Coherent System of Models for a Family of Modular Curves

Tim Kneezel

Abstract

Modular curves of the form $X_0(N)$ are intrinsically interesting curves to investigate. They contain a wealth of information and cross over the boundaries of geometric, algebraic, and analytic mathematics. We set out to compute all of the information for a specific family of related modular curves, namely $X_0(N)$ for those integers N dividing 36. In this paper, we work out the parameters for the curves, the coordinates of the important points in relation to those parameters, and then we find equations for the important maps between the curves. Also, since $X_0(36)$ has genus one, and therefore has a natural group structure, we include a brief section on the subgroup generated by its cusps.

1 Introduction

In order to begin to understand the properties of a modular curve like $X_0(N)$, it is imperative to have a good working model for the curve. In this context, this means having a specific set of equations for describing the curve. So we will be selecting specific functions on each of the curves and then using the properties of the curves to find equations relating the functions. This of course begs the question "If there are many choices for such a model, what criteria make a given model 'good'?"

One of the main desired qualities is that the selected functions are completely supported on a specific kind of special points of the modular curve, called the cusps. This means that we choose our parameters to be functions which have zeros and poles only at the cusps. This was possible to do in every case observed in this study. Another important feature of the model is to be able to explicitly state formulae for the different naturally arising maps between the curves. These formulae are exceedingly helpful in beginning to understand the relationships between the different curves.

However, before we delve into these concepts, we should define these terms for the sake of completeness.

2 Overview of the Basics

The *upper half plane of* **C**, most often denoted as $H = \{x + iy : x \in (-\infty, \infty), y \in (0, \infty)\}$, is the most fundamental starting point for work with modular functions. The modular group $SL_2(\mathbf{Z})$, which is a group under matrix multiplication, acts on *H* in a very specific manner which makes it possible to define modular functions *f* on H.

$SL_2(\mathbf{Z})$ is defined by:

$$\text{all } \gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \text{ with } ad - bc = 1 \text{ and } a, b, c, d \in \mathbf{Z} \tag{2.1}$$

and $\Gamma = SL_2(\mathbf{Z})$ acts on *H* by:

$$\text{for } z \in H, \begin{bmatrix} a & b \\ c & d \end{bmatrix}(z) = \frac{az + b}{cz + d} \tag{2.2}$$

Note that for $\gamma(\infty)$ we take this to be defined as the limit as z goes to infinity of $\gamma(z)$.

That is, $\gamma(\infty) = \lim_{z \to \infty} \gamma(z) = \lim_{z \to \infty} \frac{az + b}{cz + d} = \frac{a}{c}$ and $\gamma(\infty) = \infty$ if c = 0.

For any two elements $x \in H$ and $y \in H$, we say that *x is equivalent to y modulo* Γ, denoted $x \sim y$ modulo Γ, if there exists some $\gamma \in \Gamma$ such that $\gamma(x) = y$. This is easily seen to be an equivalence relation and the proof is left to the reader. This is the Γ-equivalence class of z, denoted Γz.

Example 2.1

Let $\gamma = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}$. Clearly, $\gamma \in \Gamma$ as 2*1-1*1=1. Also $\gamma(i) = \frac{1 + 2i}{1 + i} = \frac{3 + i}{2}$. Therefore, we see that $i \sim \frac{3 + i}{2}$ modulo $SL_2(\mathbf{Z})$.

A modular function *f* is then a function on *H* which respects this group action seen in equation 2.2. This means that

$$\forall \gamma \in \Gamma \text{ and } \forall z \in H, \ f(\gamma(z)) = f(z) \tag{2.3}$$

If we then take *H* and mod out by the group action Γ, then we get the quotient space denoted as H/Γ. Formally, H/Γ is the set of Γ-equivalence classes $\{\Gamma z : z \in H\}$. A fundamental domain of H/Γ, call it F, is particularly useful for visualizing what the quotient looks like.

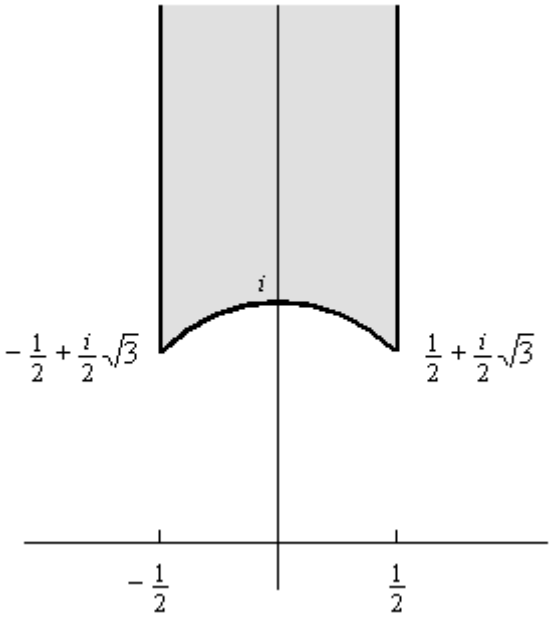
From [K] we can see that if G is any subgroup of Γ, then F_G is called a *fundamental domain* of G if it satisfies the following two criterion:

1. If any two points are equivalent under G, then they must be the same point in F_G or they both lie on the boundary of F_G.
2. If z_1 is any point in *H*, then there exists some point z_2 in F_G such that $z_1 \sim z_2$.

One such fundamental domain for the action of $SL_2(\mathbf{Z})$ is shown in Chapter 3 of [K] to be

$$F = \{z \in H : -\tfrac{1}{2} \le \mathrm{Re}\, z \le \tfrac{1}{2}, |z| \ge 1\} \tag{2.4}$$

which looks like



Since we have to allow for there to be two distinct points, both on the boundary of F_G, to be equivalent, it is reasonable to view the two boundaries as being pulled towards each other and being glued together. This is not just an intuitive process, but results from the fact that under the group action of $SL_2(\mathbf{Z})$

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}(z) = z + 1 \tag{2.5}$$

Similarly, the lower boundary is glued to itself via the operation

$$\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}(z) = \frac{-1}{z} \tag{2.6}$$

All of this results in something resembling the surface of a sphere with a little hole poked in the top of it. It is helpful to visualize the lines 2x+1=0 and 2x-1=0, from the picture above of F, wrapping around the y-axis and sticking together. The semicircular boundary at the bottom is then glued to itself. The resulting space is of *H* modulo Γ is defined to be X(1). Thus,

$$X(1) = H \big/ \Gamma \tag{2.7}$$

Similarly, we can also look at $\Gamma_0(N)$, where

$$\Gamma_0(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma : c \equiv 0 \bmod(N) \right\} \tag{2.8}$$

It is straightforward to verify that $\Gamma_0(N)$ is a subgroup of Γ. Note that since $\Gamma_0(N)$ is a subgroup of Γ, elements that used to be equivalent by Γ may no longer be equivalent by $\Gamma_0(N)$. Analogously, we define $X_0(N)$ to be the quotient space resulting from *H* modulo the group action from $\Gamma_0(N)$. That is

$$X_0(N) = H \big/ \Gamma_0(N) \tag{2.9}$$

The *genus* of the curve $X_0(N)$ can best be described using topological ideas. $X_0(N)$ can be viewed as a surface over *H* resembling the surface of a sphere, in which case, the genus of $X_0(N)$ is the number of holes that go all the way through the sphere. A genus zero curve would resemble the surface of a sphere, while a genus one curve would resemble the surface of a torus. Note that even though $X_0(N)$ clearly looks like a surface it is customary to refer to it as a complex curve. This is because it really is a two dimensional surface over **R**, but it is only a one dimensional curve over **C** and we are working over *H* which is a subset of **C** by definition.

The *cusps* of $X_0(N)$ are points that are added to $X_0(N)$ in order to fill in the holes that are in it. Note the holes referred to here are not the same as the holes in the above description of genus. They are more like little punctures in the surface of sphere than they are like the hole in a torus. Recall that in constructing the quotient X(1) from *H*, it was necessary to fill in the one missing puncture hole in order for X(1) to look like the surface of a sphere. This hole can be seen as coming from the fact that there was no upper boundary to the fundamental domain F. Then we throw in "the cusp at infinity" to fill in that hole and we have a smooth sphere. That works fine for X(1), but $X_0(N)$ has additional puncture holes that need to be filled in as well. For the extra cusps, we simply extend the action of Γ_0 to the rational numbers on the real axis of the complex plane. Note, under the full modular group Γ all the rational numbers were all equivalent to infinity as can be seen in the following example. Since they were all a part of one equivalence class for an element of Γ, we have only added new elements (i.e. the necessary cusps) to $H \big/ \Gamma_0$, but nothing new was added to $H \big/ \Gamma$.

Example 2.2

For any rational number $\frac{p}{q}$ in lowest terms, with $q \neq 0$, then we know from the Chinese Remainder Theorem that there exist two integers, call them r and s, such that rp + sq = 1. Therefore we see that $\gamma = \begin{bmatrix} p & -s \\ q & r \end{bmatrix}$ is in $SL_2(\mathbf{Z})$ and that $\gamma(\infty) = \frac{p}{q}$. This directly implies that $\infty \sim \frac{p}{q}$ modulo $SL_2(\mathbf{Z})$ and also that $\infty \sim \frac{p}{q}$ modulo $\Gamma_0(q)$ as γ is also clearly in $\Gamma_0(q)$.

Example 2.3

For a more concrete example, we look at $\gamma = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$. It is clear that $\gamma \in \Gamma$ and that $\gamma(\infty) = 0$, so $\infty \sim 0$ modulo Γ. However, it is straightforward to show (and the reader is invited to do so) that for N>1, there is no $\gamma \in \Gamma_0(N)$ with the property that $\gamma(\infty) = 0$.

The number of cusps necessary to fill in all the holes on any given curve $X_0(N)$ is given by (see [Sh])

$$\text{number of cusps on } X_0(N) = \sum_{d|N} \varphi\left(d, \tfrac{N}{d}\right) \tag{2.10}$$

There is a special class of cusps called *Galois conjugate cusps* of $X_0(N)$. These are points which are not equivalent modulo $\Gamma_0(N)$, but which have exactly the same ramification indices over each of the lower curves and which cannot be distinguished over **Q**. They are similar to complex conjugates which always appear as a pair of roots in polynomials over **R** that cannot even be distinguished over **R**, but which can be distinguished over **C**.

When we begin to relate one curve with another, we find some interesting results. It is straightforward to verify that, for N dividing M, $\Gamma_0(M)$ is a subgroup of $\Gamma_0(N)$. Therefore, there is an obvious function, formally given by $\Gamma_0(M)z \to \Gamma_0(N)z$, of the quotients given by $\pi_1(z) = z$. This map is often called the forgetful map. For d dividing $\frac{M}{N}$, it can be verified that $\pi_d(z) = dz$, is also a well defined function.

Example 2.4

If d divides $\frac{M}{N}$, $\gamma = \begin{bmatrix} e & f \\ g & h \end{bmatrix}$, $\gamma \in \Gamma_0(M)$ and $\gamma(z_1) = \frac{ez_1 + f}{gz_1 + h} = z_2$, then $\sigma = \begin{bmatrix} e & df \\ \frac{g}{d} & h \end{bmatrix}$ is an element of $\Gamma_0(N)$ since g must divide M for $\gamma \in \Gamma_0(M)$ and d divides $\frac{M}{N}$ implies that d divides g and that $\frac{g}{d}$ divides N. Then we note that $\sigma(dz_1) = \frac{edz_1 + df}{gz_1 + h} = dz_2$.

Thus, if we are looking at two curves, $X_0(N)$ and $X_0(M)$, then we can talk about $X_0(M)$ lying over $X_0(N)$ by any of these maps (since if we mod *H* out by a smaller group action, we get a bigger curve). Every point, except for a finite number of points, in $X_0(N)$ has exactly n number of points lying over it in $X_0(M)$ for a fixed n called the *degree* of the map. We can find n by a number of different methods but, as given by [Sh], it suffices to know that

$$n = [\Gamma_0(M):\Gamma_0(N)] = \text{the index of } \Gamma_0(M) \text{ over } \Gamma_0(N) \tag{2.11}$$

However, at each of those finite number of points which have less than n points lying above it in $X_0(M)$, we then know that some of those points must have an extra multiplicity in order for the number to add up to n. This is called *ramification*. This is an intuitive definition of ramification which suits our purposes here. For a formal definition, see [Sil].

This is similar to what happens to prime numbers in the integers of a number field F after adjoining some element *r* to the field. Sometimes the prime number remains prime in F[*r*] so there is no ramification. Sometimes the prime number becomes r^n for some integer n in F[*r*]. Sometimes the prime number is a multiple of two new elements in F[*r*]. See Example 2.4.

Example 2.5

We will look at the extension $\mathbf{Z}[\sqrt{3}]$. The number 3, which is prime in **Z**, now ramifies since in $\mathbf{Z}[\sqrt{3}]$, $3 = (\sqrt{3})^2$ and $\sqrt{3}$ is prime in $\mathbf{Z}[\sqrt{3}]$. The number 2, which is also prime in **Z**, now splits since in $\mathbf{Z}[\sqrt{3}]$, $2 = (\sqrt{3}+1)(\sqrt{3}-1)$. Note that this is not exactly the same situation as is happening in $X_0(N)$. This is because it is possible to adjoin elements to **Z** which do not affect some prime. For example, in $\mathbf{Z}[\sqrt{5}]$, 3 is still a prime so there is no ramification or splitting. However, it is a strong enough analogy to begin to understand what is going on.

It is known that ramification in the previously defined maps from $X_0(N)$ to $X_0(M)$ can occur only at the cusps and over the "elliptic points" of the curve. Since we were able to choose functions supported on the cusps (i.e. the function has zeros and poles at the cusps of the curve in question and nowhere else), the ramification over the elliptic points was not an issue in our calculations. We will therefore leave out the definition of elliptic points as superfluous information for us. The ramification at the cusps, however, was then crucial to establishing relations between functions. Refer to Section 8 for the ramification at the cusps in each of the $X_0(N)$ for N dividing 36.

A particularly nice property of any function *f*, not identically 0, on a projective (i.e. no puncture holes) algebraic curve C, is that the number of zeros of *f* is equal to the number of poles of *f* [Sil]. Thus, if we count each zero of *f* as +1 and each pole of *f* as –1, then the sum over all the zeros and poles of *f*, including any relevant multiplicities, equals zero. The *divisor* of *f* is a representation of all of the points where *f* has either a zero or a pole. We denote the multiplicity of the zeros or poles as a coefficient equal to the number of poles and zeros at a point next to the point in parentheses, i.e.

$$\text{divisor of } f = (f) = (+\{\text{zeros}\}-\{\text{poles}\}) \qquad (2.12)$$

Example 2.5

If $f = \dfrac{x^3(x+2)}{(x+3)^2}$ and $C = \mathbf{A}^1(\mathbf{R}) = \mathbf{R} \cup \{\infty\}$, then the divisor of *f* is given by:

$(f) = 3(0) - 3(\infty) + 1(-2) - 1(-2) - 2(-3) + 2(\infty) = 3(0) + (-2) - 2(-3) - (\infty)$

and note that 3 + 1 – 2 – 1 = 0

3 Choosing Parameters on $X_0(N)$

We can now begin to discuss how to pick out functions on $X_0(N)$ that will give us a good model with which to calculate.

The *parameters* for any given $X_0(N)$ are functions which generate the function field. On any genus zero curve, only one parameter, denoted h_N, is required and it is always possible to choose it to have divisor (P) – (Q), for any P and Q. In keeping with our decisions on what makes a model good, we choose the parameter in genus zero cases to have divisor (0) – (∞). Any other function with a single pole at infinity is just the picked parameter plus a constant. On any genus one curve, two parameters denoted x_N and y_N, are required but there is a special equation, called the Weierstrass equation, closely linking the two parameters.

There is a function called the discriminant function, Δ, which is a weight 12 function (see [K]) and is useful for creating functions on *H* with specific divisors. However, it has some problems to worry about which are briefly discussed below. It is defined to be

$$\Delta(z) = e^{2\pi i z}\prod_{n=1}^{\infty}\left(1-e^{2\pi i n z}\right)^{24} \tag{3.1}$$

If we let $q = e^{2\pi i z}$, then we can discuss the *q-expansion for* Δ which is a power series expansion for the function near the cusp infinity. The q-expansion for Δ is given by

$$\text{and}\quad \Delta_k = \Delta(q^k) = q^k\prod_{n=1}^{\infty}\left(1-q^{kn}\right)^{24} \tag{3.2}$$

Δ_k and any quotient of Δ_k's are always functions as long as the weights cancel out and each k divides the N in $X_0(N)$. That is, if the product of the function weights in the numerator of the quotient is n, then the product of the weights in the denominator of the quotient must also be n. However, having the 24^{th} power in the definition makes the coefficients get very large very fast and thus difficult to deal with. Also, quite often Δ is a power of some other function, so we would then be using an unnecessarily large function.

An exceptionally powerful solution to the problems of Δ is the 24^{th} root of Δ, called the *Dedekind eta-function*, which is given by

$$\eta(z) = e^{2\pi i z/24}\prod_{n=1}^{\infty}\left(1-e^{2\pi i n z}\right) \tag{3.3}$$

$$\eta_k = \eta(q^k) = q^{k/12}\prod_{n=1}^{\infty}\left(1-q^{kn}\right) \tag{3.4}$$

The eta-functions are much nicer because of their smaller coefficients.

If we are looking at $X_0(N)$, there exists a Dedekind eta-function η_k for each k dividing N. One of the reasons that the Dedekind eta-function is so helpful is that it is possible, not to mention fairly easy, to find a product of appropriate eta-functions such that the eta-product has the desired divisor. This will be shown explicitly in Section 4 of this paper.

However, before we get too excited with the advantages of our eta-function, we must look at its most serious flaw. Because of the leading $q^{1/12}$ term in the definition of the eta-function, we have to make sure that we manage to kill off that term one way or another in the eta-product. Otherwise our eta-product or eta-quotient is not even a function on $X_0(N)$. Fortunately, [L] gives us a set of criteria which, if satisfied, guarantee that our eta-product will be a function on $X_0(N)$.

Theorem 3.1 – Ligozat's Theorem

The Dedekind eta-product, $\prod_{d|N}(\eta_d)^{r_d}$, is a function on $X_0(N)$ if:

1. $\sum_{d|N} r_d \frac{N}{d} \equiv 0 \bmod 24$
2. $\sum_{d|N} r_d d \equiv 0 \bmod 24$
3. $\sum_{d|N} r_d = 0$
4. $\prod_{d|N}\left(\frac{N}{d}\right)^{r_d} \in \mathbf{Q}^2$

So as long as we make sure to check Ligozat's criteria then our selected eta-product is guaranteed to be a function on $X_0(N)$.

Being able to map between the curves explicitly is done through the use of different π_d maps. Recall from section 2, that if we assume we are looking at $X_0(N)$ and $X_0(M)$ where N divides M, then there is a π_d for each d dividing (M/N). It is defined such that $\pi_d : X_0(M) \to X_0(N)$ and for z in $X_0(M)$,

$$\pi_d(z) = dz \tag{3.5}$$

This also clearly implies that for the eta-products

$$\pi_d(q) = q^d \tag{3.6}$$

In general for $f : C_1 \to C_2$, where C_1 and C_2 are curves (not necessarily modular curves), we use the notation f^* to indicate either the induced map on divisor groups or function fields (see [Sil]). It is often called the pullback of f. Specifically, ${\pi_d}^*$ is either of these maps induced by π_d. If we are thinking of ${\pi_d}^*$ as the induced map on divisor groups, then induced map on divisor groups ${\pi_d}^*(z)$ is simply the inverse image of z under π_d.

One final pair of relations are known as the Atkin-Lehner involution, or w_d, and its pullback called w_d^*. Since it is an involution, $w_d^2(x) = x$ for any x in $X_0(M)$.

Theorem 3.2 – Atkin-Lehner Theorem

$\forall d \mid N, \left(d, \frac{N}{d}\right) = 1, d \neq 1$

$\exists w_d : X_0(N) \to X_0(N)$

such that $\pi_d : X_0(N) \to X_0(\frac{N}{d})$ satisfies $\pi_d = \pi_1 \circ w_d$

In order to figure out the equations for π_d and w_d in terms of our selected parameter h_N of $X_0(N)$, we are going to need to know the ramification indices for each of the cusps up to our larger curve $X_0(M)$. In these instances, it is handy to have a handful of *ramification diagrams* already churned out. These diagrams are a great visual aid for seeing how points ramify between curves. See Section 7 of this paper for a list of all of the cusp ramification diagrams for $X_0(N)$ where N divides 36. Note that if N divides M and M divides P, then it is perfectly straightforward to compose the diagrams, multiplying the respective indices to get the total ramification between $X_0(N)$ and $X_0(P)$. It is similar to the composition of algebraic field extensions and the multiplying of the degrees to get the total extension degree.

In order to find out which cusps of $X_0(M)$ lie over which cusps of $X_0(N)$ for each of the π_d, there are a few tricks we can try.

First note that the sum of the ramification indices on each little ramification diagram (see section 7) equals the index of Γ_0(top) over Γ_0(bottom). This alone can sometimes give the answer. Also from the definition of π_d, it is possible to tell which cusps lie over which of the others. If we have a setup like N divides M and M divides P and we know what the ramification indices are between $X_0(N)$ and $X_0(M)$, and between $X_0(N)$ and $X_0(P)$, then we can try to guess our way through such that the composition gives the correct values between $X_0(N)$ and $X_0(P)$.

If all else fails, then we resort to using the much more powerful, but slightly difficult to apply, moduli-theoretic approach to modular curves via Tate Curves. It tells us both what element of the upper space lies over what element of the lower space and its ramification index. However, it can be a bear to use and can often be avoided for genus zero curves. A good introduction to Tate Curves can be found in Section 14 of [Sil].

4 Genus Zero Example

We are going to go through a typical genus zero curve process and select a parameter, check that the parameter is a function by Ligozat, and then get the equation for one of the π_d's. We will work on $X_0(6)$.

If we go through the cusp ramification diagrams in Section 7, or if we skip directly to Section 8 and look at the table, we find that the cusps on $X_0(6)$ are : $0, \frac{1}{2}, \frac{1}{3}, \infty$.

The divisors of each of the Δ's are given by:

$$(\Delta_1) = 6(0) + 2(\tfrac{1}{2}) + 3(\tfrac{1}{3}) + (\infty)$$

$$(\Delta_2) = 3(0) + (\tfrac{1}{2}) + 6(\tfrac{1}{3}) + 2(\infty)$$

$$(\Delta_3) = 2(0) + 6(\tfrac{1}{2}) + (\tfrac{1}{3}) + 3(\infty)$$

$$(\Delta_6) = (0) + 3(\tfrac{1}{2}) + 2(\tfrac{1}{3}) + 6(\infty)$$

So using a little linear algebra, we set up and solve a system of equations for the powers of the eta-functions. The 4x4 matrix comes from the divisors of the Δ's. The r_i's are the respective powers for the η_i's. The entries in the column vector on the right must add up to zero since $X_0(6)$ is an algebraic curve and we have used multiples of 24 since the η's are 24^{th} roots of the Δ's. We have entered them such that they represent the function f having divisor $(f) = (0) - (\infty)$.

$$\begin{bmatrix} 6 & 3 & 2 & 1 \\ 2 & 1 & 3 & 3 \\ 3 & 6 & 1 & 2 \\ 1 & 2 & 3 & 6 \end{bmatrix} \begin{bmatrix} r_1 \\ r_2 \\ r_3 \\ r_6 \end{bmatrix} = \begin{bmatrix} 24 \\ 0 \\ 0 \\ -24 \end{bmatrix}$$

Solving this gives us our powers for the eta-product.

$$r_1 = 5,\ r_2 = -1,\ r_3 = 1,\ r_6 = -5$$

We can now find our parameter for $X_0(6)$, call it h_6.

Thus,
$$h_6 = \frac{(\eta_1)^5(\eta_3)}{(\eta_2)(\eta_6)^5} \qquad (4.1)$$

We now have to check and make sure that h_6 is a function on $X_0(6)$.

1. $5*6 + (-1)*3 + 1*2 + (-5)*1 = 24 \equiv 0 \bmod 24$
2. $5*1 + (-1)*2 + 1*3 + (-5)*6 = -24 \equiv 0 \bmod 24$
3. $5 - 1 + 1 - 5 = 0$
4. $\left(6^5\right)\left(\frac{1}{3}\right)(2)(1)^5 = 72^2$

So it checks out Ligozat.

Finally, we will find the equation for $\pi_1^*(h_2)$ where h_2 is the parameter on $X_0(2)$.

Using the cusp ramification diagrams of Section 7, we find that

$$(\pi_1^*(h_2)) = 3(0) + (\tfrac{1}{3}) - 3(\tfrac{1}{2}) - (\infty) \qquad (4.2)$$

We need to get all of the poles at ∞ since that implies we have a polynomial in h_6. This means that we first need to figure out the coordinate of $\frac{1}{2}$. This is quite simple to do for genus zero curves. We go back to the matrix above that we used to get h_6 and we now find an eta-product with divisor $(x) = (\frac{1}{2}) - (\infty)$. So we find that:

$$x = \frac{(\eta_2)^3(\eta_3)^9}{(\eta_1)^3(\eta_6)^9} \qquad (4.3)$$

Now, we use the definition of η_i to get the q-expansion of x and the q-expansion of h_6 and then we can compare the q-expansions. It is important to note that the q-expansion are based on ∞, so if all the poles are at ∞ and there are k poles there, then the q-expansion starts with the term q^{-k}. Also, since this is a genus zero curve, all functions with a single pole at infinity like h_6 must only differ from h_6 by a constant.

We find that $h_6(q) = q^{-1} - 5 + 10q - 16q^2 + 35q^3 - 66q^4 \ \ldots$
and that $x(q) = q^{-1} + 3 + 10q - 16q^2 + 35q^3 - 66q^4 \ \ldots$
By inspection we can see that $h_6+8 = x$, which is to say that $h_6(\frac{1}{2}) = x(\frac{1}{2}) - 8 = 0 - 8 = -8$

So the coordinate of $\frac{1}{2}$ is –8.

Now, back to the problem at hand.
We know that $(\pi_1^*(h_2)) = 3(0) + (\frac{1}{3}) - 3(\frac{1}{2}) - (\infty)$

and we just found that $(h_6+8) = (\frac{1}{2}) - (\infty)$,

so then $((\pi_1^*(h_2))\,(h_6+8)^3) = 3(0) + (\frac{1}{3}) - 3(\frac{1}{2}) - (\infty) + 3(\frac{1}{2}) - 3(\infty) = 3(0) + (\frac{1}{3}) - 4(\infty)$.

Now, multiplying the q-expansions of $\pi_1^*(h_2)$ and $(h_6+8)^3$ we find that
$(\pi_1^*(h_2))\,(h_6+8)^3 = h_6^3(h_6+9)$

And so we get $\pi_1^*(h_2) = \dfrac{h_6^3(h_6+9)}{(h_6+8)^3}$

5 Special Case of Group Structure on Genus One Curve $X_0(36)$

A corollary of the Riemann-Roch theorem, as stated in [Sil], says that
If $\deg(D) > 2g - 2$, then $\ell(D) = \deg(D) + 1 - g$
where $\ell(D)$ is the number of linearly independent functions with poles at most on D.

For all genus one curves, this implies that if we pick any point such that D = (P), then deg(D) = 1 > 2*1-2 =0. Therefore, $\ell(D) = 1+1-1 = 1$

This implies that the one linearly independent function is just the family of constant functions. Thus there is no non-constant function with a single pole at P for any point P.

Now pick D = 2(P). Then $\ell(D) = 2+1-1 = 2$. This implies there exists an x with (x) = (Q)+(R)–2(P) where Q and R are points on the curve.

Now pick D = 3(P). Then $\ell(D) = 3+1-1 = 3$. This implies there exists a y with (y) = (A)+(B)+(C)–3(P) where A, B and C are points on the elliptic curve.

Now pick D = 6(P). Then $\ell(D) = 6+1-1 = 6$. However, we have 7 functions in the basis for this: 1, x, y, x^2, xy, x^3, y^2. Therefore x and y satisfy an elliptic equation of the form $y^2 = ax^3+bxy+cx^2+dy+ex+f$. This is known as the Weierstrass Equation and every genus one curve has this property. In particular, the Weierstrass Equation for the genus one curve studied here can be found in section 6 under $X_0(36)$.

It is always possible to define a group structure on these kinds of (genus one) curves with the following construction. Since the Weierstrass Equation is a cubic, any straight line crossing one of the points on the curve, must cross exactly three points on the curve. We must note, though, that we include the point at infinity as being on the curve and is the additive identity for the group. Also note that if the line is tangent to the curve then that will count as more than one crossing of the curve. Knowing all that, then addition on the curve works as follows:

If P and Q are points on the curve, and the straight line connecting them also crosses the curve in another spot then that point equals –(P+Q).

The above formulation of addition on the curve $X_0(N)$ is equivalent to saying that:

If P and Q are points on the curve, then P+Q=R if and only if there exists a function *f* on $X_0(N)$ such that the divisor of *f* has the property that

$$(f) = (R) + (\infty) - (P) - (Q) \qquad (5.1)$$

Example 5.1

On $X_0(36)$, the point 0 + the point $\frac{1}{2}$ = the point ∞ since we can look at the function given by our parameter *x* which has divisor $(x) = (0) + (\frac{1}{2}) - 2(\infty)$ as can be seen in section 6. Therefore, the function $\frac{1}{x}$ has divisor $(\frac{1}{x}) = (\infty) + (\infty) - (0) - (\frac{1}{2})$.

It is natural to ask how the special points from the modular curve view of $X_0(N)$, i.e. the cusps, relate to the group structure of the curve. There is a general theorem stating that the cusps have a finite order which implies that there is a finite subgroup containing all of the cusps. What is really surprising here though, was that the "good" cusps – the non-Galois conjugate cusps – formed a group of their own isomorphic to $\mathbf{Z}/6\mathbf{Z}$, and then that the complete set of cusps create a group isomorphic to $(\mathbf{Z}/6\mathbf{Z})\mathrm{x}(\mathbf{Z}/2\mathbf{Z})$.

Group Structure on cusps: isomorphic to $\left(\mathbf{Z}/6\mathbf{Z}\right)\mathrm{x}\left(\mathbf{Z}/2\mathbf{Z}\right)$

+	∞	0	$\frac{1}{18}$	$\frac{1}{4}$	$\frac{1}{9}$	$\frac{1}{2}$	$\frac{5}{12}$	$\frac{1}{3}$	$\frac{1}{6}$	$\frac{1}{12}$	$\frac{2}{3}$	$\frac{5}{6}$
∞	∞	0	$\frac{1}{18}$	$\frac{1}{4}$	$\frac{1}{9}$	$\frac{1}{2}$	$\frac{5}{12}$	$\frac{1}{3}$	$\frac{1}{6}$	$\frac{1}{12}$	$\frac{2}{3}$	$\frac{5}{6}$
0	0	$\frac{1}{18}$	$\frac{1}{4}$	$\frac{1}{9}$	$\frac{1}{2}$	∞	$\frac{1}{3}$	$\frac{1}{6}$	$\frac{1}{12}$	$\frac{2}{3}$	$\frac{5}{6}$	$\frac{5}{12}$
$\frac{1}{18}$	$\frac{1}{18}$	$\frac{1}{4}$	$\frac{1}{9}$	$\frac{1}{2}$	∞	0	$\frac{1}{6}$	$\frac{1}{12}$	$\frac{2}{3}$	$\frac{5}{6}$	$\frac{5}{12}$	$\frac{1}{3}$
$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{9}$	$\frac{1}{2}$	∞	0	$\frac{1}{18}$	$\frac{1}{12}$	$\frac{2}{3}$	$\frac{5}{6}$	$\frac{5}{12}$	$\frac{1}{3}$	$\frac{1}{6}$
$\frac{1}{9}$	$\frac{1}{9}$	$\frac{1}{2}$	∞	0	$\frac{1}{18}$	$\frac{1}{4}$	$\frac{2}{3}$	$\frac{5}{6}$	$\frac{5}{12}$	$\frac{1}{3}$	$\frac{1}{6}$	$\frac{1}{12}$
$\frac{1}{2}$	$\frac{1}{2}$	∞	0	$\frac{1}{18}$	$\frac{1}{4}$	$\frac{1}{9}$	$\frac{5}{6}$	$\frac{5}{12}$	$\frac{1}{3}$	$\frac{1}{6}$	$\frac{1}{12}$	$\frac{2}{3}$
$\frac{5}{12}$	$\frac{5}{12}$	$\frac{1}{3}$	$\frac{1}{6}$	$\frac{1}{12}$	$\frac{2}{3}$	$\frac{5}{6}$	∞	0	$\frac{1}{18}$	$\frac{1}{4}$	$\frac{1}{9}$	$\frac{1}{2}$
$\frac{1}{3}$	$\frac{1}{3}$	$\frac{1}{6}$	$\frac{1}{12}$	$\frac{2}{3}$	$\frac{5}{6}$	$\frac{5}{12}$	0	$\frac{1}{18}$	$\frac{1}{4}$	$\frac{1}{9}$	$\frac{1}{2}$	∞
$\frac{1}{6}$	$\frac{1}{6}$	$\frac{1}{12}$	$\frac{2}{3}$	$\frac{5}{6}$	$\frac{5}{12}$	$\frac{1}{3}$	$\frac{1}{18}$	$\frac{1}{4}$	$\frac{1}{9}$	$\frac{1}{2}$	∞	0
$\frac{1}{12}$	$\frac{1}{12}$	$\frac{2}{3}$	$\frac{5}{6}$	$\frac{5}{12}$	$\frac{1}{3}$	$\frac{1}{6}$	$\frac{1}{4}$	$\frac{1}{9}$	$\frac{1}{2}$	∞	0	$\frac{1}{18}$
$\frac{2}{3}$	$\frac{2}{3}$	$\frac{5}{6}$	$\frac{5}{12}$	$\frac{1}{3}$	$\frac{1}{6}$	$\frac{1}{12}$	$\frac{1}{9}$	$\frac{1}{2}$	∞	0	$\frac{1}{18}$	$\frac{1}{4}$
$\frac{5}{6}$	$\frac{5}{6}$	$\frac{5}{12}$	$\frac{1}{3}$	$\frac{1}{6}$	$\frac{1}{12}$	$\frac{2}{3}$	$\frac{1}{2}$	∞	0	$\frac{1}{18}$	$\frac{1}{4}$	$\frac{1}{9}$

6 Information on $X_0(N)$ for N = {factors of 36}

The following information is the main result of my work. All of the terms have been defined and explained in the above sections. The reader is encouraged to check their understanding of the ideas presented here by working out a few of the results given below for themselves.

$X_0(2)$

Genus = 0

Parameter:

$$h_2 = \left(\frac{\eta_1}{\eta_2}\right)^{24}$$

$$h_2(q) = q^{-1} - 24 + 276q - 2048q^2 + 11202q^3 \ldots$$

$$(h_2) = (0) - (\infty)$$

Cusps and Coordinates of Cusps:

Cusp c	Coordinate h_2(c)	Eta-product with divisor (c) – (∞)
0	0	h_2
∞	∞	--

Moduli-Theoretic Maps:

$\pi_1: X_0(2) \rightarrow X(1)$

$$\pi_1^*(j) = \frac{(h_2 + 256)^3}{h_2^2}$$

$\pi_2: X_0(2) \rightarrow X(1)$

$$\pi_2^*(j) = \frac{(h_2 + 16)^3}{h_2}$$

$w_2: X_0(2) \rightarrow X_0(2)$

$$w_2^*(h_2) = \frac{4096}{h_2}$$

$X_0(3)$

Genus = 0

Parameter:

$$h_3 = \left(\frac{\eta_1}{\eta_3}\right)^{12}$$

$$h_3(q) = q^{-1} - 12 + 54q - 76q^2 - 243q^3 + 1188q^4 - 1384q^5 \ldots$$

$$(h_3) = (0) - (\infty)$$

Cusps and Coordinates of Cusps:

Cusp c	Coordinate $h_3(c)$	Eta-product with divisor (c) – (∞)
0	0	h_3
∞	∞	--

Moduli-Theoretic Maps:

$\pi_1: X_0(3) \rightarrow X(1)$

$$\pi_1^*(j) = \frac{(h_3 + 27)(h_3 + 243)^3}{h_3^3}$$

$\pi_3: X_0(3) \rightarrow X(1)$

$$\pi_3^*(j) = \frac{(h_3 + 27)(h_3 + 3)^3}{h_3}$$

$w_3: X_0(3) \rightarrow X_0(3)$

$$w_3^*(h_3) = \frac{729}{h_3}$$

$X_0(4)$

Genus = 0

Parameter:

$$h_4 = \left(\frac{\eta_1}{\eta_4}\right)^8$$

$$h_4(q) = q^{-1} - 8 + 20q - 62q^4 + 216q^6 - 641q^8 \ \ldots$$

$$(h_4) = (0) - (\infty)$$

Cusps and Coordinates of Cusps:

Cusp c	Coordinate $h_4(c)$	Eta-product with divisor (c) – (∞)
0	0	h_4
$\frac{1}{2}$	-16	$\frac{(\eta_2)^{24}}{(\eta_1)^8(\eta_4)^{16}}$
∞	∞	--

Moduli-Theoretic Maps:

$\pi_1: X_0(4) \rightarrow X_0(2)$

$$\pi_1^*(h_2) = \frac{h_4^2}{h_4 + 16}$$

$\pi_2: X_0(4) \rightarrow X_0(2)$

$$\pi_2^*(h_2) = h_4(h_4 + 16)$$

$w_4: X_0(4) \rightarrow X_0(4)$

$$w_4^*(h_4) = \frac{256}{h_4}$$

$X_0(6)$

Genus = 0

Parameter:

$$h_6 = \frac{(\eta_1)^5(\eta_3)}{(\eta_2)(\eta_6)^5}$$

$$h_6(q) = q^{-1} - 5 + 10q - 16q^2 + 35q^3 - 66q^4 \ \ldots$$

$$(h_6) = (0) - (\infty)$$

Cusps and Coordinates of Cusps:

Cusp c	Coordinate h_6(c)	Eta-product with divisor (c) – (∞)
0	0	h_6
$\frac{1}{2}$	-8	$\frac{(\eta_2)^3(\eta_3)^9}{(\eta_1)^3(\eta_6)^9}$
$\frac{1}{3}$	-9	$\frac{(\eta_2)^8(\eta_3)^4}{(\eta_1)^4(\eta_6)^8}$
∞	∞	--

Moduli-Theoretic Maps:

π_1: $X_0(6) \rightarrow X_0(3)$

$$\pi_1^*(h_3) = \frac{h_6^2(h_6+8)}{(h_6+9)^2}$$

π_3: $X_0(6) \rightarrow X_0(3)$

$$\pi_2^*(h_3) = \frac{h_6(h_6+8)^2}{h_6+9}$$

w_2: $X_0(6) \rightarrow X_0(6)$

$$w_2^*(h_6) = -8\left(\frac{h_6+9}{h_6+8}\right)$$

π_1: $X_0(6) \rightarrow X_0(2)$

$$\pi_1^*(h_2) = \frac{h_6^3(h_6+9)}{(h_6+8)^3}$$

π_3: $X_0(6) \rightarrow X_0(2)$

$$\pi_3^*(h_2) = \frac{h_6(h_6+9)^3}{h_6+8}$$

w_3: $X_0(6) \rightarrow X_0(6)$

$$w_3^*(h_6) = -9\left(\frac{h_6+8}{h_6+9}\right)$$

$X_0(9)$

Genus = 0

Parameter:

$$h_9 = \left(\frac{\eta_1}{\eta_9}\right)^3$$

$$h_9(q) = q^{-1} - 3 + 5q^2 - 7q^5 + 3q^8 + 15q^{11} \ldots$$

$$(h_9) = (0) - (\infty)$$

Cusps and Coordinates of Cusps:

Cusp c	Coordinate h_9(c)	Eta-product with divisor (c) – (∞)
0	0	h_9
$\frac{1}{3}, \frac{2}{3}$	roots of $h_9^2 + 9h_9 + 27 = 0$	--
∞	∞	--

Moduli-Theoretic Maps:

π_1: $X_0(9) \rightarrow X_0(3)$

$$\pi_1^*(h_3) = \frac{h_9^3}{h_9^2 + 9h_9 + 27}$$

π_3: $X_0(9) \rightarrow X_0(3)$

$$\pi_3^*(h_3) = h_9(h_9^2 + 9h_9 + 27)$$

w_9: $X_0(9) \rightarrow X_0(9)$

$$w_9^*(h_9) = \frac{27}{h_9}$$

$X_0(12)$

Genus = 0

Parameter:

$$h_{12} = \frac{(\eta_1)^3(\eta_4)(\eta_6)^2}{(\eta_2)^2(\eta_3)(\eta_{12})^3}$$

$$h_{12}(q) = q^{-1} - 3 + 2q + q^3 - 2q^7 - 2q^9 + 2q^{11} + \ldots$$

$$(h_{12}) = (0) - (\infty)$$

Cusps and Coordinates of Cusps:

Cusp c	Coordinate $h_{12}(c)$	Eta-product with divisor (c) – (∞)
0	0	h_{12}
$\frac{1}{2}$	-6	$\frac{(\eta_2)^7(\eta_3)}{(\eta_1)^3(\eta_4)^2(\eta_6)(\eta_{12})^2}$
$\frac{1}{3}$	-4	$\frac{(\eta_3)^3(\eta_4)}{(\eta_1)(\eta_{12})^3}$
$\frac{1}{4}$	-3	$\frac{(\eta_4)^4(\eta_6)^2}{(\eta_2)^2(\eta_{12})^4}$
$\frac{1}{6}$	-2	$\frac{(\eta_1)(\eta_4)^2(\eta_6)^9}{(\eta_2)^3(\eta_3)^3(\eta_{12})^6}$
∞	∞	--

Moduli-Theoretic Maps:

π_1: $X_0(12) \rightarrow X_0(6)$

$$\pi_1^*(h_6) = \frac{h_{12}^2}{h_{12}+2}$$

π_2: $X_0(12) \rightarrow X_0(6)$

$$\pi_2^*(h_6) = h_{12}(h_{12}+6)$$

w_4: $X_0(12) \rightarrow X_0(12)$

$$w_4^*(h_{12}) = -4\left(\frac{h_{12}+3}{h_{12}+4}\right)$$

π_1: $X_0(12) \to X_0(4)$

$$\pi_1^*(h_4) = \frac{h_{12}^3(h_{12}+4)}{(h_{12}+3)^3}$$

π_3: $X_0(12) \to X_0(4)$

$$\pi_3^*(h_4) = \frac{h_{12}(h_{12}+4)^3}{h_{12}+3}$$

w_3: $X_0(12) \to X_0(12)$

$$w_3^*(h_{12}) = -3\left(\frac{h_{12}+4}{h_{12}+3}\right)$$

$X_0(18)$

Genus = 0

Parameter:

$$h_{18} = \frac{(\eta_1)^2(\eta_6)(\eta_9)}{(\eta_2)(\eta_3)(\eta_{18})^2}$$

$$h_{18}(q) = q^{-1} - 2 + q^2 + q^5 - q^8 - q^{11} \ldots$$

$$(h_{18}) = (0) - (\infty)$$

Cusps and Coordinates of Cusps:

Cusp c	Coordinate h_{18}(c)	Eta-product with divisor (c) – (∞)
0	0	h_{18}
$\frac{1}{2}$	-3	$\frac{(\eta_2)^2(\eta_9)}{(\eta_1)(\eta_{18})^2}$
$\frac{1}{3}, \frac{2}{3}$	roots of $h_{18}^2 + 6h_{18} + 12 = 0$	--
$\frac{1}{6}, \frac{5}{6}$	roots of $h_{18}^2 + 3h_{18} + 3 = 0$	--
$\frac{1}{9}$	-2	$\frac{(\eta_6)(\eta_9)^3}{(\eta_3)(\eta_{18})^3}$
∞	∞	--

Moduli-Theoretic Maps:

π_1: $X_0(18) \rightarrow X_0(9)$

$$\pi_1^*(h_9) = \frac{h_{18}^2(h_{18}+3)}{(h_{18}+2)^2}$$

π_2: $X_0(18) \rightarrow X_0(9)$

$$\pi_2^*(h_9) = \frac{h_{18}(h_{18}+3)^2}{(h_{18}+2)}$$

w_2: $X_0(18) \rightarrow X_0(18)$

$$w_2^*(h_{18}) = -2\left(\frac{h_{18}+3}{h_{18}+2}\right)$$

π_1: $X_0(18) \to X_0(6)$

$$\pi_1^*(h_6) = \frac{h_{18}^3}{h_{18}^2+3h_{18}+3}$$

π_3: $X_0(18) \to X_0(6)$

$$\pi_3^*(h_6) = h_{18}(h_{18}^2+6h_{18}+12)$$

w_9: $X_0(18) \to X_0(18)$

$$w_9^*(h_{18}) = -3\left(\frac{h_{18}+2}{h_{18}+3}\right)$$

$X_0(36)$

Genus = 1

Parameters:

$$x = x_{36} = \frac{(\eta_2)^2(\eta_{12})(\eta_{18})}{(\eta_4)(\eta_6)(\eta_{36})^2}$$
$$x = x_{36}(q) = q^{-2} - 2 + q^4 + q^{10} - q^{16} - q^{22} \ldots$$
$$(x) = (0) + (\tfrac{1}{2}) - 2(\infty)$$

$$y = \frac{(\eta_1)^2(\eta_9)(\eta_{12})(\eta_{18})}{(\eta_2)(\eta_3)(\eta_{36})^3}$$
$$y(q) = q^{-3} - 2q^{-2} + 1 + 2q^3 - 2q^4 + q^9 \ldots$$
$$(y) = 2(0) + (\tfrac{1}{9}) - 3(\infty)$$

$$y^2 = x^3 - 4xy + 2x^2 - 6y$$

Cusps and Coordinates of Cusps:

Cusp c	Coordinate x(c)	Coordinate y(c)
0	0	0
$\frac{1}{2}$	0	-6
$\frac{1}{3}, \frac{2}{3}$	roots of $x^2 + 6x + 12 = 0$	roots of $y^2 - 12y + 48 = 0$
$\frac{1}{4}$	-3	3
$\frac{1}{6}, \frac{5}{6}$	roots of $x^2 + 6x + 12 = 0$	roots of $y^2 + 12 = 0$
$\frac{1}{9}$	-2	0
$\frac{1}{12}, \frac{5}{12}$	roots of $x^2 + 3x + 3 = 0$	roots of $y^2 + 3 = 0$
$\frac{1}{18}$	-2	2
∞	∞	∞

Moduli-Theoretic Maps:

π_1: $X_0(36) \rightarrow X_0(18)$

$$\pi_1^*(h_{18}) = \frac{y}{x+2}$$

π_2: $X_0(36) \to X_0(18)$

$$\pi_2^*(h_{18}) = x$$

w_4: $X_0(36) \to X_0(36)$

$$w_4^*(x, y) = \left(\frac{2x(3y - x^2)}{y^2}, \frac{4(x+3)}{y + 2x + 4} \right)$$

π_1: $X_0(36) \to X_0(12)$

$$\pi_1^*(h_{12}) = \frac{xy - x^2 + 3y}{x^2 + 3x + 3}$$

π_3: $X_0(36) \to X_0(12)$

$$\pi_3^*(h_{12}) = y + 2x$$

w_9: $X_0(36) \to X_0(36)$

$$w_9^*(x, y) = \left(\frac{-3(x+2)}{x+3}, \frac{-3(y - x^2 - 2x}{(x+3)^2} \right)$$

7 Cusp Ramification Diagrams

These diagrams are convenient visual aides in trying to figure out how different cusps ramify over certain curves. Analogously to towers of field extensions, the indices multiply in the obvious way in order to "skip" a curve.

Example 7.1

To find the index of the cusp $\frac{1}{3}$ in $X_0(18)$ over the cusp 0 in $X_0(3)$, by π_3 can be done in either of two ways: we could look at the tower $X_0(18) \xrightarrow{\pi_1} X_0(9) \xrightarrow{\pi_3} X_0(3)$, or we could look at the tower $X_0(18) \xrightarrow{\pi_3} X_0(6) \xrightarrow{\pi_1} X_0(3)$. The first tower and referencing below tells us that the index of the cusp $\frac{1}{3}$ in $X_0(18)$ over the cusp $\frac{2}{3}$ in $X_0(9)$, by π_1 is 2 and that the index of the cusp $\frac{2}{3}$ in $X_0(9)$ over the cusp 0 in $X_0(3)$, by π_3 is 1. Therefore we get that the index of the cusp $\frac{1}{3}$ in $X_0(18)$ over the cusp 0 in $X_0(3)$, by π_3 is 2 by multiplying the indices and composing the π_d's. It is left to the reader to check that they both give the same answer.

The indices in these diagrams were calculated using the Moduli-Theoretic approach to the curves. However, since this paper has taken the classical approach to modular curves, we give a description below on how to calculate the indices using the classical approach. Note that the method below gives the index for a cusp c in $X_0(N)$ over the cusp ∞ in $X(1)$. It is then necessary to use the above tower manipulations to find out what the index of a cusp c in $X_0(N)$ is over a cusp m in $X_0(M)$.

First it is necessary to choose a basis for the left cosets of $\Gamma / \Gamma_0(N)$. This is to say that a set of elements of Γ which are not in $\Gamma_0(N)$, $\{\gamma_0, ... \gamma_k\}$, must be chosen such that

1) Every element of $\Gamma_0(N)$ is in one of the equivalence classes $\gamma_i \Gamma$ for $i = 0,...,k$ and
2) that none of the γ_i are equivalent.

Checking condition 1 is just checking that any arbitrary element of $\Gamma_0(N)$ can be represented in at least one of the equivalence classes. Checking condition 2 amounts to checking that $\gamma_j^{-1}\gamma_i \notin \Gamma_0(N)$, which means that any arbitrary element of $\Gamma_0(N)$ can be represented in at most one of the equivalence classes.

Now we note that from [K], $\bigcup_{i=1}^{k} \gamma_i^{-1} F$ is a fundamental domain for $\Gamma_0(N)$, where F is the fundamental domain for Γ given by equation (2.4).

For each element γ_i of *B* which takes ∞ to c (or an equivalent point modulo $\Gamma_0(N)$), we do the following manipulation. We pick an arbitrary element z in F such that $-\frac{1}{2} \le \mathrm{Re}(z) \le \frac{1}{2}$ and Im(z)>>0 so that z is near the cusp ∞ in $X_0(N)$. We act on z first by γ_i^{-1}, then by π_d, then by A_i where A_i is a matrix in Γ which takes the resulting coefficients of z to ∞ in X(1). That is, if $\gamma_i^{-1} = \begin{bmatrix} e & f \\ g & h \end{bmatrix}$, then $A_i = \begin{bmatrix} r & s \\ g & -de \end{bmatrix}$ where r and s are integers such that $A_i \in \Gamma$ (which can be found using the Chinese Remainder Theorem again). We then count how many times each of the resulting expressions, acting on F, cover our original fundamental domain F.

Example 7.2

Find the index of the cusp ∞ in $X_0(2)$ for π_2. First of all we need a basis *B* for the left cosets of $\Gamma / \Gamma_0(2)$.

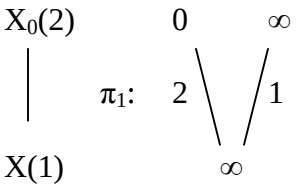
Let $B = \left\{ \gamma_0 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \gamma_1 = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}, \gamma_2 = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} \right\}$ be our basis.

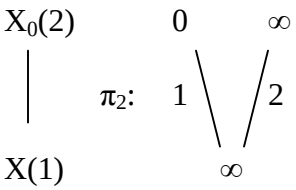
Checking condition 1 we note that $\gamma_0^{-1} = \gamma_0$, that $\gamma_0^{-1}\gamma_1 = \gamma_1$ and $\gamma_0^{-1}\gamma_2 = \gamma_2$, and neither of these are in $\Gamma_0(2)$. Also $\gamma_1^{-1}\gamma_2 = \begin{bmatrix} 1 & 0 \\ -1 & 1 \end{bmatrix}\begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ -1 & 0 \end{bmatrix}$ which is also clearly not in $\Gamma_0(2)$. It is left to the reader to check that condition 2 hold for *B*.

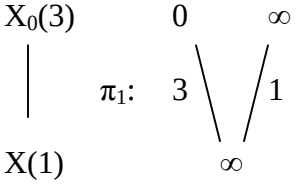
Well, $\gamma_0(\infty) = \infty$, $\gamma_1^{-1}(\infty) = -1$, and $\gamma_2^{-1}(\infty) = -1$. However we know that $-1 \sim 0$ as $\gamma(-1) = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}(-1) = \frac{-1+1}{0+1} = 0$ and $\gamma \in \Gamma_0(N)$. So for the index of the cusp 0 in $X_0(2)$ for π_2, we must then look at γ_1 and γ_2. For the index of the cusp ∞ in $X_0(2)$ for π_2, we just have to look at γ_0.

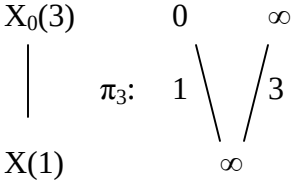
$z \xrightarrow{\gamma_0} z \xrightarrow{\pi_2} 2z \xrightarrow{A_0} 2z$ where $A_0 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$. Now 2z covers F twice. This can be seen by letting 2z act on F (i.e. we let z range through all of the points in F). We clearly get a domain, call it F', which has the same form as F but is twice as wide. Those points of F' which are also in F cover F once. The points outside of F are equivalent to points in F modulo $SL_2(\mathbf{Z})$ and cover F once again.

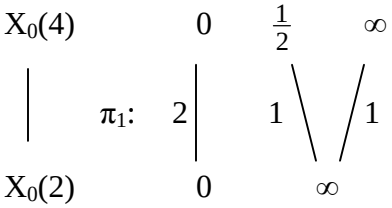
A similar procedure (left to the reader) will show that each of γ_1 and γ_2 cover a different half of F and they combine to cover F one time total.

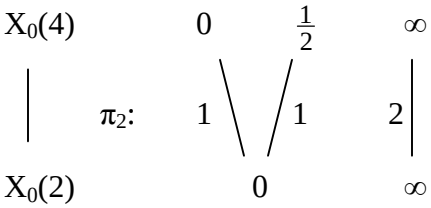

$X_0(2)$
0
∞
π_1:
2
1
$X(1)$
∞

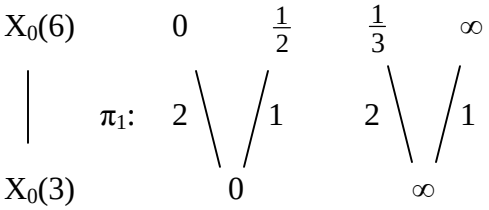

$X_0(2)$
0
∞
π_2:
1
2
$X(1)$
∞

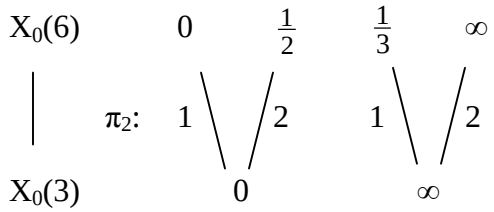

$X_0(3)$
0
∞
π_1:
3
1
$X(1)$
∞

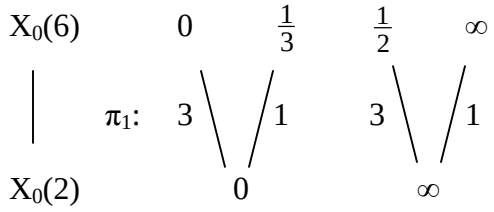

$X_0(3)$
0
∞
π_3:
1
3
$X(1)$
∞

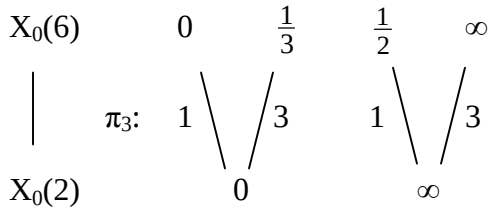

$X_0(4)$
0
$\frac{1}{2}$
∞
π_1:
2
1
1
$X_0(2)$
0
∞

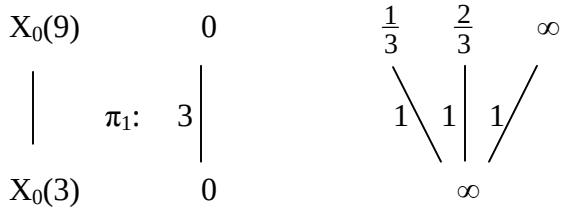

$X_0(4)$
0
$\frac{1}{2}$
∞
π_2:
1
1
2
$X_0(2)$
0
∞

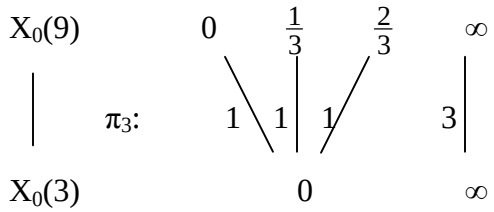

$X_0(6)$
0
$\frac{1}{2}$
$\frac{1}{3}$
∞
π_1:
2
1
2
1
$X_0(3)$
0
∞

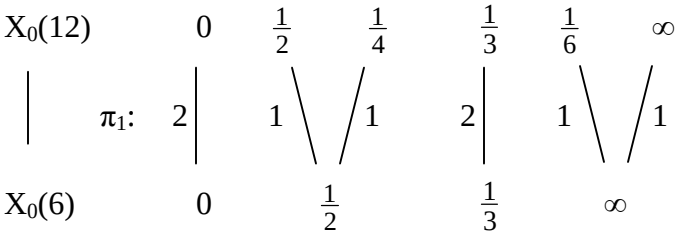

X0(6)
0
1/2
1/3
∞
π2:
1
2
1
2
X0(3)
0
∞

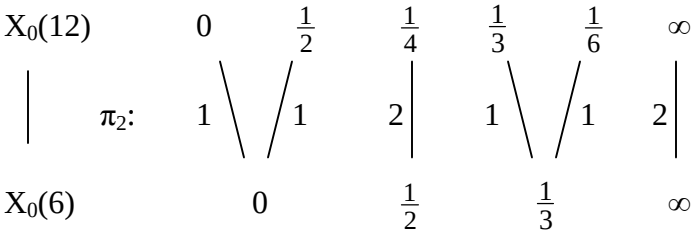

X0(6)
0
1/3
1/2
∞
π1:
3
1
3
1
X0(2)
0
∞

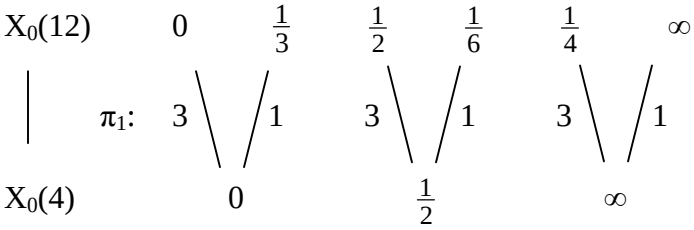

X0(6)
0
1/3
1/2
∞
π3:
1
3
1
3
X0(2)
0
∞

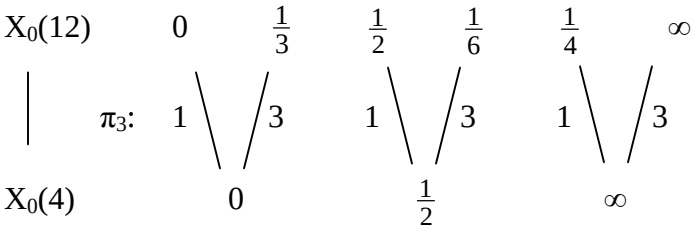

X0(9)
0
1/3
2/3
∞
π1:
3
1
1
1
X0(3)
0
∞

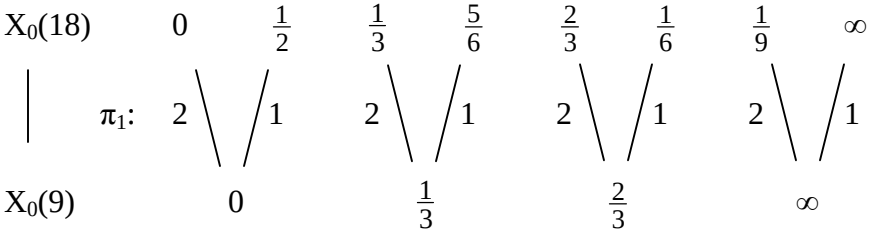

X0(9)
0
1/3
2/3
∞
π3:
1
1
1
3
X0(3)
0
∞

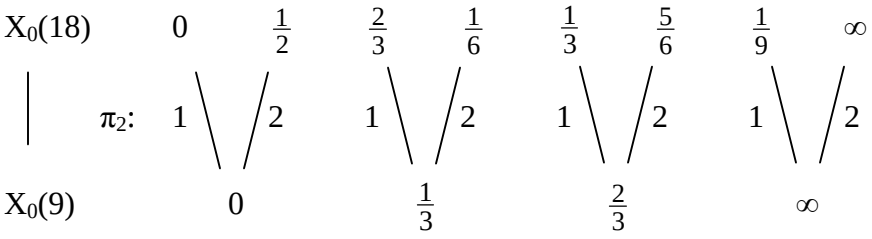

X0(12)
0
1/2
1/4
1/3
1/6
∞
π1:
2
1
1
2
1
1
X0(6)
0
1/2
1/3
∞

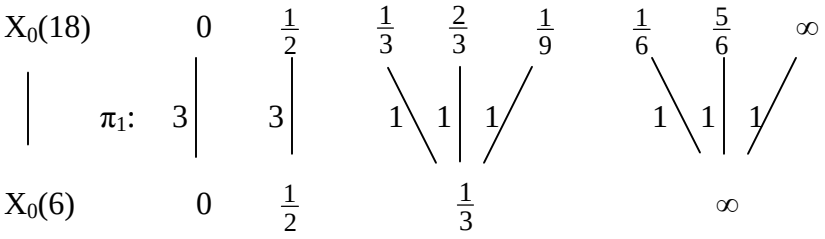

X0(12)
0
1/2
1/4
1/3
1/6
∞
π2:
1
1
2
1
1
2
X0(6)
0
1/2
1/3
∞

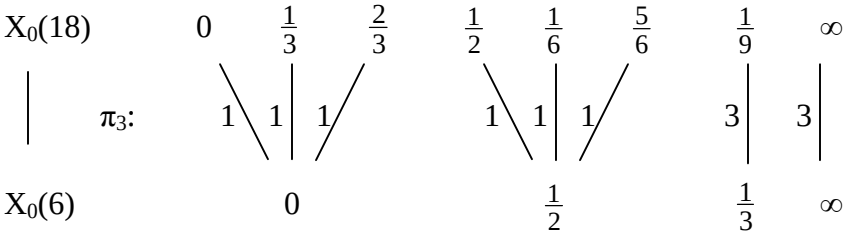

X0(12)
0
1/3
1/2
1/6
1/4
∞
π1:
3
1
3
1
3
1
X0(4)
0
1/2
∞

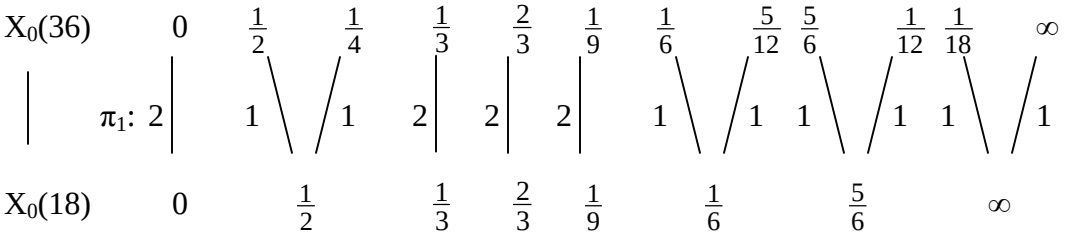

X0(12)
0
1/3
1/2
1/6
1/4
∞
π3:
1
3
1
3
1
3
X0(4)
0
1/2
∞

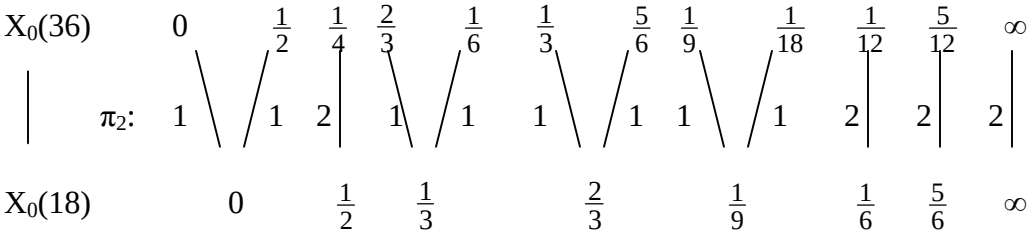

X0(18)
0
1/2
1/3
5/6
2/3
1/6
1/9
∞
π1:
2
1
2
1
2
1
2
1
X0(9)
0
1/3
2/3
∞

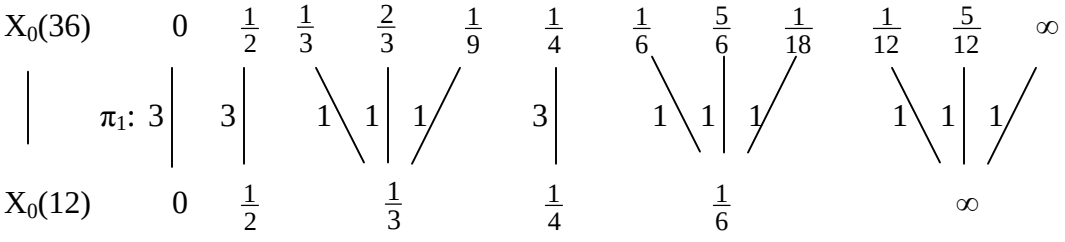

X0(18)
0
1/2
2/3
1/6
1/3
5/6
1/9
∞
π2:
1
2
1
2
1
2
1
2
X0(9)
0
1/3
2/3
∞

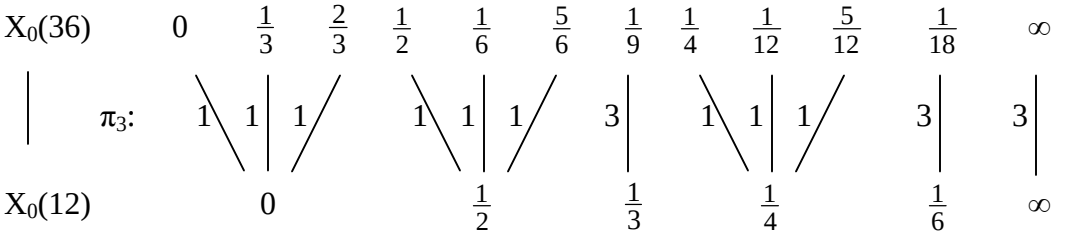

X0(18)
0 1/2 1/3 2/3 1/9 1/6 5/6 ∞
π1:
3 3 1 1 1 1 1 1
X0(6)
0 1/2 1/3 ∞


X0(18)
0 1/3 2/3 1/2 1/6 5/6 1/9 ∞
π3:
1 1 1 1 1 1 3 3
X0(6)
0 1/2 1/3 ∞


X0(36)
0 1/2 1/4 1/3 2/3 1/9 1/6 5/12 5/6 1/12 1/18 ∞
π1:
2 1 1 2 2 2 1 1 1 1 1 1
X0(18)
0 1/2 1/3 2/3 1/9 1/6 5/6 ∞


X0(36)
0 1/2 1/4 2/3 1/6 1/3 5/6 1/9 1/18 1/12 5/12 ∞
π2:
1 1 2 1 1 1 1 1 1 2 2 2
X0(18)
0 1/2 1/3 2/3 1/9 1/6 5/6 ∞


X0(36)
0 1/2 1/3 2/3 1/9 1/4 1/6 5/6 1/18 1/12 5/12 ∞
π1:
3 3 1 1 1 3 1 1 1 1 1 1
X0(12)
0 1/2 1/3 1/4 1/6 ∞


X0(36)
0 1/3 2/3 1/2 1/6 5/6 1/9 1/4 1/12 5/12 1/18 ∞
π3:
1 1 1 1 1 1 3 1 1 1 3 3
X0(12)
0 1/2 1/3 1/4 1/6 ∞

8 Divisors of $X_0(N)$ for N = {factors of 36}

The following is merely an extension of the above section. The divisor of Δ_k in $X_0(N)$, for all k dividing N, were each computed using the cusp ramification diagrams from section 7 and then laid out in the table below. To calculate the divisor for any specific Δ_k in any specific $X_0(N)$, it is necessary to choose an appropriate tower of curves such that it starts at $X_0(N)$ and goes all the way down to X(1) and that the π_{d_i}'s are chosen such that the product over the d_i's equals k. For example, the tower $X_0(12) \xrightarrow{\pi_2} X_0(6) \xrightarrow{\pi_3} X_0(2) \xrightarrow{\pi_1} X(1)$ gives the divisor of Δ_6 in $X_0(12)$.

N	Divisors for $X_0(N)$
2	$\begin{array}{c\|cc} & (\Delta(q)) & (\Delta(q^2)) \\ \hline 0 & 2 & 1 \\ \infty & 1 & 2 \end{array}$
3	$\begin{array}{c\|cc} & (\Delta(q)) & (\Delta(q^3)) \\ \hline 0 & 3 & 1 \\ \infty & 1 & 3 \end{array}$
4	$\begin{array}{c\|ccc} & (\Delta(q)) & (\Delta(q^2)) & (\Delta(q^4)) \\ \hline 0 & 4 & 2 & 1 \\ \frac{1}{2} & 1 & 2 & 1 \\ \infty & 1 & 2 & 4 \end{array}$
6	$\begin{array}{c\|cccc} & (\Delta(q)) & (\Delta(q^2)) & (\Delta(q^3)) & (\Delta(q^6)) \\ \hline 0 & 6 & 3 & 2 & 1 \\ \frac{1}{3} & 2 & 1 & 6 & 3 \\ \frac{1}{2} & 3 & 6 & 1 & 2 \\ \infty & 1 & 2 & 3 & 6 \end{array}$
9	$\begin{array}{c\|ccc} & (\Delta(q)) & (\Delta(q^3)) & (\Delta(q^9)) \\ \hline 0 & 9 & 3 & 1 \\ \frac{1}{3} = \frac{2}{3} & 1 & 3 & 1 \\ \infty & 1 & 3 & 9 \end{array}$

12

	$(\Delta(q))$	$(\Delta(q^2))$	$(\Delta(q^3))$	$(\Delta(q^4))$	$(\Delta(q^6))$	$(\Delta(q^{12}))$
0	12	6	4	3	2	1
$\frac{1}{6}$	1	2	3	1	6	3
$\frac{1}{4}$	3	6	1	12	2	4
$\frac{1}{3}$	4	2	12	1	6	3
$\frac{1}{2}$	3	6	1	3	2	1
∞	1	2	3	4	6	12

18

	$(\Delta(q))$	$(\Delta(q^2))$	$(\Delta(q^3))$	$(\Delta(q^6))$	$(\Delta(q^9))$	$(\Delta(q^{18}))$
0	18	9	6	3	2	1
$\frac{1}{9}$	2	1	6	3	18	9
$\frac{1}{6}=\frac{5}{6}$	1	2	3	6	1	2
$\frac{1}{3}=\frac{2}{3}$	2	1	6	3	2	1
$\frac{1}{2}$	9	18	3	6	1	2
∞	1	2	3	6	9	18

36

	$(\Delta(q))$	$(\Delta(q^2))$	$(\Delta(q^3))$	$(\Delta(q^4))$	$(\Delta(q^6))$	$(\Delta(q^9))$	$(\Delta(q^{12}))$	$(\Delta(q^{18}))$	$(\Delta($
0	36	18	12	9	6	4	3	2	
$\frac{1}{18}$	1	2	3	1	6	9	3	18	
$\frac{1}{12}=\frac{5}{12}$	1	2	3	4	6	1	12	2	
$\frac{1}{9}$	4	2	12	1	6	36	3	18	
$\frac{1}{6}=\frac{5}{6}$	1	2	3	1	6	1	3	2	
$\frac{1}{4}$	9	18	3	36	6	1	12	2	
$\frac{1}{3}=\frac{2}{3}$	4	2	12	1	6	4	3	2	
$\frac{1}{2}$	9	18	3	9	6	1	3	2	
∞	1	2	3	4	6	9	12	18	3

9 Quick Matlab program to find the cusps of $X_0(N)$

This function is best used to find out what the cusps are on $X_0(N)$. The points eligible to be cusps on $X_0(N)$ are those fractions $\frac{p}{q}$ between 0 and 1, inclusive, such that q divides N and p ranges from 0 to q. Clearly, we can assume that $\frac{p}{q}$ is in lowest terms as well.

Note: for all N, $0 \sim 1$ and $\frac{1}{N} \sim \infty$, since

$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ and $\begin{bmatrix} 1 & 0 \\ N & 1 \end{bmatrix}$ are in $\Gamma_0(N)$ for all N and

$f\left(\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}(0)\right) = 1$ and $f\left(\begin{bmatrix} 1 & 0 \\ N & 1 \end{bmatrix}(\infty)\right) = \frac{1}{N}$

Example 9.1: Look at $X_0(12)$

The eligible cusps are then: $0, \frac{1}{2}, \frac{1}{3}, \frac{2}{3}, \frac{1}{4}, \frac{3}{4}, \frac{1}{6}, \frac{5}{6}, \infty$

It is then quick to check that $\frac{1}{3} \sim \frac{2}{3}, \frac{1}{4} \sim \frac{3}{4}, \frac{1}{6} \sim \frac{5}{6}$ using the program. So then our cusps on $X_0(12)$ would be: $0, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \frac{1}{6}, \infty$

```
function y=congruent(p, q, r, s, N, k)
%This function will find matrices of SL_2(Z)
%such that [a b;c d](p/q)=(r/s) in X_0(N).
%  Note: (p/q) and (r/s) must be in lowest terms.
%  Note: 0 = (0/1).  It can't check if p/q ~ infinity,
%        but that is easy enough to do by hand since
%        [a b;c d](infinity) = a/c.
for x=-k:k
   [(N*r*x+q)/s (r-p*((N*r*x+q)/s))/q;N*x (s-p*N*x)/q]
end
%k is just a guess on the number of matrices to check to see if p/q ~ r/s
%k=10 is usually more than sufficient
```

Now you just have to look and see if any of the resulting matrices have all integer entries. If so, then $\frac{p}{q} \sim \frac{r}{s}$. If not, then $\frac{p}{q} \not\sim \frac{r}{s}$.

References

[DI] F. Diamond and J. Im, *Modular Forms and Modular Curves*, Seminar on Fermat's Last Theorem, Providence, RI (1995), pp. 5-10.

[H] R. Hartshorne, *Algebraic Geometry*, Springer-Verlag, New York, NY (1977).

[K] N. Koblitz, *Introduction to Elliptic Curves and Modular Forms*, Springer-Verlag, New York, NY (1993).

[L] G. Ligozat, *Courbes modulaires de genre 1*, Bull. Soc. Math. France Mémoires, **43** (1975).

[M] K. McMurdy, *A Splitting Criterion for Galois Representations Associated to Exceptional Modular Forms*, Ph.D. thesis, University of California, Berkeley, 2001.

[Sh] Shimura, *Introduction to the arithmetic theory of automorphic functions*, Princeton University Press (1971).

[Sil] J.H. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, New York, NY (1986).