmod{\pi^{p+1}}$. In that case, $(\omega_F, \omega_F|_{w_{c_p}=}) \equiv 0 \pmod{\pi^{p+1}} \Rightarrow t = 0$ and we are done.
Part II

Examples
Chapter 6

What Is an Example?

The splitting criterion given in Part I applies to the representation coming from a newform $f$ of weight $k \pmod{p}$ on $X_1(N)$ which is “exceptional”. This means that $\epsilon(p) = a_p^2$ and $k = p$, where $\epsilon$ is the character of $f$ and $a_p$ is the coefficient of $q^p$ in the $q$-expansion of $f$, i.e. the $T_p$ eigenvalue of $f$. So any example must first start with such an $f$, which there is a systematic way of finding. First of all, we have a formula from [DI] for the dimension of the space of cusp forms of weight $k$ for $\Gamma_1(N)$ when $N > 4$ and $k > 2$:

$$(k - 1) \frac{N^2}{24} \prod_{p|N} (1 - p^{-2}) - \frac{N}{4} \prod_{p|N} (1 - p^{-2} + v_p(N)(1 - p^{-1})^2)$$  \hspace{1cm} (6.1)$$

We want the genera of the curves we work with to be as small as possible. So we simply let $k$ be a small odd prime and find the smallest values of $N$ for which $d_{N,k} = \dim S_k(\Gamma_1(N)) > 0$. For example, one sees immediately that $d_{7,3} = 1$ and $d_{6,5} = 2$. In addition we also know from [DI] all of the cusp forms on $X_1(N)$ explicitly for $N \leq 4$. On $X_1(4)$ the smallest odd-weight cusp form has weight 5 and on $X_1(3)$ the smallest odd-weight cusp form has weight 7. There are no odd-weight cusp forms of level 1 or 2. Then there is the matter of determining whether these newforms are exceptional. We will be able to find the $q$-expansions of these forms explicitly, so that will not be hard to check.

Now, we will not actually compute the representation $\rho_f$ or its restriction. The criterion developed in Part I says that we can determine whether $\rho_{f,p}$ is split by checking the triviality of two inner products. First, there is the inner product $\left< [f], [f'] \right>_I$ in $H^1_{DR}(I)$ where $I$ is the Igusa curve $I_1(N)$ and $[f]$ (resp $[f']$) is the class corresponding to $f$ (resp $f' = \theta f$). Then there is the inner product $(F, F|w_{\zeta_p})_{\infty}$ where $F$ is a lifting of $f$ to a newform on $X_1(Np)$ and $w_{\zeta_p}$ is an Atkin-Lehner automorphism.

To calculate these inner products we first need to have good models for the appropriate modular curves, namely $X_1(N)$, $X_1(Np)$, and $I_1(N)$. So a great deal of work will be put into the development of techniques for obtaining such models. In the end we will have a very efficient, systematic method for getting
exceptionally useful models, not only for curves of the form $X_0(M)$ but also for the various degeneracy maps between them. Then as needed in each specific example we will be able to generate the finite extension of function fields up to $X_1(N)$, $X_1(Np)$, or $I_1(N)$. Once we have a good model for $X_1(Np)$ we will be able to calculate $(F, F|_{w_{\zeta_p}})_\infty$ using a straightforward formula due to Coleman. Likewise we will use a formula of Gross to calculate $< [f], [f'] >_I$ once we have a good model for $I_1(N)$. 
Chapter 7

Getting Models for Modular Curves

7.1 Introduction

In some literature, a model for a modular curve is a scheme together with an analytic isomorphism from its \( \mathbb{C} \)-valued points onto a classical modular curve over \( \mathbb{C} \). What we actually need for arithmetic purposes, though, is something more. We need an embedding of this scheme into projective space over some small ring (preferably contained in a number field) so that we can actually do calculations in terms of coordinate functions. From [H] we know that this can only be done by choosing global sections of some invertible sheaf on the curve. If the sections generate the sheaf at the stalks, they do correspond to a morphism to projective space. Then there are similar conditions which ensure that the morphism is in fact a closed immersion.

For example, in [Ga], Steven Galbraith has obtained many embeddings of modular curves into projective space using the canonical morphism. This is the morphism which comes from the invertible sheaf of holomorphic differentials, equivalent to weight 2 cusp forms on a modular curve. It is an embedding provided the genus is at least 2 and the curve is not hyperelliptic. Another sheaf which can be used is the sheaf of differentials with at most simple poles at the cusps, equivalent to weight 2 holomorphic forms on a modular curve. More generally, one can use the invertible sheaf \( L(D) \) for any divisor \( D \) on the curve. The canonical sheaf is isomorphic to \( L(K_c) \) where \( K_c \) is the canonical divisor. The second example is the sheaf isomorphic to \( L(K_c + \text{cusps}) \).

Often the invertible sheaf which one chooses is determined by what kind of functions or differentials are readily available. If one has \( q \)-expansions and divisors for very well understood weight 2 forms then it is natural to work with a sheaf of differentials. In the examples that we will work with, we will actually have the \( q \)-expansions of many functions, i.e. weight 0 forms, whose divisors are easy to calculate. So for our purposes it is very natural to work directly with
The functions which we will work with are called eta products and they are very nice for many reasons. First of all, their divisors are very easy to calculate, and are supported only on the cusps. Also, with a little cleverness it is relatively easy to calculate their \( q \)-expansions at all of the cusps. This will make it easy to find equations for the maps between models for different modular curves, which actually makes the models much more useful.

7.2 Review of Divisors and Basic Theorems of Algebraic Curves

Divisors of functions are very useful when obtaining models for modular curves. Practically speaking, one looks for equations relating some functions on the curve, and the divisors of the functions dictate what form the equations can have. So we will begin this section by reviewing the most basic definitions and theory of the divisor group of an algebraic curve. For example, we will define the divisor of a function and of a differential, and subsequently the notion of linear equivalence of divisors.

After defining the vector space \( L(D) \) and the canonical class of divisors, we will be able to state the Riemann-Roch Theorem. Then we will concentrate more on maps between curves and the corresponding maps on divisor groups. Finally we will state a theorem of Hurwitz which tells us how much ramification there can be in such a map. Again, this is important because understanding the maps between the models makes them much more useful.

Throughout this section the proofs will be omitted and we refer the reader to [Si] from which much has been taken directly. The main goal of this section is to set notation for the kind of work we will do in our examples and to state precisely versions of the main results which we will rely on most heavily.

Definition. Let \( C \) be an algebraic curve over an algebraically closed field \( K \). The divisor group \( \text{Div}(C) \) is the free abelian group generated by the points of \( C \).

In other words, a divisor on a curve \( C \) is something of the form \( \sum_{P \in C} n_P(P) \) where the \( n_P \)'s are integers and almost all zero. We then define the degree \( \deg(D) \) to be the sum of the \( n_P \)'s. The subgroup of divisors \( D \) for which \( \deg(D) = 0 \) is called \( \text{Div}^0(C) \), and all of our work will take place within this subgroup. Also, we define the support, \( \text{supp}(D) \) to be the set of points \( P \in C \) for which \( n_P \neq 0 \).

Now, for a function \( f \) and a point \( P \) on \( C \), let \( \text{ord}_P(f) \) be the order to which \( f \) vanishes at \( P \) or minus the order to which \( 1/f \) vanishes. We can define the divisor \( \text{div}(f) \) by taking \( n_P \) to be \( \text{ord}_P(f) \). This definition is immediately validated by the fact that the map \( \text{Div} : K(C)^* \to \text{Div}(C) \) is a group homomorphism. The following theorem gives a good idea of what this homomorphism looks like.
CHAPTER 7. GETTING MODELS FOR MODULAR CURVES

**Theorem 7.1.** Let $C$ be a smooth curve over an algebraically closed field $K$, and $f$ some function in $K(C)^*$. 

(a) $\text{div}(f) = 0 \iff f \in K^*$  
(b) $\deg(\text{div}(f)) = 0$

We see that the image of $K(C)^*$ is contained in $\text{Div}^0(C)$, and that the kernel is simply the constant functions. A divisor $D$ which is $\text{Div}(f)$ for some $f$ is called a principal divisor, and two divisors, $D$ and $D'$, are said to be linearly equivalent if their difference is principal. 

Similarly, we can define $\text{Div}(\omega)$ for any differential $\omega \in \Omega^1_C$ as follows. For any point $P$ let $t$ be a uniformizer at $P$, i.e. a function with $\text{ord}_P(t) = 1$. Then since $\Omega^1_C$ is a one dimensional $K(C)$ vector space, $\omega/dt$ is a well defined function and we can take $\text{ord}_P(\omega)$ to be $\text{ord}_P(\omega/dt)$. Then as before we take $\text{Div}(\omega)$ to be $\sum_{P \in C} \text{ord}_P(\omega)P$. Also because $\Omega^1_C$ is one dimensional over $K(C)$, we can see that the divisors of all differentials lie in one special linear equivalence class, called the canonical class. In the discussion that follows, we will always take $K_c$ to be any divisor in the canonical class.

From the previous theorem, we see that the set of functions $f \in K(C)^*$ such that $\text{Div}(f) \geq 0$ is a one dimensional $K$ vector space. As it turns out, the subset of $K(C)^*$ with divisors greater than or equal to a given divisor is always a finite dimensional $K$ vector space. The dimension of this vector space goes up as we allow the function to have more poles without putting restrictions on its zeroes. This motivates the following definition:

**Definition.** Let $L(D)$ be the vector space of functions $f \in K(C)^*$ such that $\text{Div}(f) \geq -D$, and $l(D)$ be the dimension of $L(D)$.

$L(D)$ can actually be defined as an invertible sheaf on $C$, but for our purposes it will not be necessary to look beyond the global sections.

Now we can state one of the most useful theorems for the study of algebraic curves, the Riemann-Roch Theorem.

**Theorem 7.2 (Riemann-Roch).** Let $C$ be a smooth curve over an algebraically closed field $K$, $D$ any divisor on $C$, and $g$ the genus of $C$. Then

$$l(D) - l(K_c - D) = \deg(D) - g + 1 \quad (7.1)$$

**Corollary 7.2.1.** (a) $l(K_c) = g$  
(b) $\deg(K_c) = 2g - 2$  
(c) $\deg(D) > 2g - 2 \rightarrow l(D) = \deg(D) - g + 1$

Now we shift our focus to the study of maps between algebraic curves, and begin by defining the degree of a map.

**Definition.** Let $\phi : C_1 \rightarrow C_2$ be a non-constant map of smooth curves. Then we define

$$\deg(\phi) = [K(C_1) : \phi^*(K(C_2))]$$
7.2. REVIEW OF DIVISORS AND BASIC THEOREMS OF ALGEBRAIC CURVES

**Definition.** Let $\phi$ be as above, $P$ a point in $C_1$, and $t_{\phi(P)}$ be a uniformizer at $\phi(P)$. Then we define the ramification index of $\phi$ at $P$ to be

$$e_{\phi}(P) = \text{ord}_P(\phi^* t_{\phi(P)})$$

Intuitively, the degree of a map is the number of points in $C_1$ lying over most points of $C_2$. When the cover is branched, the ramification index counts how many points have been squeezed together in that fiber. More specifically, the ramification index at $P$ counts how many points which are close to $P$ lie above a given point which is close to $Q$. As one might expect, for any point $Q$ in $C_2$, the following formula holds true:

$$\deg(\phi) = \sum_{P \in \phi^{-1}(Q)} e_{\phi}(P)$$  \hspace{1cm} (7.2)

Now, let $\phi$ be as above. We can define a homomorphism $\phi^* : \text{Div}(C_2) \to \text{Div}(C_1)$ by taking each point $Q$ to $\sum_{P \in \phi^{-1}(Q)} e_{\phi}(P)P$, and extending by linearity. This map preserves principal divisors. In fact, if $f$ is a function on $C_2$ and $\phi^*(f)$ is the pullback to a function on $C_1$, then we have the following:

$$\text{div}(\phi^*(f)) = \phi^*(\text{div}(f))$$  \hspace{1cm} (7.3)

From the previous two equations, one begins to see how important the ramification of a map is in understanding that map. In fact, in many cases, knowing the ramification of a map all but determines the map. One basic theorem of algebraic curves which states how much ramification there can be is due to Hurwitz:

**Theorem 7.3 (Hurwitz).** Let $\phi$ be a non-constant separable map of smooth curves. Then

$$2g_1 - 2 \geq (\deg(\phi))(2g_2 - 2) + \sum_{P \in C_1} (e_{\phi}(P) - 1)$$

where $g_i$ is the genus of $C_i$. Furthermore, equality holds if and only if either:

1. $\text{char}(K) = 0$; or
2. $\text{char}(K) = p > 0$ and $p$ does not divide $e_{\phi}(P)$ for all $P \in C_1$.

This theorem is often called the Hurwitz Genus Formula because it enables us to calculate the genus of one of the curves if we know the other genus and the ramification. For our purposes, however, we will always know the genera of all the curves. What we will want to know is how much ramification there is so that we can calculate divisors of functions which we pull back. This will enable us to find a formula for that function in terms of the parameters on $C_1$, giving us the map between the curves explicitly, which is of course one of our main goals.
7.3 Ligozat and Eta Products

We have now explained how we will go about using functions on the modular curves to get embeddings into projective space. We have also explained how the divisors of these functions will be used to get equations between the functions and maps between the curves. What we still need to do is to say what functions in particular we will use. As was mentioned in the introduction, there is a large class of functions which have exactly the properties we need. Namely, their divisors are supported on the cusps and are very easy to calculate. Also, it is not too difficult to calculate the \( q \)-expansions and values of these functions at all of the cusps. These very special functions are called eta products and the point of this section is to define eta products, state a theorem of Ligozat which tells us when an eta product is an honest-to-goodness function on a modular curve, and to give some explicit examples.

We begin our discussion by recalling \( \Delta(z) \), the famous weight 12 cusp form for \( SL_2(\mathbb{Z}) \). Its \( q \)-expansion is given by the formula

\[
\Delta(z) = c \cdot q \prod_{n=1}^{\infty} (1 - q^n)^{24}
\]

and its divisor on the rational curve \( X(1) \) is simply \((\infty)\). We can pull back \( \Delta \) by various different maps to get other weight 12 cusp forms of higher level. For example, on \( X_0(3) \) we can pull back by the identity map which is of degree 4, unramified at infinity and totally ramified at the cusp \((0)\). So on \( X_0(3) \), \( \text{div}(\Delta(z)) = 3(0) + (\infty) \). Also, we can pull back by the map \( z \rightarrow 3z \) which is of degree 4, totally ramified at \((\infty)\) and unramified at \((0)\). So on \( X_0(3) \), \( \text{div}(\Delta(3z)) = (0) + 3(\infty) \). Now, the interesting thing is that the quotient \( \Delta(z)/\Delta(3z) \) is now a function on \( X_0(3) \) with divisor \( 2(0) - 2(\infty) \). Since \( X_0(3) \) is a rational curve, this function must have a square root, which we will call \( H_3 \).

Its \( q \)-expansion is given by:

\[
H_3(q) = q^{1/2} \prod_{n=1}^{\infty} (1 - q^n)^{12} = q^{3/2} \prod_{n=1}^{\infty} (1 - q^{3n})^{12} = q \prod_{n=1}^{\infty} (1 - q^{3n})^{12}
\]

More generally, one can always get a function by taking a quotient of pullbacks of \( \Delta \). Then you can try to determine whether this function is a power of a function with lower degree. Equivalently, one can simply start with the 24th root of \( \Delta \) (the largest root for which the \( q \)-expansion is reasonable), construct the same type of quotient, and then ask what the smallest power is which is an honest function. So we begin by defining \( \text{eta} \), essentially a 24th root of \( \Delta \).

\[
\text{eta}(m) = q^{m/24} \prod_{n=1}^{\infty} (1 - q^{mn}) \in q^{m/24} \mathbb{Z}[q]
\]

By itself, \( \text{eta}(m) \) can be considered only as a formal \( q \)-expansion, but we have already seen that \( (\text{eta}(1)/\text{eta}(3))^{12} \) is actually a function on \( X_0(3) \). It is a very good example of what we now define as an eta product.
Definition. For level $\Gamma_0(N)$ we define an eta product to be any formal $q$-expansion of the form:
\[
\prod_{d|N} (\text{eta}(d))^{r_d}, r_d \in \mathbb{Z}
\]

Now, we have an incredibly useful theorem due to Ligozat which tells us when an eta product gives an actual function on $X_0(N)$.

**Theorem 7.4 (Ligozat).** Let the notation be as above. Then an eta product is the $q$-expansion of an actual function on $X_0(N)$ if and only if the following conditions hold.

(A) $\sum_{d|N} r_d \cdot \frac{N}{d} \equiv 0 \pmod{24}$
(B) $\sum_{d|N} r_d \cdot d \equiv 0 \pmod{24}$
(C) $\sum_{d|N} r_d = 0$
(D) $\prod_{d|N} (\frac{N}{d})^{r_d} \in \mathbb{Q}^2$.

**Example 7.1.** Take $N = 6$ and \{r_1, r_2, r_3, r_6\} to be \{5, -1, 1, -5\}. Then the theorem tells us that the following is a function on $X_0(6)$.

\[
(\text{eta}1)^5(\text{eta}3) \\
(\text{eta}2)(\text{eta}6)^5
\]

The conditions in the previous theorem are not all mysterious. Condition C ensures that the form, if it is a form, is of weight 0. Condition B verifies that the powers of $q$ in the $q$-expansion are integral. Condition A does the same for the Atkin-Lehner involution of the form. Condition D requires a little more careful treatment of $\text{eta}$ as a function on the upper half-plane, and an understanding of exactly why it is not a weight 1/2 form in the first place.

Although we will not use it in our examples, there is an analogous theorem of Ligozat for determining when an eta product gives a cusp form of weight 2.

**Theorem 7.5 (Ligozat).** The following conditions are sufficient for an eta product to be a weight 2 cusp form on $X_0(N)$.

(A) $\sum_{d|N} r_d \cdot d \equiv 0 \pmod{24}$
(B) $\sum_{d|N} r_d \cdot \frac{N}{d} \equiv 0 \pmod{24}$
(C) $\sum_{d|N} r_d = 4$
(D) $\prod_{d|N} (\frac{N}{d})^{r_d} \in \mathbb{Z}^2$.

### 7.4 Application of Cusp Theory

Thanks to Ligozat, we have the $q$-expansions of many functions on $X_0(N)$. In order to find equations relating these functions, however, we need to be able to
do two things. First of all, we must be able to calculate the divisor of one of
these functions. Secondly, we must be able to determine its value at cusps which
are not in the support. For the latter we will actually calculate the \( q \)-expansions
at these cusps which will certainly suffice. The approach we will take begins
with understanding some basic maps between modular curves. In the end we
will show that an eta product comes from the pullbacks of the modular form \( \Delta \)
on \( X(1) \) by these various maps. We know the divisor of \( \Delta \), namely \( (\infty) \), and its
\( q \)-expansion. So all we need to understand is what pulling back does to divisors
and \( q \)-expansions of modular forms. That will comprise the meat of this section.

**Definition.** Let \( M, N, \) and \( d \) be positive integers with \( Md|N \). Then we define
the map \( \pi_d : X_0(N) \to X_0(M) \) by \( \pi_d(E, C) = (E/C[d], C[M]/C[d]) \).

This is a moduli-theoretic definition in the sense that each point in \( X_0(N) \)
is represented by an elliptic curve \( E \) with \( C \) a cyclic subgroup of order \( N \). \( C[d] \)
is the \( d \)-torsion of \( C \). \( E/C[d] \) is then the quotient which has \( C[M]/C[d] \) as a
cyclic subgroup of order \( M \). \( \pi_1 \) sometimes called the forgetful map because
it leaves the elliptic curve \( E \) unchanged and simply forgets all but the level \( M \)
structure given by \( C[M] \).

Recall that for a map of curves \( \Phi : C_1 \to C_2 \) and \( f \) a function on \( C_2 \) with
divisor \( \sum_{i=1}^{\infty} a_i P_i \), the divisor of the pullback of \( f \) is given by:

\[
(\Phi^*f) = \sum_{i=1}^{\infty} \left( \sum_{Q \in \phi^{-1}(P_i)} a_i \epsilon_{\Phi}(Q)Q \right)
\]

The theory of divisors of modular forms is well developed in [Sh] and we see
that they behave in the same way. So all we need to know to calculate the
divisor of a pullback of \( \Delta \) is the ramification indices of the cusps lying over \( \infty \)
for the given map. In other words, we must see how many points close to the
cusp upstairs lie over a point close to infinity.

**Example 7.2.** \( \text{Div}(\pi_3^*\Delta) \) on \( X_0(6) \)

Consider the map \( \pi_3 : X_0(6) \to X(1) \). We will calculate the ramification
index \( \epsilon_{\pi_3} \) at each of the four cusps lying over \( \infty \), namely \( 0, \frac{1}{2}, \frac{1}{3}, \infty \). Using the
formula for divisors of pullbacks we will then be able to calculate \( \text{Div}(\pi_3^*\Delta) \).
For simplicity we will work over any \( p \)-adic field \( K \).

Any point close to the cusp 0 represents the pair \( (K^*/q^6, < q >) \) for some
unique \( q \). Now, applying \( \pi_3 \) we have \( \pi_3(K^*/q^6, < q >) = K^*/ < q^6, q^2 >= K^*/q^2 \). Any point close to \( \infty \) on \( X(1) \) also corresponds to \( K^*/q \) for some
unique \( q \). Therefore we see that close to the cusp 0, the map \( \pi_3 \) is \( 2 : 1 \), ie.
\( \epsilon_{\pi_3}(0) = 2 \).

Any point close to the cusp \( \frac{1}{2} \) represents the pair \( (K^*/q^3, < -q >) \) for some
unique \( q \). Now, applying \( \pi_3 \) we have \( \pi_3(K^*/q^3, < -q >) = K^*/ < q^2, q^2 >= K^*/q \). So we see that close to \( \frac{1}{2} \) the map \( \pi_3 \) is \( 1 : 1 \), ie. \( \epsilon_{\pi_3}(\frac{1}{2}) = 1 \).

Any point close to the cusp \( \frac{1}{3} \) represents the pair \( (K^*/q^2, < \omega q >) \) where \( \omega \)
is a primitive cube root of unity. Now, applying \( \pi_3 \) we have \( \pi_3(K^*/q^2, < \omega q >) \)}
\( \pi \) which we obtain is given by:
\[
(\text{preserves the differential } dt \Delta(\cdot, q) \text{ and } \Omega^1) = \mathcal{K}^* / < q, \omega^2 > = \mathcal{K}^* / q^6. \]
For the last step we are using the fact that cubing is an isomorphism if you’ve already modded out by the cube roots of unity. So we see that close to the cusp \( \frac{1}{3} \) the map \( \pi_3 \) is 6 : 1, ie. \( e_{\pi_3}(\frac{1}{3}) = 6 \).

Any point close to the cusp \( \infty \) represents the pair \((\mathcal{K}^* / q, < \zeta_6 >)\) where \( \zeta_6 \) is a fixed primitive root of unity. Now, applying \( \pi_3 \) we have \( \pi_3(\mathcal{K}^* / q, < \zeta_6 >) = \mathcal{K}^* / < q, \zeta_6^2 > = \mathcal{K}^* / q^3 \). Again, we are cubing in the last step which is an isomorphism. So we see that close to the cusp \( \infty \) the map \( \pi_3 \) is 3 : 1, ie. \( e_{\pi_3}(\infty) = 3 \).

The result of these calculations, using the formula for pulling back divisors, is that:
\[
\text{Div}(\pi_3^* \Delta) = 2(0) + 1(\frac{1}{2}) + 6(\frac{1}{3}) + 3(\infty)
\]

Now that we have seen how to calculate the divisor of a \( \Delta \)-pullback, we now turn our attention to the \( q \)-expansion, which is dependent on two things. First we need a map from the disc to the modular curve, which is the same as picking an elliptic curve with level structure to lie over each point in the disc. Then we must choose continuously a holomorphic differential for the elliptic curve lying over each point. There is a canonical map from the disc \(|q| < 1\) into \( X_0(\mathbb{N}) \) which takes \( q = 0 \) to the cusp \( \infty \). It takes nonzero \( q \)'s to the isomorphism class of elliptic curves represented by \( \mathcal{K}^* / q \) with cyclic subgroup \( < \zeta_N > \). There is also a canonical holomorphic differential, \( \frac{dt}{q} \), for each of these elliptic curves. Now, \( \Delta \) is a weight 12 form on \( X(1) \) with \( \Delta(q) = q + \cdots \). This means that \( \Delta \) takes the elliptic curve \( E = \mathcal{K}^* / q \) to the section of the sheaf \( \Omega^1_{E_0} \otimes 12 \) given by \((q + \cdots)(\frac{dt}{q})^{12}\). So suppose we are pulling back by a map \( f : X_0(\mathbb{N}) \to X(1) \) which takes the pair \((E_1, C)\) to the elliptic curve \( E_2 \). The pullback by \( f \) of \( \Delta \) applied to the pair \((E_1, C)\) will first apply \( \Delta \) to \( E_2 \) to obtain a section of \( \Omega^1_{E_2} \otimes 12 \). Then it will pull back to a section of \( \Omega^1_{E_1} \otimes 12 \) by the map from \( E_1 \) to \( E_2 \). When we let \((E_1, C)\) vary over all \( q \)'s and divide out by the continuously chosen section of \( \Omega^1_{E_0} \otimes 12 \) we are left with a function on the disc. Its expansion is precisely the \( q \)-expansion of the pulled back form.

**Example 7.3.** \( q \)-expansions of \( \pi_3^* \Delta \) on \( X_0(6) \)

Again we will work with \( \pi_3 : X_0(6) \to X(1) \), but this time we will calculate four different \( q \)-expansions of \( \pi_3^* \Delta \), one at each cusp. First we consider the map from the disc to \( X_0(6) \) which takes nonzero \( q \)'s to the pair \((\mathcal{K}^* / q^6, < q >)\) and \( q = 0 \) to the cusp 0. We will still choose the canonical differential \( \frac{dt}{q^4} \) for each curve. We have already seen that \( \pi_3(\mathcal{K}^* / q^6, < q >) = \mathcal{K}^* / q^3 \), and \( \Delta(\mathcal{K}^* / q^2) = (q^2 + \cdots)(\frac{dt}{q})^{12} \). Furthermore, the map from \( \mathcal{K}^* / q^6 \) to \( \mathcal{K}^* / q^2 \) preserves the differential \( \frac{dt}{q^4} \). Therefore the \( q \)-expansion of \( \pi_3^* \Delta \) at the cusp 0 which we obtain is given by: \( \pi_3^* \Delta(q)_{10} = q^2 + \cdots \).

Next we consider the map which takes nonzero \( q \)'s to \((\mathcal{K}^* / q^3, < -q >)\) and \( q = 0 \) to the cusp \( \frac{1}{3} \). Again we choose the canonical differential. We have already seen that \( \pi_3(\mathcal{K}^* / q^3, < -q >) = \mathcal{K}^* / q \), and \( \Delta(\mathcal{K}^* / q) = (q + \cdots)(\frac{dt}{q})^{12} \). Again
the map from $\overline{K'/q^3}$ to $\overline{K'/q}$ preserves the differential $dt$. Therefore the $q$-expansion of $\pi_5^*\Delta$ at the cusp $\frac{1}{3}$ which we obtain is given by: $\pi_5^*\Delta(q)\big|_{\frac{1}{3}} = q + \cdots$.

Next we consider the map which takes nonzero $q$'s to $(\overline{K'/q^2}, <\omega_q>)$ and $q = 0$ to the cusp $\frac{1}{3}$. Again we choose the canonical differential. We have already seen that $\pi_3(\overline{K'/q^2}, <\omega_q>) = \overline{K'/q^6}$, and $\Delta(\overline{K'/q^6}) = (q^6 + \cdots)(\frac{dt}{q})^{12}$. However, this time the map from $\overline{K'/q^2}$ to $\overline{K'/q^6}$ was the cubing map, which does not preserve the differential $\frac{dt}{q}$. One can easily check that this differential pulls back to $3\frac{dt}{q}$. Therefore the $q$-expansion of $\pi_5^*\Delta$ at the cusp $\frac{1}{3}$ which we obtain is given by: $\pi_5^*\Delta(q)\big|_{\frac{1}{3}} = 3^{12}(q^6 + \cdots)$.

Finally we consider the map which takes nonzero $q$'s to $(\overline{K'/q}, <\zeta_6>)$ and $q = 0$ to the cusp $\infty$. We have already seen that $\pi_3(\overline{K'/q}, <\zeta_6>) = \overline{K'/q^3}$, and $\Delta(\overline{K'/q^3}) = (q^3 + \cdots)(\frac{dt}{q})^{12}$. Again, the map is the cubing map, so $\frac{dt}{q}$ pulls back to $3\frac{dt}{q}$. Therefore the $q$-expansion of $\pi_5^*\Delta$ at the cusp $\infty$ which we obtain is given by: $\pi_5^*\Delta(q)\big|_{\infty} = 3^{12}(q^3 + \cdots)$.

Note. It is interesting that the $q$-expansion of $\pi_5^*\Delta$ at infinity using the canonical map and canonical differential was not $\Delta(q^3)$ as one might expect. However, the previous calculation easily generalizes to show that for any form $f$ of weight $k$ and any $\pi_d$, we have $\pi_d^*f(q)\big|_{\infty} = d^k f(q^d)\big|_{\infty}$. As a special case we see that pulling back by the forgetful map always preserves $q$-expansions at infinity.

Now we are finally ready to calculate everything we would like to know about an eta product, namely its divisor and its value at every cusp not in the support. Since all the tools for this calculation have been more than adequately developed we will jump right into an example, the previously defined function on $X_0(6)$ given by:

$$H_6 = \frac{(eta1)^5(eta3)}{(eta2)(eta6)^5}$$

We begin by expressing a power of $H_6$ as some constant times a product and quotient of pullbacks of $\Delta$.

$$H_6^{24} = \frac{(\pi_1^*\Delta)^5(3)^{12}(\pi_3^*\Delta)}{(2)^{12}(\pi_2^*\Delta)(6)^{12}(\pi_6^*\Delta)^5} = c \cdot \frac{(\pi_1^*\Delta)^5(\pi_3^*\Delta)}{(\pi_2^*\Delta)(\pi_6^*\Delta)^5}$$

We have already seen that $\text{Div}(\pi_1^*\Delta) = 2(0) + 1(\frac{1}{2}) + 2(\frac{1}{3}) + 1(\infty)$. By similar calculations we also have:

- $\text{Div}(\pi_3^*\Delta) = 6(0) + 3(\frac{1}{2}) + 2(\frac{1}{3}) + 1(\infty)$
- $\text{Div}(\pi_2^*\Delta) = 3(0) + 6(\frac{1}{2}) + 1(\frac{1}{3}) + 2(\infty)$
- $\text{Div}(\pi_6^*\Delta) = 1(0) + 2(\frac{1}{2}) + 3(\frac{1}{3}) + 6(\infty)$

Therefore the divisor of $(H_6)^{24}$ is:

$$\begin{bmatrix}
0 & \frac{1}{2} & \frac{1}{3} & \infty
\end{bmatrix} \cdot \begin{bmatrix}
6 & 3 & 2 & 1 \\
3 & 6 & 1 & 2 \\
2 & 1 & 6 & 3 \\
1 & 2 & 3 & 6
\end{bmatrix} \cdot \begin{bmatrix}
5 \\
-1 \\
1 \\
-5
\end{bmatrix} = 24(0) - 24(\infty)$$
7.5. MODELS FOR $X_0(N)$

Therefore the divisor of $H_6$ must simply be $(0) - (\infty)$.

Now we will calculate the value of $H_6$ at the cusp $\frac{1}{2}$ by calculating the $q$-expansions of all 4 pullbacks. Of course it is important to use the same map from the disc and choice of holomorphic differentials. We will again use the map which takes nonzero $q$’s to the pair $(\mathcal{K}/q^3, < -q >)$ and the usual differential $\frac{dt}{t}$. We already know that the $q$-expansion of $\pi_3^*\Delta$ is given simply by $q + \cdots$.

By similar calculations we obtain:

$$
\begin{align*}
\pi_1^*\Delta(q)|_{\frac{1}{2}} &= q^3 + \cdots \\
\pi_2^*\Delta(q)|_{\frac{1}{2}} &= 2^{12}(q^6 + \cdots) \\
\pi_6^*\Delta(q)|_{\frac{1}{2}} &= 2^{12}(q^2 + \cdots)
\end{align*}
$$

Therefore the $q$-expansion of $(H_6)^{24}$ is given by:

$$
\frac{(q^3 + \cdots)^5(3)^{-12}(q + \cdots)}{(2)^{-12}(2)^{-12}(q^6 + \cdots)(6)^{-60}(2)^{60}(q^2 + \cdots)^5} = 3^{18}(1 + \cdots)
$$

Therefore the value of $(H_6)^{24}$ at the cusp $\frac{1}{2}$ must be $3^{18}$. But this means the value of $H_6$ at $\frac{1}{2}$ must be a root of unity times 9. One needs this value to find a formula for the forgetful map down to $X_0(2)$, and upon comparing $q$-expansions one finds that $H_6(\frac{1}{2}) = -9$.

7.5 Models for $X_0(N)$

Now we are able to find lots of functions on $X_0(N)$, calculate their divisors, and determine their values at cusps not in the support. So finding equations relating these functions and hence equations for the curves themselves and the maps between them is only a matter of comparing $q$-expansions. The following is a table of data obtained by these methods which will be used in the subsequent examples.

$X_0(3)$

- genus: 0
- cusps: 0 and $\infty$
- parameter: $H_3 = (\frac{\eta_1}{\eta_3})^{12}$
- divisor: $(H_3) = (0) - (\infty)$

$X_0(4)$

- genus: 0
- cusps: $0, \frac{1}{2}, \infty$
- parameter: $H_4 = (\frac{\eta_1}{\eta_4})^8$
- divisor: $(H_4) = (0) - (\infty)$
- other values: $H_4(\frac{1}{2}) = -16$
CHAPTER 7. GETTING MODELS FOR MODULAR CURVES

\[ X_0(5) \]
genus: 0
cusps: 0 and \( \infty \)
parameter: \( H_5 = \left( \frac{\eta(1)}{\eta(5)} \right)^6 \)
divisor: \( (H_5) = (0) - (\infty) \)

\[ X_0(7) \]
genus: 0
cusps: 0 and \( \infty \)
parameter: \( H_7 = \left( \frac{\eta(1)}{\eta(7)} \right)^4 \)
divisor: \( (H_7) = (0) - (\infty) \)

\[ X_0(10) \]
genus: 0
cusps: 0, \( \frac{1}{2}, \frac{1}{5}, \infty \)
parameter: \( H_{10} = \left( \frac{\eta(1)}{\eta(2)}(\eta(10))^2 \right)^4 \)
divisor: \( (H_{10}) = (0) - (\infty) \)
other values: \( H_{10}(\frac{1}{2}) = -5 \) and \( H_{10}(\frac{1}{5}) = -4 \)

Equation for \( \pi_1 : X_0(10) \to X_0(5) \)

\[ \pi_1^* H_5 = \frac{H_{10}^2 (H_{10} + 5)}{(H_{10} + 4)^2} \]

\[ X_0(20) \]
genus: 1
cusps: 0, \( \frac{1}{2}, \frac{1}{4}, \frac{1}{5}, \frac{1}{10}, \infty \)
parameters: \( x = \frac{(\eta(2))^2 (\eta(10))^2}{(\eta(2))^2 (\eta(20))^3} \) and \( y = \frac{(\eta(2))^2 (\eta(4) (\eta(5))^2 (\eta(10)))}{(\eta(2))^2 (\eta(20))^3} \)
divisors: \( (x) = 2(\frac{1}{1}) - 2(\infty) \), \( (y) = (\frac{1}{2}) + (\frac{1}{4}) + (\frac{1}{5}) - 3(\infty) \)

\( (x, y) \) coordinates of cusps:

\[ \{0, \frac{1}{2}, \frac{1}{4}, \frac{1}{5}, \frac{1}{10}, \infty\} \leftrightarrow \{(5,20), (5,0), (0,0), (1,0), (1,4), \infty\} \]

Equation for curve:

\[ y^2 = x^3 + 4xy - 6x^2 + 5x \]

Equation for \( \pi_1 : X_0(20) \to X_0(10) \)

\[ \pi_1^* H_{10} = \frac{y - 5x + 5}{x - 1} \]

Equation for \( \pi_1 : X_0(20) \to X_0(4) \)

\[ \pi_1^* H_4 = \frac{(x - 5)(y - 5x + 5)^2}{x^2y} \]

\[ X_0(21) \]
7.5. MODELS FOR $X_0(N)$

**Genus:** 1

**Cusps:** $0, \frac{1}{3}, \frac{1}{7}, \infty$

**Parameters:** $x = \frac{(\eta_7)(\eta_3)^3}{(\eta_1)(\eta_21)}$ and $y = x^2 - \frac{(\eta_3)(\eta_7)^7}{(\eta_1)(\eta_21)}$

**Divisors:** $(x) = 2(\frac{1}{3}) - 2(\infty), (x^2 - y) = 4(\frac{1}{7}) - 4(\infty)$

$(x, y)$ coordinates of cusps:

$$\{0, \frac{1}{3}, \frac{1}{7}, \infty\} \rightarrow \{(7, 22), (0, 1), (1, 1), \infty\}$$

**Equation for curve:**

$$y^2 = x^3 + 3xy - 8x^2 + 2y + 4x - 1$$

**Equation for $\pi_1 : X_0(21) \rightarrow X_0(7)$**

$$\pi_1^*H_7 = \frac{xy - 7x^2 + 7y + 6x - 7}{x^2 - y}$$

**Equation for $\pi_1 : X_0(21) \rightarrow X_0(3)$**

$$\pi_1^*H_3 = \frac{(x^2 - 7y + 21x - 42)(y - 3x - 1)^3(x^2 - y)}{(x - 1)^3x^5}$$
Chapter 8

Example 1

8.1 A Weight 5 Newform on \( X_1(4) \)

There is only one nontrivial character of level 4, call it \( \epsilon \). Then we have a weight one form for \( \Gamma_1(4) \) with character \( \epsilon \) whose \( q \)-expansion is given by the formula:

\[
E_{1,4,\epsilon}(q) = 1 - \frac{2}{B_{1,\epsilon}} \cdot \sum_{n=1}^{\infty} (\sum_{d|n} \epsilon(d))q^n = 1 + 4q + 4q^2 + 4q^4 + 8q^5 + \cdots \tag{8.1}
\]

Here \( B_{1,\epsilon} \) is the generalized Bernoulli number which one easily calculates to be \(-1/2\). Now, \( S_5(\Gamma_1(4)) \) is a one dimensional vector space generated by the newform whose \( q \)-expansion is given by \( E_{1,4,\epsilon}^{-1}(q)(\text{eta}2)^{12} \). Using the formula from the previous section we have:

\[
(\text{eta}2)^{12} = q \prod_{n=1}^{\infty} (1 - q^{2n})^{12} = q - 12q^3 + 54q^5 - 88q^7 \cdots \tag{8.2}
\]

Taking the quotient of the two forms we find that the newform we are looking for of weight 5 for \( \Gamma_1(4) \) has following \( q \)-expansion.

\[
f(q) = f_{5,4,\epsilon}(q) = q - 4q^2 + 16q^4 - 14q^5 \cdots \tag{8.3}
\]

Of course we are only interested in exceptional forms (mod \( p \)) so we need to check two things. First we should have \( k = p \) where \( k \) is the weight. This form is weight 5 and defined over \( \mathbb{Z}[1/4] \). Since 4 is invertible (mod 5) we can clearly reduce the coefficients to obtain the \( q \)-expansion of a form defined over \( \mathbb{F}_5 \). Now, we also must have \( \epsilon(p) = a_p^2, \epsilon(5) = 1 \) and \( a_5 = -14 \equiv 1 \), so this form is in fact exceptional.

To apply the main theorem and determine whether \( \rho_{f,p} \) is split, there are two inner products which we must actually work out. First we will find expansions for the differentials \( v_f \) and \( v_{f'} \) on \( I = I_1(4) \) at the supersingular points, and use the formula from \([G]\) to calculate \( \langle [f],[f'] \rangle_{I} \). If this inner product were
A Good Model for $I_1(4)$

From Gross we know that the Igusa curve $I_1(4)$ in characteristic 5 is a moduli scheme for elliptic curves together with embeddings of $\mathbb{Z}/4\mathbb{Z}$ and $\mu_5$. It is a degree 4 extension of $X_1(4) = X_0(4)$, totally ramified at the 2 supersingular points and unramified elsewhere. Also, since $X_1(20)$ is of genus 3 and it reduces to 2 isomorphic copies of $I_1(4)$ intersecting at the supersingular points, we know that the genus of $I_1(4)$ must be 1. Finally, we know that the Hass invariant $A$ with $A(q) = 1$ splits as $A = a^4$. So the $q$-expansion of any form on $X_1(4)$ is actually the $q$-expansion of a function on $I_1(4)$ since we can simply divide the weight $k$ form by $a^k$. We will use this last fact to get the $q$-expansion of a function on $I_1(4)$ which generates a degree 4 extension over the function field of $X_1(4)$. Provided the new curve is nonsingular at the supersingular points, it will be a suitable model for the calculation of the inner product. Then we need only determine which differentials correspond to the forms $f$ and $f'$ and take the inner product of the corresponding classes $[f]$ and $[f']$ using the formula from [G].

Recall the weight 1 form $E_{1,4,\epsilon}$ on $X_1(4)$. Dividing this form by $a$ we obtain a function on $I_1(4)$ which we call $y$. Then $y^4$ is a function on $X_1(4)$ whose divisor we will now calculate. First we compare $E_{1,4,\epsilon}^6$ with the weight 6 form on $X_1(4)$ whose $q$-expansion is given by $(\eta \tau^2)^{12}$. It is easy to show that the divisor of this eta product is simply $(0) + \left(\frac{1}{2}\right) + (\infty)$. Therefore the quotient is a function on $X_1(4)$, call it $g$, with at most a simple pole at each cusp. Comparing $q$-expansions we find:

$$g \cdot H_4 \cdot (H_4 + 16) = H_4^3 + 48H_4^2 + 768H_4 + 4096 = (H_4 + 16)^3$$

Therefore the divisor of $g$ is $2\left(\frac{1}{2}\right) - (0) - (\infty)$. This means the divisor of $E_{1,4,\epsilon}^6$ is $3\left(\frac{1}{2}\right)$ and in particular the divisor of $E_{1,4,\epsilon}^4$ must be $2\left(\frac{1}{2}\right)$.

Now, since we know the divisor of $a^4 = A$ on $X_1(4)$ is just $ss$, the divisor of $y^4$ on $X_1(4)$ is just $2\left(\frac{1}{2}\right) - ss$. On $X_1(4)$ both supersingular points satisfy $H_4^2 + H_4 + 1 = 0$. Also, $H_4\left(\frac{1}{2}\right) = -16 \equiv -1 \pmod{5}$. Therefore, we must have the equation:

$$y^4 = \frac{c(H_4 + 1)^2}{H_4^2 + H_4 + 1} \quad (8.4)$$

By comparing $q$-expansions we see that the constant $c$ is equal to 1. Since $y$ generates a degree 4 extension, it generates the whole extension of function fields from $X_1(4)$ up to $I_1(4)$. Furthermore, it is easy to check that
this model for $I_1(4)$ is nonsingular at the supersingular points. Therefore we can use it to calculate the inner product $<[f],[f']>_{I_1}$. But first we must figure out what the differentials $v_f$ and $v_{f'}$ are in terms of the two parameters, $H_4$ and $y$.

### 8.3 Differentials $v_f$ and $v_{f'}$ on $I_1(4)$

$f$ is a weight 5 form so $f/a^3$ is actually the weight 2 form which corresponds to the differential $v_f$. Comparing modular forms we have:

$$
\frac{f}{a^3} \cdot y = \frac{(\text{eta}2)^{12}}{E_{1,4,e}a} \cdot \frac{E_{1,4,e}a}{a} = \frac{(\text{eta}2)^{12}}{a^4} = \frac{(\text{eta}2)^{12}}{A}
$$

But this is a weight 2 form on $X_1(4)$ which as a form has divisor $\text{cusps} - ss$. Therefore $v_f \cdot y(H_4^2 + H_4 + 1)$ is the pullback of a differential on $X_1(4)$ with divisor $-2(\infty)$. So we must have:

$$
v_f = \frac{c \cdot dH_4}{y(H_4^2 + H_4 + 1)} \tag{8.5}
$$

for some constant $c$. By comparing $q$-expansions we find that $c = -1$.

The modular form $f'$ in the exceptional case is simply $\theta f$. Since $f$ was a weight 5 form and we are in characteristic 5, this means that $f'$ has weight $5 + 5 + 1 = 11$. So the differential $v_{f'}$ is the differential corresponding to the weight 2 form given by $f'/a^9$. However, the $q$ expansion of $f'$ is what one gets upon applying the $\theta$ operator to the function $f/a^5$. Therefore the differential $v_{f'}$ is also equal to the exact differential, $d(f/a^5)$. So what we need to know is which function in terms of the parameters, $H_4$ and $y$, is equal to the function $f/a^5$. Again comparing modular forms we have:

$$
\frac{f}{a^5} = \frac{(\text{eta}2)^{12}}{(E_{1,4,e})a^5} = \left( \frac{E_{1,4,e}}{a} \right) \cdot \frac{12}{(E_{1,4,e})^2a^3} = y \cdot \frac{(\text{eta}2)^{12}}{(E_{1,4,e})^2A}
$$

If we forget about the $y$, the rest of this function lives on $X_1(4)$ where it has the divisor $\text{cusps} - (\frac{1}{2}) - ss$. Therefore for some constant $c$ we must have:

$$
\frac{f}{a^5} = \frac{c \cdot yH_4}{H_4^2 + H_4 + 1}
$$

Upon comparing $q$-expansions we see that $c = 1$. Therefore we have:

$$
v_{f'} = d\left( \frac{yH_4}{H_4^2 + H_4 + 1} \right) \tag{8.6}
$$
8.4 Computing $<[f],[f']>_I$ on $I_1(4)$

The formula of Gross for the inner product $<[f],[f']>_I$ requires at least the beginning of a power series expansion for both differentials at each of the two supersingular points. This means we need to choose a uniformizing parameter at each of these supersingular points before we can begin. We know that the function $y$ has a simple pole at each supersingular point, so $1/y$ makes a perfectly good uniformizing parameter at both places. We begin by calculating $dH_4$ in terms of $dy$ from the equation relating $y$ and $H_4$.

\[
y^4 = \frac{(H_4+1)^2}{H_4^2+H_4+1} \]
\[
4y^3dy = \frac{(H_4^2+H_4+1)^2(2H_4+1)^2(H_4+1)}{(H_4^2+H_4+1)^2} dH_4
\]
\[
= \frac{1-H_4^2}{(H_4^2+H_4+1)} dH_4
\]
\[
dH_4 = \frac{(H_4^2+H_4+1)^2}{1-H_4^2} (4y^3)dy
\]

Now we plug into the formula for $v_f$:

\[
v_f = \frac{-1}{y(H_4^2+H_4+1)} \frac{(H_4^2+H_4+1)^2}{1-H_4^2} (4y^3)dy
\]
\[
= \frac{4y^2(H_4^2+H_4+1)}{H_4^2-1} dy
\]
\[
= \frac{4(H_4+1)^2}{H_4^2-1} \frac{dy}{y^2}
\]
\[
= -4 \frac{H_4+1}{H_4^2-1} d\left(\frac{1}{y}\right)
\]

Let $\alpha_1$ and $\alpha_2$ be the values of $H_4$ at the two supersingular points, i.e. the distinct roots of $H_4^2 + H_4 + 1$. The expansions of $v_f$ at these two points begin:

\[
v_f = (-4 \cdot \frac{\alpha_1+1}{\alpha_1-1} + \cdots) d(1/y)
\]
\[
v_f = (-4 \cdot \frac{\alpha_2+1}{\alpha_2-1} + \cdots) d(1/y)
\]
Now we will attempt to do the same for \( v_f' \).

\[
v_f' = \frac{d \left( \frac{y H_4}{H_4 + H_4 + 1} \right)}{(H_4^2 + H_4 + 1)^2}
= \frac{y (1 - H_4^2)}{(H_4^2 + H_4 + 1)^2} \cdot dH_4 + \frac{H_4}{H_4 + 1} dy
= 4 y^4 dy + \frac{H_4 y^4}{(H_4 + 1)^2} dy
= y^4 \left( \frac{4 (H_4 + 1)^2 + H_4}{(H_4 + 1)^2} \right) dy
= y^4 \left( \frac{-H_4^2 + H_4 + 1}{(H_4 + 1)^2} \right) dy
= -dy
= (1/y)^{-2} d(1/y)
\]

So the expansions of \( v_f' \) at the two supersingular points are identically:

\[
v_f' = (1/y)^{-2} d(1/y)
\]

Plugging directly into the formula of Gross we now have:

\[
< [f], [f'] > = -4 \cdot \frac{a_1 + 1}{a_1 - 1} \cdot 1 + (-4 \cdot \frac{a_2 + 1}{a_2 - 1}) \cdot 1
= -4 \left( \frac{(a_1 + 1)(a_2 - 1) + (a_2 + 1)(a_1 - 1)}{(a_1 - 1)(a_2 - 1)} \right)
= -4 \left( \frac{2a_1 a_2 - 2}{a_1 a_2 - (a_1 + a_2) + 1} \right)
= -4 \left( \frac{2(1) - 2}{(1) - (-1) + 1} \right)
= 0
\]

Again, if this inner product had been nontrivial, we would know that \( \rho_{f,p} \) was nonsplit without going any further. Since it is trivial, though, we must also check the inner product in \( H^0(X_1(20), \Omega) \). In particular we must find the differentials corresponding to \( F \) and \( F' \) on some model for \( X_1(20) \) and take their inner product using Coleman’s formula. The representation will be split if this inner product is sufficiently trivial.

### 8.5 A Good Model for \( X_1(20) \)

We already have a very good model for \( X_0(20) \) as well as equations for various maps down to smaller modular curves. So all we have left to do is generate the extension of function fields from \( X_0(20) \) up to \( X_1(20) \). This extension has Galois group \( (\mathbb{Z}/20\mathbb{Z})^*/ \langle \pm 1 \rangle \) so it is cyclic of degree 4. Therefore it is generated by some function \( v \) on \( X_1(20) \) whose fourth power is a function on \( X_0(20) \). We
will find such a \( v \) initially by dividing two weight one forms on \( X_1(20) \). Then we will calculate the divisor of \( v^4 \) as a function on \( X_0(20) \). At this point then we could find an equation of the form \( v^4 = f(x, y) \) and take \( v \) to be our third parameter. However we will simplify our equation by first multiplying \( v \) by an appropriate function on \( X_0(20) \) to obtain a nicer parameter, \( u \).

Recall that we have a weight 1 form on \( X_1(4) \) given by:

\[
E_{1,4,\epsilon}(q) = 1 + 4 \sum_{n=1}^{\infty} (\sum_{d|n} \epsilon(d)) q^n
\]  

We also have a weight 1 form on \( X_1(5) \) with character \( \tau \) determined by \( \tau(2) = i \). Its \( q \)-expansion is given by:

\[
E_{1,5,\tau}(q) = 1 + (3 - i) \sum_{n=1}^{\infty} (\sum_{d|n} \tau(d)) q^n
\]  

The quotient, \( v \), is a function on \( X_1(20) \). Since it has a character of exponent 4, it must generate the desired extension over the function field of \( X_0(20) \). Calculating the divisor of \( v^4 \) directly is too difficult, but there is an easier way. First we will figure out the divisors of \( E_{1,4,\epsilon}^4 \) on \( X_0(4) \) and \( E_{1,5,\tau}^4 \) on \( X_0(5) \). Then we can pull back by the maps down from \( X_0(20) \) and subtract to get the divisor of the quotient, \( v^4 \).

We have already determined the divisor of \( E_{1,4,\epsilon}^4 \) on \( X_0(4) \), namely \( 2(\frac{1}{2}) \). We have only to pull back by the map \( \pi_1 : X_0(20) \to X_0(4) \). Since the divisor of \( E_{1,4,\epsilon}^4 \) is supported on the cusps this is very easy. Using the methods of the previous chapter we see that two cusps of \( X_0(20) \) lie over the cusp \( \frac{1}{2} \) by the map \( \pi_1 \), namely \( \frac{1}{2} \) and \( \frac{1}{20} \). Furthermore, \( e_{\pi_1}(\frac{1}{2}) = 5 \) and \( e_{\pi_1}(\frac{1}{20}) = 1 \). Therefore the divisor of \( E_{1,4,\epsilon}^4 \) on \( X_0(20) \) must be \( 2(\frac{1}{2}) + 10(\frac{1}{20}) \).

There is a very convenient weight 4 form on \( X_0(5) \) whose \( q \)-expansion is given by the eta product \((\text{eta1})^4(\text{eta5})^4 \). It is easily shown to have divisor \((\infty) + (0)\). So the quotient \( g = E_{1,5,\tau}^4/(\text{eta1})^4(\text{eta5})^4 \) is a function with at most a simple pole at both cusps. Using the parameter \( H_5 \) and comparing \( q \)-expsansions we find that:

\[
g \cdot H_5 = H_5^2 + (22 - 4i)H_5 + 117 - 44i = (H_5 + 11 - 2i)^2
\]

Therefore the divisor of \( g \) must be \( 2H_{10}^{-1}(-11 + 2i) - (\infty) - (0) \). But this means the divisor of \( E_{1,5,\tau}^4 \) must be \( 2H_{10}^{-1}(-11 + 2i) \).

Now we will pull back by the map \( \pi_2 : X_0(10) \to X_0(5) \). Since the divisor is supported on a noncusp point, we must use the explicit formula given in the previous chapter for \( \pi_2^*H_5 \) in terms of \( H_{10} \). We find that there are two points lying above \( H_{10}^{-1}(-11 + 2i) \), namely \( H_{10}^{-1}(-6 + 2i) \) and \( H_{10}^{-1}(-4 - 2i) \), with ramification indices 2 and 1 respectively. Therefore on \( X_0(10) \) the divisor of \( E_{1,5,\tau}^4 \) is given by:

\[
(E_{1,5,\tau}^4) = 4(H_{10} + 6 - 2i) + 2H_{10}^{-1}(-4 - 2i) + 4(\infty)
\]
CHAPTER 8. EXAMPLE 1

Now we are ready to pull back again via $\pi_1: X_0(20) \to X_0(10)$. We find that there is only one point lying above $H_{10}^{-1}(-4 - 2i)$ with $x$ and $y$ coordinates $(-1 + 2i, 2 + 6i)$. The ramification index is of course equal to the degree of the map which is 2. The cusp $\infty$ splits as $\infty$ and $\frac{1}{10}$. Therefore the divisor of $E_{1,5,\tau}^4$ on $X_0(20)$ is given by:

$$E_{1,5,\tau}^4 = 4(H_{10} + 6 - 2i) + 4(-1 + 2i, 2 + 6i) + 4(\infty) + 4(\frac{1}{10})$$

So the divisor of $v^4 = E_{1,4,\epsilon}^4/E_{1,5,\tau}^4$ is given by:

$$(v^4) = 10\left(\frac{1}{2}\right) - 2\left(\frac{1}{10}\right) - 4(\infty) - 4(-1 + 2i, 2 + 6i) - 4(H_{10} + 6 - 2i)$$

We can obviously simplify things by multiplying $v$ by $(H_{10} + 6 - 2i)$. Two other functions which are very convenient for us to use are (listed along with their divisors):

$$(x + y - 5) = 2\left(\frac{1}{2}\right) + \left(\frac{1}{10}\right) - 3(\infty)$$

$$(y + (i - 2)x - (i + 2)) = \left(\frac{1}{10}\right) + (-1 + 2i, 2 + 6i) + (1 - 2i, 2 - 4i) - 3(\infty)$$

So our final choice of parameter is:

$$u = \frac{E_{1,4,\epsilon}(H_{10} + 6 - 2i)(y + (i - 2)x - (i + 2))}{E_{1,5,\tau}(y + x - 5)}$$

(8.9)

Then we have:

$$(u^4) = 2\left(\frac{1}{2}\right) - 2\left(\frac{1}{10}\right) + 4(1 - 2i, 2 - 4i) - 4(\infty)$$

(8.10)

and

$$u^4 = \frac{(y + x - 5)(y - x + 1)(x - (1 - 2i))^2}{(x - 1)^3}$$

(8.11)

8.6 Holomorphic Differentials on $X_1(20)$

Now that we have a good model for $X_1(20)$ we are almost ready to calculate the inner product $(F, F')$ using Coleman’s formula. All we have to do first is figure out which holomorphic differentials on our model correspond to $F$ and $F'$, and then find suitable uniformizing parameters for the supersingular annuli. After that it will be a simple, but lengthy and tedious, $p$-adic calculation. So, let us turn our attention to the holomorphic differentials on our model for $X_1(20)$.

We have one obvious way to get holomorphic differentials, and that is to pull back the holomorphic differentials on $X_0(20)$ by $\pi_1$, the forgetful map. Since our equation is in Weierstrass form, it is easy to show that a basis for these differentials is $-\frac{dx}{2(\sqrt{5}x^3 - 6y)}$. So we will immediately take $\omega_0$ to be the pullback by $\pi_1$ of this differential. However, this only gives us a one dimensional vector space, when we know that the total dimension of holomorphic differentials is
3. Fortunately there is a sneaky way to get two more linearly independent holomorphic differentials, \( \omega_1 \) and \( \omega_2 \), from \( \omega_0 \).

We start by calculating the divisors of the differential \( \omega_0 \) and the function \( u \) on \( X_1(20) \). Looking at the divisor of \( u^4 \) as a function on \( X_0(20) \), we see that any point lying above the cusps \( \frac{1}{2} \) and \( \frac{3}{10} \) must have ramification index 2 or 4 (the degree of the extension is 4). Using the Hurwitz genus formula then it is easy to show that both cusps must split into two points with ramification index exactly 2, and that the extension is unramified elsewhere. So let \( A_{\frac{1}{2}}, B_{\frac{1}{2}}, A_{\frac{3}{10}}, \) and \( B_{\frac{3}{10}} \) be those points. Then the divisor of \( u \) must be:

\[
(u) = (A_{\frac{1}{2}}) + (B_{\frac{1}{2}}) - (A_{\frac{3}{10}}) - (B_{\frac{3}{10}}) + \pi_1^*((1 - 2i, 2 - 4i) - (\infty))
\]

Furthermore, knowing the ramification makes the divisor of \( \omega_0 \) a simple calculation:

\[
(\omega_0) = (A_{\frac{1}{2}}) + (B_{\frac{1}{2}}) + (A_{\frac{3}{10}}) + (B_{\frac{3}{10}})
\]

Now, we want to reduce the problem to finding functions on \( X_0(20) \) so we start by noticing the following fact:

\[
(u\omega_0) = \pi_1^*\left(\frac{1}{2} + (1 - 2i, 2 - 4i) - (\infty)\right)
\]

So if we find a function \( g_1 \) on \( X_0(20) \) with divisor at least \((\infty) - (1 - 2i, 2 - 4i) - (\frac{1}{2})\), and Riemann-Roch tells us there is one, we can get a new holomorphic differential by taking:

\[
\omega_1 = g_1 \cdot u \cdot \omega_0
\]

With a little arithmetic one comes up with the desired function:

\[
g_1 = \frac{x + 2i + 1}{y - ix + 5i}
\]

Using the same reasoning one finds a third holomorphic differential by taking:

\[
\omega_2 = \left(\frac{y - (2 + i)x + (2 + i)}{x - 1}\right) \cdot \frac{1}{u} \cdot \omega_0
\]

Now we have a basis for the holomorphic differentials on \( X_1(20) \), but we don’t know which holomorphic differentials correspond to the weight 2 forms, \( F \) and \( F' \). We know that \( F \) and \( F' \) are newforms which reduce (mod 5) to \( f \) and \( f' \). So we want to get a basis of newforms for \( S_2(\Gamma_1(20)) \). To do this it suffices to look at \( q \) expansions of the \( \omega_i \) and diagonalize using one or more Hecke Operators.

\[
\omega_0(q) = q - 2q^3 - q^5 + 2q^7 + \cdots
\]
\[
\omega_1(q) = q + (-1 + i)q^2 + (-2i)q^4 + (-2 - i)q^5 + \cdots
\]
\[
\omega_2(q) = q + (-1 - i)q^2 + (2i)q^4 + (-2 + i)q^5 + \cdots
\]

We know that complex conjugation should preserve newforms, so one might be suspicious that the \( \omega_i \) are already newforms. One needs only look at the action
of the operator $U_2$ to confirm this suspicion. Furthermore, if we choose $i$ to be congruent to 2 (mod 5) we find that $\omega_1$ reduces to $f$ and $\omega_2$ reduces to $f' = df$. If we choose $i$ to be congruent to $-2$ (mod 5) the reverse happens.

8.7 Supersingular Annuli on $X_1(20)$

Now that we know which differentials we are working with, the next thing we need is a parameterization of the supersingular region of $X_1(20)$. We know that the supersingular region will consist of two annuli since there are two supersingular points (mod 5). So what we are really looking for is a uniformizing parameter for each of these supersingular annuli. Again, we will make heavy use of our models for $X_0(N)$ and the maps between them.

On $X(1)$ the supersingular region is given by $v(j) > 0$, so it is a disc. First we step up to $X_0(5)$ using the map:

$$j = H_5 + 5^3 \cdot 2 + \frac{5^5 \cdot 7 \cdot 3^2}{H_5} + \frac{5^8 \cdot 13 \cdot 2^2}{H_5^2} + \frac{5^{10} \cdot 7 \cdot 3^2}{H_5^3} + \frac{5^{13} \cdot 2 \cdot 3}{H_5^4} + \frac{5^{15}}{H_5^5}$$

By simply comparing valuations term by term, we see that the inverse image of the disc on $X(1)$ is the annulus, $0 < v(H_5) < 3$. Now we step up to $X_0(10)$ using the map:

$$H_5 = \frac{H_{10}^2(H_{10} + 5)}{(H_{10} + 4)^2}$$

Again, by comparing valuations, we see that the inverse image of the annulus on $X_0(5)$ is the annulus $0 < v(H_{10}) < 1$. At this point things get a little more difficult.

First we step up to $X_0(20)$ using the map:

$$\pi_1^* H_{10} = \frac{y - 5x + 5}{x - 1}$$

and the equation for the curve, $y^2 = x^3 + 4xy - 6x^2 + 5x$. By comparing valuations we find that the points lying above the supersingular region of $X_0(10)$ are exactly those with $0 < v(x) < 1$. The key to understanding this region is to look at the equation for the curve as a quadratic polynomial in $y$. As such, it has the following discriminant:

$$d = 4x^2(-2 + (x + \frac{5}{x}))$$

This has two distinct analytic square roots on the annulus $0 < v(x) < 1$ corresponding to the two distinct choices for $\sqrt{-2}$. So the supersingular region on $X_0(20)$ is actually the union of 2 width-1 annuli, given philosophically by the formula:

$$A_\pm : t \to (t, 2t \pm t\sqrt{-2 + (t + \frac{5}{t})})$$
8.8. **COMPUTING** \((F, F|W_{\zeta_p})_\infty\) **ON** \(X_1(20)\)  

and more precisely by the formula:

\[ A_\pm : t \to (t, 2t \pm t \cdot \sqrt{-2}(5t^{-1} + 21 + t + 7t^2 + \cdots)) \]

Here the coefficients of the series are really in \(\mathbb{Z}_5\) but are given (mod 25) and will be given (mod 25) for the rest of this example. This precision will turn out to be sufficient for our purposes.

Now, when we step up to \(X_1(20)\) we are adjoining a fourth root of some function on \(X_0(20)\) according to Equation 8.11. In terms of the parameter \(t\) this is the same as adjoining a fourth root of the analytic function given by the series expansion:

\[ u^4 = (20 \pm 5\sqrt{-2}) + (8 \pm \sqrt{-2})t + (22 \pm 2\sqrt{-2})t^2 + (14 \pm 23\sqrt{-2})t^3 + \cdots \]

This is equivalent to adjoining a fourth root of \(t\). Therefore the two supersingular annuli are totally ramified in the extension from \(X_0(20)\) to \(X_1(20)\) and we can choose as a new parameter any fourth root of \(t\), which we will call \(s\). To be more specific, the two annuli \(A_\pm\) are now of width 1/4 and given by the formula:

\[
\begin{align*}
x &= s^4 \\
y &= 2s^4 \pm s^4 \cdot \sqrt{-2}(5s^{-4} + 21 + 7s^8 + \cdots) \\
u &= (20 \pm 10\sqrt{-2})s^{-3} + (6 \pm 11\sqrt{-2})s + (23 \pm 16\sqrt{-2})s^5 + \cdots
\end{align*}
\]

8.8 **Computing** \((F, F|w_{\zeta_p})_\infty\) **on** \(X_1(20)\)

In terms of the parameters, \(x, y,\) and \(u\), the two holomorphic differentials corresponding to \(F\) and \(F'\) are given by the formulae:

\[
\begin{align*}
F &= \frac{x + 15}{y - 7x + 10} \cdot u \cdot \frac{dx}{-2(y - 2x)} \\
F' &= \frac{y - 9x + 9}{x - 1} \cdot \frac{1}{u} \cdot \frac{dx}{-2(y - 2x)}
\end{align*}
\]

So after a little arithmetic we find that their expansions in terms of the parameter \(s\) are given by:

\[
\begin{align*}
F &= ((15 \pm 20\sqrt{-2})s^{-3} + (16 \pm 16\sqrt{-2})s + (21 \pm 4\sqrt{-2})s^5 + \cdots) \frac{ds}{s} \\
F' &= ((5 \pm 10\sqrt{-2})s^{-5} + (9 \pm 17\sqrt{-2})s^{-1} + (1 \pm \sqrt{-2})s^3 + \cdots) \frac{ds}{s}
\end{align*}
\]

As expected the two forms have zero residue, so we are able to apply the formula for \((F, F')_\infty\). Over each annulus we must sum up \(a_i b_{-i}\) where the \(a_i\)'s and \(b_i\)'s are the coefficients of \(F\) and \(F'\) after factoring out \(\frac{ds}{\pi}\). Then we add the
results from the two annuli. On $A_+$ we get:

\[
\sum a_i b_{-i} = (5 + 10 \sqrt{-2})(21 + 4 \sqrt{-2}) + \\
(9 + 17 \sqrt{-2})(16 + 16 \sqrt{-2}) + (1 + \sqrt{-2})(15 + 20 \sqrt{-2})
\]

\[= 5 \sqrt{-2} + 16 \sqrt{-2} + 10 \sqrt{-2}
\]

\[= 6 \sqrt{-2}
\]

On $A_-$ we get:

\[
\sum a_i b_{-i} = (5 - 10 \sqrt{-2})(21 - 4 \sqrt{-2}) + \\
(9 - 17 \sqrt{-2})(16 - 16 \sqrt{-2}) + (1 - \sqrt{-2})(15 - 20 \sqrt{-2})
\]

\[= - 5 \sqrt{-2} - 16 \sqrt{-2} - 10 \sqrt{-2}
\]

\[= - 6 \sqrt{-2}
\]

What we have just shown is that $(F, F')_\infty$ is trivial (mod 25). Since $F|_{w_{\zeta_p}}$ is equal to $c_\zeta F'$ for some integral constant $c_\zeta$, we have also shown that $(F, F|_{w_{\zeta_p}})_\infty$ is divisible not only by $\pi^p$ but in fact by $\pi^{p+1}$. Therefore we can conclude by the main theorem the that representation $\rho_{f,p}$ is indeed split.
Chapter 9

Example 2

9.1 A Weight 7 Newform on $X_1(3)$

There is only one nontrivial character of level 3, call it $\epsilon$. Then we have a weight one form for $\Gamma_1(3)$ with character $\epsilon$ whose $q$-expansion is given by the formula:

$$E_{1,3,\epsilon}(q) = 1 - \frac{2}{B_{1,\epsilon}} \sum_{n=1}^{\infty} \left( \sum_{d|n} \epsilon(d) \right) q^n = 1 + 6q + 6q^3 + 6q^4 + 12q^7 + \cdots$$

(9.1)

Here $B_{1,\epsilon}$ is the generalized Bernoulli number which one easily calculates to be $-1/3$. Now, $S_7(\Gamma_1(3))$ is a one dimensional vector space generated by the newform whose $q$-expansion is given by $E_{1,3,\epsilon}(q)(\text{eta}1)^6(\text{eta}3)^6$. Using the formula for the $q$-expansion of an eta product we have:

$$(\text{eta}1)^6(\text{eta}3)^6 = \left( q^{1/4} \prod_{n=1}^{\infty} (1 - q^n)^6 \right) \left( q^{3/4} \prod_{n=1}^{\infty} (1 - q^{3n})^6 \right)$$

(9.2)

Taking the product of the two $q$-expansions we find that the newform we are looking for of weight 7 for $\Gamma_1(3)$ has the following $q$-expansion:

$$f(q) = f_{7,3,\epsilon}(q) = q - 27q^3 + 64q^4 - 286q^7 + \cdots$$

(9.3)

Now, since the form is defined over $\mathbb{Z}[1/3]$ and 3 is invertible (mod 7), we can clearly reduce to get a form defined over $\mathbb{F}_7$. We must also check to see that $\epsilon(7) = a_7^2$. $\epsilon(7) = \epsilon(1) = 1$ and we see that $a_7 = -286 \equiv 1$. So the form is in fact exceptional.

As in the previous example, there are now two things which we must do with this form. First we will find the two differentials $v_f$ and $v_{f'}$ on $I_1(3)$ and take the inner product of the corresponding classes using the formula of Gross. If this inner product is nontrivial, we will know right away that $\rho_{f,p}$ is nonsplit by the main theorem. However, as in the first example, this inner product is in fact trivial, so we must proceed to checking the inner product $(F,F|w_{c_0})_\infty$ on $H^0(X_1(21),\Omega)$. This will tell us whether the representation is actually split.
9.2 A Good Model for $I_1(3)$

As in the previous example, we know that the Igusa curve $I_1(3)$ in characteristic 7 is a moduli scheme for elliptic curves together with embeddings of $\mathbb{Z}/3\mathbb{Z}$ and $\mu_7$. It is a degree 6 extension of $X_1(3) = X_0(3)$, totally ramified at the two supersingular points and unramified elsewhere. Also, since $X_1(21)$ is of genus 5 and reduces to 2 isomorphic copies of $I_1(3)$ intersecting at the supersingular points, we know that the genus of $I_1(3)$ must be 2. Finally, we know that the Hass invariant $A$ with $A(q) = 1$ splits as $A = a^6$. So the $q$-expansion of any form on $X_1(3)$ is actually the $q$-expansion of a function on $I_1(3)$ since we can divide the weight $k$ form by $a^k$. We will use this last fact to get a function on $I_1(3)$ which generates a degree 6 extension over the function field of $X_1(3)$. Provided the new curve is nonsingular at the supersingular points, it will be a suitable model for the calculation of the inner product. Then we need only determine which differentials correspond to the forms $f$ and $f'$ and take their inner product using the formula due to Gross.

Recall the weight 1 form $E_{1,3,\epsilon}$ on $X_1(3)$. Dividing this form by $a$ we obtain a function on $I_1(3)$ which we call $y$. Then $y^6$ is a function on $X_1(3)$ whose divisor we will now calculate. First we compare $E_{1,3,\epsilon}^6$ with the weight 6 form on $X_1(3)$ whose $q$-expansion is given by $(\eta_1)^6(\eta_3)^6$. It is easy to show that the divisor of this eta product is simply $(0) + (\infty)$. Therefore the quotient is a function on $X_1(3)$, call it $g$, with at most a simple pole at each cusp. Comparing $q$-expansions we find:

$$g \cdot H_3 = H_3^2 + 54H_3 + 729 = (H_3 + 27)^2$$

Therefore the divisor of $g$ is $2H_3^{-1}(-27) - (\infty) - (0)$. This means the divisor of $E_{1,3,\epsilon}^6$ must be $2H_3^{-1}(-27)$.

Now, since we know the divisor of $a^6 = A$ is just $ss$, the divisor of $y^6$ on $X_1(3)$ is just $2H_3^{-1}(-27) - 2s$. On $X_1(3)$ both supersingular points satisfy the equation $H_3^2 + 4H_3 + 1$. Therefore we must have the equation:

$$y^6 = \frac{c(H_3 + 27)^2}{H_3^2 + 4H_3 + 1} \quad (9.4)$$

By comparing $q$-expansions we see that the constant $c$ is equal to 1.

Since $y$ generates a degree 6 extension, it generates the whole extension of function fields from $X_1(3)$ up to $I_1(3)$. Furthermore, it is easy to check that this model for $I_1(3)$ is nonsingular at the supersingular points. Therefore we can use it to calculate the inner product $<[f],[f']>_I$. But first we must figure out what the differentials $v_f$ and $v_{f'}$ are in terms of the two parameters $H_3$ and $y$. 


9.3 Differentials \( v_f \) and \( v_f' \) on \( I_1(3) \)

\( f \) is a weight 7 form so \( f/a^5 \) is actually the weight 2 form which corresponds to the differential \( v_f \). Comparing modular forms we have:

\[
\frac{f}{a^5} \cdot y = \frac{E_{1,3,\epsilon}(\eta_1)^6(\eta_3)^6}{a^5} \cdot \frac{E_{1,3,\epsilon}}{a} = \frac{E_{1,3,\epsilon}^2(\eta_1)^6(\eta_3)^6}{A}
\]

But this is a weight 2 form on \( X_1(3) \). We have already seen that the divisor of \( E_{1,3,\epsilon}^2 \) is \( 2H_3^{-1}(-27) \), so the divisor of \( E_{1,3,\epsilon}^2 \) must be \( \frac{2}{3}H_3^{-1}(-27) \) (divisors of forms can be fractional at elliptic points). The divisor of this weight 2 form is then \( \frac{2}{3}H_3^{-1}(-27) + (0) + (\infty) - ss \). Using Shimura’s formula we know that the differential corresponding to this weight 2 form would then have divisor \(-ss\). Therefore \( v_f \cdot y(2H_3^2 + 4H_3 + 1) \) is the pullback of a differential on \( X_1(3) \) with divisor \(-2(\infty)\). So we must have:

\[
v_f = \frac{c \cdot dH_3}{y(H_3^2 + 4H_3 + 1)}
\]

for some constant \( c \). By comparing \( q \)-expansions we find that \( c = -1 \).

As in the first example, \( v_f' \) is an exact differential and is equal to \( d(f/a^7) \). So all we have to do is determine which function in terms of the parameters \( H_3 \) and \( y \) is equal to the function \( f/a^7 \). Again comparing modular forms we have:

\[
\frac{f}{a^7} = \frac{E_{1,3,\epsilon}(\eta_1)^6(\eta_3)^6}{a^7} \cdot \frac{E_{1,3,\epsilon}}{a} = \frac{(\eta_1)^6(\eta_3)^6}{A}
\]

If we forget about the \( y \), the rest of this function lives on \( X_1(3) \) where it has the divisor \((0) + (\infty) - ss\). Therefore for some constant \( c \) we must have:

\[
\frac{f}{a^7} = \frac{c \cdot yH_3}{H_3^2 + 4H_3 + 1}
\]

Upon comparing \( q \)-expansions we see that \( c = 1 \). Therefore we have:

\[
v_f' = d\left(\frac{yH_3}{H_3^2 + 4H_3 + 1}\right)
\]

9.4 Computing \( \langle [f], [f'] \rangle_I \) on \( I_1(3) \)

Again we will need at least the beginning of a power series expansion for the two differentials at each of the supersingular points before we can use the formula of Gross to calculate the inner product. So first we must fix a uniformizer at each of the two supersingular points. Again, the function \( y \) has a simple pole at each supersingular point, so \( 1/y \) makes a great uniformizer at both places. We begin then by calculating \( dH_3 \) in terms of \( dy \) from the equation relating \( y \) and
\[ y^6 = \frac{(H_3 + 27)^2}{H_3^2 + 4H_3 + 1} \]
\[ = \frac{(H_3 - 1)^2}{H_3^2 + 4H_3 + 1} \]
\[ 6y^5 \, dy = \frac{(H_3^2 + 4H_3 + 1)(2H_3 - 1) - (H_3 - 1)^2(2H_3 + 4)}{(H_3^2 + 4H_3 + 1)^2} \, dH_3 \]
\[ = \frac{1 - H_3^2}{(H_3^2 + 4H_3 + 1)^2} \, dH_3 \]
\[ dH_3 = \frac{(H_3^2 + 4H_3 + 1)^2}{1 - H_3^2} (6y^5) \, dy \]

Now we plug into the formula for \( v_f \):
\[ v_f = \frac{-1}{y(H_3^2 + 4H_3 + 1)} \frac{(H_3^2 + 4H_3 + 1)^2}{1 - H_3^2} (6y^5) \, dy \]
\[ = \frac{y(H_3^2 + 4H_3 + 1)}{1 - H_3^2} \, dy \]
\[ = \frac{(H_3 - 1)^2}{1 - H_3^2} \, dy \]
\[ = \frac{1}{y^2} \, dy \]
\[ = H_3 + 1 \, d\left( \frac{1}{y} \right) \]

Let \( \alpha \) and \( -4 - \alpha \) be the values of \( H_3 \) at the two supersingular points, i.e. the distinct roots of \( H_3^2 + 4H_3 + 1 \). The expansions of \( v_f \) at these two points begin:
\[ v_f = \left( \frac{\alpha - 1}{\alpha + 1} \right) d(1/y) \]
\[ v_f = \left( \frac{-5 - \alpha}{3 - \alpha} \right) d(1/y) \]

Now we will attempt to do the same for \( v_f' \).
\[ v_{f'} = d \left( \frac{yH_3}{H_3^2 + 4H_3 + 1} \right) \]
\[ = \frac{(H_3^2 + 4H_3 + 1)(yH_3 + H_3 \, dy) - yH_3(2H_3 + 4) \, dH_3}{(H_3^2 + 4H_3 + 1)^2} \]
\[ = \frac{y(1 - H_3^2)}{(H_3^2 + 4H_3 + 1)^2} \, dH_3 + \frac{H_3}{H_3^2 + 4H_3 + 1} \, dy \]
\[ = 6y^6 \, dy + \frac{H_3y^6}{(H_3 - 1)^2} \, dy \]
\[ = y^6 \left( \frac{6(H_3 - 1)^2 + H_3}{(H_3 - 1)^2} \right) \, dy \]
\[ = y^6 \left( \frac{6H_3^2 - 11H_3 + 6}{(H_3 - 1)^2} \right) \, dy \]
\[ = y^6 \left( \frac{-H_3^2 + 4H_3 + 1}{(H_3 - 1)^2} \right) \, dy \]
\[ = -dy \]
\[ = (1/y)^{-2} d(1/y) \]

So the expansions of \( v_{f'} \) at the two supersingular points are identically:
\[ v_{f'} = (1/y)^{-2} d(1/y) \]
Plugging directly into the formula of Gross we now have:

\[
< f, f' > = \left( \frac{a - 1}{a + 1} \right) \cdot 1 + \left( \frac{-5 - a}{-a} \right) \cdot 1
\]

\[
= \frac{(a - 1)(-3 - a) + (-5 - a)(a + 1)}{(a + 1)(-3 - a)}
\]

\[
= \frac{-2a^2 - 8a - 2}{a - 4}  
\]

\[
= \frac{-2(a^2 + 4a + 1)}{(a^2 + 4a + 1) - 2}
\]

\[
= 0
\]

Again, if this inner product had been nontrivial, we would know already by the main theorem that \( \rho_{f,p} \) was nonsplit. It is trivial, though, so we must also check the inner product in \( H^0(X_1(21), \Omega) \). In particular we must find the differentials corresponding to \( F \) and \( F' \) on a suitable model for \( X_1(21) \) and take their inner product using the formula from [C1]. Then \( \rho_{f,p} \) will be split if and only if this inner product is trivial enough.

9.5 A Good Model for \( X_1(21) \)

As in the previous example, we will obtain a model for \( X_1(21) \) by generating the extension of function fields up from the curve \( X_0(21) \). This extension has Galois group isomorphic to \((\mathbb{Z}/21\mathbb{Z})^*/\langle \pm 1 \rangle\) so it is cyclic of degree 6. So to generate the extension it will suffice to find a function on \( X_1(21) \) whose 6th power is a function on \( X_0(21) \), but no smaller power. As in the previous example we will obtain such a function by dividing two weight 1 forms on \( X_1(21) \).

Recall that we have a weight 1 form on \( X_1(3) \) given by

\[
E_{1,3,\epsilon}(q) = 1 + 6 \sum_{n=1}^{\infty} \sum_{d|n} \epsilon(d)q^n
\]  

(9.7)

We also have a weight 1 form on \( X_1(7) \) with character \( \tau \) determined by \( \tau(5) = -\omega \), where \( \omega \) is the primitive cube root of unity \( -\frac{1 + \sqrt{-3}}{2} \). Its \( q \)-expansion is given by:

\[
E_{1,7,\tau}(q) = 1 + (2 - \sqrt{-3}) \sum_{n=1}^{\infty} \sum_{d|n} \tau(d)q^n
\]  

(9.8)

The quotient, \( v \), is a function on \( X_1(21) \). Since it has character of exponent 6, it must generate the desired extension of function fields. Calculating the divisor of \( v^6 \) as a function on \( X_0(21) \) directly would again be very difficult. However, we have good maps down to \( X_0(7) \) and \( X_0(3) \). So we will first find the divisors of the forms \( E_{1,3,\epsilon}^6 \) and \( E_{1,7,\tau}^6 \) on the curves \( X_0(3) \) and \( X_0(7) \). Then we can pull back these divisors and subtract to get the divisor of \( v^6 \) on \( X_0(21) \).

We have already determined the divisor of \( E_{1,3,\epsilon}^6 \) on \( X_0(3) \), namely \( 2H_3^{-1}(\mathbf{-27}) \). Now we will pull back by the map \( \pi_1 : X_0(21) \to X_0(3) \). Using the explicit formula for this map, we find that there are four points of \( X_0(21) \) lying above \( H_3^{-1}(\mathbf{-27}) \). Given by their \( x \) and \( y \) coordinates, these points are:
\[
\left( \frac{-1+3\sqrt{-3}}{2}, \frac{-13+3\sqrt{-3}}{2} \right), \left( \frac{-1-3\sqrt{-3}}{2}, \frac{-13-3\sqrt{-3}}{2} \right), \\
\left( \frac{35+7\sqrt{21}}{2}, -62 - 14\sqrt{21} \right), \text{ and } \left( \frac{35-7\sqrt{21}}{2}, -62 + 14\sqrt{21} \right). 
\]

The ramification indices of these points are 1, 1, 3, and 3 respectively. So if we call these points \( P_1 \) through \( P_4 \), the divisor of \( E_{1,3,\epsilon}^6 \) (pulled back by \( \pi_1 \) to a form on \( X_0(21) \)) is \( 2P_1 + 2P_2 + 6P_3 + 6P_4 \).

On \( X_0(7) \) we have a very convenient weight 6 form given by the eta product \((\text{eta}1)^6(\text{eta}7)^6\) which has divisor \(2(0) + 2(\infty)\). Again, \( E_{1,7,\tau}^6 \) has trivial character so it is also a weight 6 form on \( X_0(7) \). Taking \( g \) to be the quotient \( E_{1,7,\tau}^6/(\text{eta}1)^6(\text{eta}7)^6 \) and comparing \( q \)-expansions we obtain the equation:

\[
g \cdot H_7^2 = \left( H_7 - \left( \frac{-13+3\sqrt{-3}}{2} \right) \right)^4
\]

Therefore the divisor of \( g \) must be \( 4H_7^{-1} \left( \frac{-13+3\sqrt{-3}}{2} \right) - 2(\infty) - 2(0) \). But this means that on \( X_0(7) \) the divisor of \( E_{1,7,\tau}^6 \) must be \( 4H_7^{-1} \left( \frac{-13+3\sqrt{-3}}{2} \right) \).

Now we will pull back by the map \( \pi_1 : X_0(21) \rightarrow X_0(7) \). Using the explicit formula for this map, we find that there are two points of \( X_0(21) \) lying above \( H_7^{-1} \left( \frac{-13+3\sqrt{-3}}{2} \right) \). Given by their \( x \) and \( y \) coordinates, these points are \( \left( \frac{-1-3\sqrt{-3}}{2}, \frac{-13-3\sqrt{-3}}{2} \right) \) and \( \left( \frac{-1+3\sqrt{-3}}{2}, 7 - 3\sqrt{3} \right) \). The ramification indices of these points are 1 and 3 respectively. So if we call these points \( Q_1 \) and \( Q_2 \), the divisor of \( E_{1,7,\tau}^6 \) (pulled back by \( \pi_1 \) to a form on \( X_0(21) \)) is \( 4Q_1 + 12Q_2 \).

So the divisor of \( v^6 = E_{1,3,\epsilon}^6/E_{1,7,\tau}^6 \) is equal to \( 2P_1 - 2P_2 + 6P_3 + 6P_4 - 12Q_2 \) (since \( Q_1 \) and \( P_2 \) were the same). So at this point we could take \( v \) as a third parameter for \( X_1(21) \) (in addition to \( x \) and \( y \)). We would want to find an equation relating the three parameters, and what one finds after comparing \( q \)-expansions is that they satisfy the equation:

\[
v^6 = \frac{(y + 4x - 8)^6(y - x + 6)^6x^5(x^2 - y)^3}{(y - \frac{3+3\sqrt{-3}}{2}x - 1)^4(x + \frac{1+3\sqrt{-3}}{2}y - 1)^6(y - 1)^6(x - 1)^6}
\]

However, we can clearly multiply \( v \) by any function on \( X_0(21) \) and get a new function which generates the same extension. So we will take as our third parameter the function \( u \) which satisfies the equation:

\[
u^6 = \frac{(x^2 - y)^3(y - \frac{3+3\sqrt{-3}}{2}x - 1)^2}{(x + \frac{1+3\sqrt{-3}}{2}y)^2x}
\]

Then the divisor of \( u^6 \) as a function on \( X_0(21) \) is given by:

\[
(u^6) = 2 \left( \frac{-1+3\sqrt{-3}}{2}, \frac{-13+3\sqrt{-3}}{2} \right) - 2 \left( \frac{-1-3\sqrt{-3}}{2}, \frac{-13-3\sqrt{-3}}{2} \right) + 12 ((1, 1) - (∞))
\]

This formula is very interesting for a variety of reasons. First of all, \( (1, 1) \) is the cusp \( (\frac{1}{4}) \) so it is of course a torsion point. Secondly, we see that any point
lying over one of the noncuspidal points must have ramification index 3 or 6. $X_{1}(21)$ has genus 5 and $X_{0}(21)$ has genus 1. So by the Hurwitz genus formula, it is easy to show that both noncuspidal points split into two points with index 3, and that there is no other ramification.

9.6 Holomorphic Differentials on $X_{1}(21)$

Now that we have a good model for $X_{1}(21)$ we will follow the same approach as in the previous example. First we will attempt to find a basis for the holomorphic differentials on $X_{1}(21)$ and then determine which differentials correspond to the weight 2 newforms $F$ and $F'$. Then will find suitable uniformizing parameters for the supersingular annuli and carry out the calculation using Coleman’s formula.

Again we have a one dimensional vector space of holomorphic differentials on $X_{0}(21)$ which can be pulled back by $\pi_{1}$, the forgetful map. Using our Weierstrass equation for $X_{0}(21)$ it is easy to see that a basis for this space is the differential $\frac{dx}{2y-3x-2}$. So we immediately take $\omega_{0}$ to be its pull-back by $\pi_{1}$. Now, the genus of $X_{1}(21)$ is 5 so we have to find 4 more linearly independent holomorphic differentials. Again we will try to reduce the problem to looking for functions on $X_{0}(21)$, and we begin by calculating the divisors of $\omega_{0}$ and $u$.

Looking at the divisor of $u$ as a function on $X_{0}(21)$ we see immediately that any point lying over $A = (\frac{-1+3\sqrt{-3}}{2}, \frac{-13+3\sqrt{-3}}{2})$ or $B = (\frac{-1-3\sqrt{-3}}{2}, \frac{-13-3\sqrt{-3}}{2})$ must have ramification index 3 or 6. Using the Hurwitz genus formula then it is easy to show that both $A$ and $B$ split into two points with ramification index 3, and the extension is unramified elsewhere. So let $A_{1}, A_{2}, B_{1}$ and $B_{2}$ be those points. Then the divisor of $u$ must be:

$$ (u) = (A_{1}) + (A_{2}) - (B_{1}) - (B_{2}) + 2\pi_{1}^{*}((1, 1) - (\infty)) $$

Furthermore, knowing the ramification tells us the divisor of $\omega_{0}$:

$$ (\omega_{0}) = 2(A_{1}) + 2(A_{2}) + 2(B_{1}) + 2(B_{2}) $$

Now we notice the following convenient fact:

$$ (u\omega_{0}) > \pi_{1}^{*}((A) + 2(1, 1) - 2(\infty)) $$

So if we can find a function $g_{1}$ on $X_{1}(21)$ with divisor at least $2(\infty) - 2(1, 1) - (A)$, and Riemann-Roch tells us there is one, we can get a new holomorphic differential by taking:

$$ \omega_{1} = \pi_{1}^{*}(g_{1}) \cdot u \cdot \omega_{0} $$

With a little arithmetic one comes up with the desired function:

$$ g_{1} = \frac{(\frac{-3+\sqrt{-3}}{6})(x - (\frac{5-\sqrt{-3}}{2}))}{y - (\frac{1+\sqrt{-3}}{6})x^{2} - (\frac{3+\sqrt{-3}}{3})x + (\frac{3+\sqrt{-3}}{6})} $$
Using the same reasoning one finds the other 3 holomorphic differentials as follows:

\[ \omega_2 = \pi_1^*(g_2) \cdot u^2 \cdot \omega_0, \quad \omega_3 = \pi_1^*(g_3) \cdot \frac{1}{u} \cdot \omega_0, \quad \omega_4 = \pi_1^*(g_4) \cdot \frac{1}{u^2} \cdot \omega_0 \]

with functions \( g_i \) given by:

\[
\begin{align*}
g_2 &= \frac{1}{x^2 - y} \\
g_3 &= \frac{y + (\frac{1+\sqrt{-3}}{2})x^2 - (3 + \sqrt{-3})x + (\frac{3+\sqrt{-3}}{2})}{(\frac{1+\sqrt{-3}}{2})(x + (\frac{1+3\sqrt{-3}}{2}))} \\
g_4 &= x^2 - y
\end{align*}
\]

Now we have a basis for the holomorphic differentials, but these differentials don’t necessarily correspond to newforms. So the next thing we must do is to get the \( q \)-expansions for these forms and diagonalize using one or more of the Hecke operators to obtain a basis of newforms. The \( q \)-expansions of the \( \omega_i \) are as follows:

\[
\begin{align*}
\omega_0(q) &= q - q^2 + q^3 - q^4 - 2q^5 - q^6 - q^7 + 3q^8 + \cdots \\
\omega_1(q) &= q + (\frac{-3 + \sqrt{-3}}{2})q^3 + (-1 - \sqrt{-3})q^4 + (\frac{1 + 3\sqrt{-3}}{2})q^7 + \cdots \\
\omega_2(q) &= q + (-1 - \sqrt{-3})q^2 + (\frac{-1 + \sqrt{-3}}{2})q^3 + (-1 + \sqrt{-3})q^4 + (1 + \sqrt{-3})q^5 + \cdots \\
\omega_3(q) &= q + (\frac{-3 - \sqrt{-3}}{2})q^3 + (-1 + \sqrt{-3})q^4 + (\frac{1 - 3\sqrt{-3}}{2})q^7 + \cdots \\
\omega_4(q) &= q + (-1 + \sqrt{-3})q^2 + (\frac{-1 - \sqrt{-3}}{2})q^3 + (-1 - \sqrt{-3})q^4 + (1 - \sqrt{-3})q^5 + \cdots 
\end{align*}
\]

By looking at the operator \( U_3 \) we see that these forms are eigenvectors with different eigenvalues. Therefore we do not have to look at any other operators. We know that the \( \omega_i \)'s are the desired newforms. Furthermore, if we choose \( \sqrt{-3} \) to be congruent to \( -2 \) (mod 7) we find that \( \omega_1 \) reduces to \( f \) and \( \omega_3 \) reduces to \( df = f' \). If we choose \( \sqrt{-3} \) to be congruent to \( 2 \) (mod 7) the reverse happens.

### 9.7 Supersingular Annuli on \( X_1(21) \)

Now that we know which differentials we are working with, the next thing we need is a parameterization of the supersingular region of \( X_1(21) \). We know that the supersingular region will consist of two annuli since there are two supersingular points (mod 7). So what we are really looking for is a uniformizing parameter for each of these supersingular annuli. Again, we will make heavy use of our models for \( X_0(N) \) and the maps between them.
On $X(1)$ the supersingular region is given by $v(j) > 0$, so it is a disc. First we step up to $X_0(7)$ using the map:

$$j = H_7 + 17 \cdot 11 \cdot 2^2 + \frac{7^4 \cdot 41 \cdot 2}{H_7} + \frac{7^6 \cdot 11 \cdot 2^4}{H_7^2} + \frac{7^7 \cdot 13^2 \cdot 5}{H_7^3} + \frac{7^9 \cdot 17 \cdot 2^4}{H_7^4} + \frac{7^{11} \cdot 23 \cdot 2}{H_7^5} + \frac{7^{13} \cdot 2^2}{H_7^6} + \frac{7^{14}}{H_7^7}$$  (9.10)

By simply comparing valuations term by term, we see that the inverse image of the disc on $X(1)$ is the annulus, $0 < v(H_7) < 2$.

Now we step up to $X_0(21)$ using the map:

$$H_7 = \frac{xy - 7x^2 + 7y + 6x - 7}{x^2 - y}$$  (9.11)

and the equation for the curve, $y^2 = x^3 + 3xy - 8x^2 + 2y + 4x - 1$. By comparing valuations we find that the points lying above the supersingular region of $X_0(7)$ are exactly those with $0 < v(x) < 1$. Again, to understand this region we must view the equation for the curve as a quadratic equation in $y$. As such, it has the following discriminant:

$$d = x^2(-23 + 4(x + \frac{7}{x}))$$

This has two distinct analytic square roots on the annulus $0 < v(x) < 1$ corresponding to the two distinct choices for $\sqrt{-23}$. So the supersingular region on $X_0(21)$ is actually the union of 2 width-1 annuli, given philosophically by the formula:

$$A_\pm : t \rightarrow (t, \frac{3t + 2}{2} \pm \frac{t}{2}\sqrt{-23 + 4(t + \frac{7}{t})})$$

and more precisely by the formula:

$$A_\pm : t \rightarrow (t, 26t + 1 \pm 25t \cdot \sqrt{-23(42t^{-1} + 43 + 48t + 17t^2 + \cdots)})$$

Here the coefficients of the series expansion for $y$ are really in $\mathbb{Z}_7$ but are given (mod 49) and will be given (mod 49) for the rest of this example. This precision will turn out to be sufficient for our purposes.

Now, when we step up to $X_1(21)$ we are adjoining a sixth root of some function on $X_0(21)$ according to Equation 9.9. In terms of the parameter $t$ this is the same as adjoining a sixth root of the analytic function given by the series expansion:

$$u^6 = (14 \pm 35\sqrt{-23})t^{-2} + (23 \pm 38\sqrt{-23})t^{-1} + (6 \pm 31\sqrt{-23}) + (47 \pm 26\sqrt{-23})t + \cdots$$

This is equivalent to adjoining a sixth root of $t$. Therefore the two supersingular annuli are totally ramified in the extension from $X_0(21)$ to $X_1(21)$ and we can
choose as a new parameter any sixth root of $t$, which we will call $s$. To be more specific, the two annuli $A_{\pm}$ are now of width $1/6$ and given by the formulae:

$$
x = s^6
$$

$$
y = 26s^6 + 1 \pm 25s^6 \cdot \sqrt{-23}(42s-6 + 43 + 48s^6 + 17s^{12} + \cdots)
$$

$$
u = (\pm 35\sqrt{-23})s^{-7} + (6 \pm 36\sqrt{-23})s^{-1} + (34 \pm 21\sqrt{-23})s^5 + \cdots
$$

9.8 Computing $(F, F|w_{\zeta_p})_{\infty}$ on $X_1(21)$

In terms of the parameters, $x$, $y$, and $u$, the two holomorphic differentials $F$ and $F'$ are given by the formulae:

$$
F = \frac{y + \left(\frac{1+\sqrt{-23}}{2}\right)x^2 - (3 + \sqrt{-3})x + \left(\frac{3+\sqrt{-3}}{2}\right)}{(x + \left(\frac{1+\sqrt{-23}}{2}\right))} \cdot \frac{1}{u} \cdot \frac{-dx}{2y - 3x - 2}
$$

$$
F' = \frac{-\left(\frac{3+\sqrt{-23}}{6}\right)(x - \left(\frac{5+\sqrt{-23}}{2}\right))}{y - \left(\frac{3+\sqrt{-23}}{6}\right)x^2 - \left(\frac{3+\sqrt{-23}}{3}\right)x + \left(\frac{3+\sqrt{-23}}{6}\right)} \cdot \frac{-dx}{2y - 3x - 2}
$$

So after a little arithmetic we find that their expansions in terms of the parameter $s$ are given by:

$$
F = (14 \pm 28\sqrt{-23})s^{-5} + (17 \pm 10\sqrt{-23})s + (10 \pm 46\sqrt{-23})s^7 + \cdots \frac{ds}{s}
$$

$$
F' = (28 \pm 35\sqrt{-23})s^{-7} + (10 \pm 5\sqrt{-23})s^{-1} + (46 \pm 15\sqrt{-23})s^5 + \cdots \frac{ds}{s}
$$

As expected the two forms have zero residues, so we are able to apply the formula for $(F, F')_{\infty}$. Over each annulus we must sum up $a_i b_{-i}$ where the $a$'s and $b$'s are the coefficients of $F$ and $F'$ after factoring out $\frac{ds}{s}$. Then we add the results from the two annuli. On $A_{+}$ we get:

$$
\sum a_i b_{-i} = (14 + 28\sqrt{-23})(46 + 15\sqrt{-23}) + (17 + 10\sqrt{-23})(10 + 5\sqrt{-23}) + (10 + 46\sqrt{-23})(28 + 35\sqrt{-23})
$$

$$
= (28\sqrt{-23}) + (38\sqrt{-23}) + (21\sqrt{-23})
$$

$$
= 38\sqrt{-23}
$$

On $A_{-}$ we get:

$$
\sum a_i b_{-i} = (14 - 28\sqrt{-23})(46 - 15\sqrt{-23}) + (17 - 10\sqrt{-23})(10 - 5\sqrt{-23}) + (10 - 46\sqrt{-23})(28 - 35\sqrt{-23})
$$

$$
= (-28\sqrt{-23}) + (-38\sqrt{-23}) + (-21\sqrt{-23})
$$

$$
= -38\sqrt{-23}
$$
When we add the two results we see that \((F, F')\) is trivial (mod 49). Since \(F|_{W_{\zeta_p}}\) is equal to \(c_\zeta F'\) for some integral constant \(c_\zeta\), we have also shown that \((F, F|_{W_{\zeta_p}})\) is divisible not only by \(\pi^p\) but in fact by \(\pi^{p+1}\). Therefore we can conclude by the main theorem that the representation \(\rho_{f,p}\) is indeed split.
Bibliography


