國　立　交　通　大　學

應　用　數　學　系

碩 士 論 文

有理橢圓曲線的模參數化

Modular Parameterization of Rational Elliptic Curves

研 究 生：涂芳婷

指導教授：楊一帆　教授

中 華 民 國 九 十 五 年 七 月

有理橢圓曲線的模參數化

Modular Parameterization of Rational Elliptic Curves

研 究 生：涂芳婷　　Student：Fang-Ting Tu

指導教授：楊一帆 教授　　Advisor：Yifan Tang

國 立 交 通 大 學

應用數學系

碩 士 論 文

A Thesis

Submitted to Department of Applied Mathematics

College of Science

National Chiao Tung University

in partial Fulfillment of the Requirements

for the Degree of

Master

in

Applied Mathematics

July 2006

Hsinchu, Taiwan, Republic of China

中華民國九十五年七月

自　序

待在交大應數已將近六個年頭，前些年，是看過不少書，也修了不少課，卻也只能用不學無術來形容。有幸於大學的最後一年碰上我的指導教授楊一帆，使我碩士這兩年的學習生涯增色不少。

教授個性溫和謙虛，縱使有我如此不材的學生，仍保有耐性傾囊相授。不論是學習遇到的困難亦或是生活中的挫折，一路走來，始終盡其所能給我最大的幫助。八股地如同小時候的作文，卻也是事實：教授是良師、是益友，他的諄諄教誨，循循善誘，「搏我以文、約我以禮」，逐漸地扎實了我的認知。獻萬分的謝意給我的指導教授，楊一帆。

除了感謝家人多年來的支持與鼓勵，在此感謝所有授予學識的老師、教授，使我的學習更有組織性；特別感謝蔡孟傑教授，許世雄教授，陳燕美教授，以及其餘兩位碩士論文的口試委員：潘戍衍教授及 Professor Michael Fuchs，使我的學習更趨完整。也謝謝我的好友們、學長姐、學弟妹，陪我偷懶、陪我學習、陪我喜怒哀樂，豐富了我的生活。

這篇論文的概念，延續了指導教授的論文，目前只完成了一部分的結果；未來的日子裡，將繼續完成其餘部分，且讓這些結果更完美。

謹以此，獻給驟逝的父親，共同分享這份未能趕上的喜悅。

有理橢圓曲線的模參數化

研究生：涂芳婷　　指導教授：楊一帆 教授

國 立 交 通 大 學

應用數學系

摘　要

二十世紀末，Andrew Wile 證明了 谷山-志村猜想，也間接地證明著名的費瑪最後定理。而這個猜想的敘述是說：只要給定任何一個有理橢圓曲線，我們都能夠找到一個自然數 N 以及模函數將其參數化。然而，目前沒有人將有理橢圓曲線是如何模參數化的型式完整寫下。

在楊一帆教授的論文"Defining equations of modular curves”裡提到我們如何利用廣義的 Dedekind eta 函數建構在模曲線 $X_0(N)$ 上模函數域的生成元，提供了將有理橢圓曲線模參數化的方法。在這裡，我們利用相同的概念以及類似的方法將本身就是模曲線且型式為 $X_0(p)$ 或 $X_0^+(p)$ 的有理橢圓曲線模參數化，其中 p 為質數。方法如下：

一. 型式為 $X_0(p)$，我們找兩個模函數 X ，Y 在無限大有極點且次數分別為二跟三。

二. 型式為 $X_0^+(p)$，我們有兩種方法：

1. 利用模曲線 $X_0(p)$ 上模函數域的生成元建構上述的兩個模函數。
2. 利用”一個全形的(holomorphic)的 differential 1-form 本身就是一個 cusp form of weight 2”的性質以及給定的有理橢圓曲線唯一決定我們要的這兩個模函數。

中華民國九十五年七月

Modular Parameterization of Rational Elliptic Curves

Fang-Ting Tu

Department of Applied Mathematics
National Chiao Tung University
Hsinchu, Taiwan

July 17, 2006

Modular Parameterization of Rational Elliptic Curves

Student: Fang-Ting Tu **Advisor: Yifan Yang**

Department of Applied Mathematics
National Chiao Tung University

July 2006

Abstract

The well-known Taniyama-Shimura conjecture states that for every rational elliptic curve

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

there is a natural integer N and a rational map such that

$$\phi : X_0(N) \to E.$$

To complete the proof of Fermat's Last Theorem, this conjecture plays an important role. Although it was proved by Andrew Wiles, it is difficult to find a rational map ϕ for a given rational elliptic curve actually. In this thesis, we will find modular functions that parameterize elliptic curves that are actually modular curves of type $X_0(p)$ or $X_0^+(p)$, where p are prime numbers.

Our basis ideas are referred to Y. Yang's *Defining equations of modular curves*. We use the Dedekind eta function and generalized Dedekind eta functions to construct generators of modular function fields on $X_0(p)$. Then we use distinct ways to parameterize the given elliptic curves, the methods are as follows.

1. For $X_0(p)$, find X with pole at ∞ of order 2, and find Y with pole at ∞ of order 3.
2. For $X_0^+(p)$,
   (a) using the generators of the function field on $X_0(p)$ to construct the functions with pole at ∞ of order 2 and 3.
   (b) using the fact that the holomorphic 1-forms on a modular curves are actually cusp forms of weight 2.

Contents

1 Introduction **2**

2 Modular curves and Modular forms **4**
2.1 Congruence subgroups of $PSL_2(\mathbb{R})$ 4
2.2 Modular curves 5
2.3 Modular forms and Modular functions 8
2.4 Petersson Inner Product and Hecke Operators 11

3 Elliptic Curves **17**
3.1 Definitions 17
3.2 Taniyama-Shimura Conjecture 20

4 Modular parameterizations **21**
4.1 Genera of $X_0(p)$ and $X_0^+(p)$ 21
4.2 Methods for finding modular parameterizations 22
4.3 Results 29

Notations

1. We use the notations $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}$, $\mathbb{Z}$, and $\mathbb{N}$ to stand for the real number field, the complex number field, the rational number field, the ring of integers, and the set of positive integers, respectively. And $\mathbb{P}^1(\mathbb{C}) = \mathbb{C} \cup \{\infty\}$, the Riemann sphere; $\mathbb{P}^1(\mathbb{Q}) = \mathbb{Q} \cup \{\infty\}$; $\mathbb{H} = \{\tau \in \mathbb{C} : \operatorname{Im} \tau > 0\}$, the upper half plane; $\mathbb{H}^* = \mathbb{H} \cup \mathbb{Q} \cup \{\infty\}$.

2. For any commutative ring R with unity 1, the vector space $M_n(R)$ is defined to be the set of square matrices with degree n over R; the general linear group $GL_n(R) = \{\gamma \in M_n(R) : \det \gamma \in R^\times\}$, where $R^\times = \{a \in R : a \text{ is an unit}\}$ is the group of invertible elements in R. The special linear group $SL_n(R)$ is defined to be the subgroup of $\mathrm{GL}_n(R)$ consisting of matrices of determine 1. In the sequel, we mostly consider the rings $R = \mathbb{R}$, $\mathbb{Z}$, or $\mathbb{Z}_N$, for $N \in \mathbb{N}$. And we denote $\{\gamma \in GL_n(\mathbb{R}) : \det \gamma > 0\}$ by $GL_n^+(\mathbb{R})$.

Chapter 1

Introduction

In a famous story about Fermat it is said that Fermat once wrote in his copy of Diophantus' Arithmetica that he had a truly marvelous proof of the fact that the equation

$$x^n + y^n = z^n$$

has no solutions in positive integers when $n \geq 3$, but the proof was too long to be contained in the margin of the book. However, during Fermat's lifetime, he never published the claimed proof. Afterwards, many great mathematicians tried to produce a legitimate proof, but to no avail, and this problem became widely known as Fermat's Last Theorem. It was not until 1995 that an English mathematician Andrew Wiles, assisted by his student Richard Taylor, finally put an end to this 350 year old puzzle.

It turns out that what Wiles did was not a direct attack on Fermat's Last Theorem, but an effort to prove the Taniyama-Shimura conjecture. In 1957, Yutaka Taniyama, a young mathematician in Japan, based on some numerical examples, made a daring conjecture that there is a one-to-one correspondence between rational elliptic curves and cusp forms. This conjecture was later made more rigorous by Goro Shimura. To be more precise, the conjecture states that the L-function of a rational elliptic function is equal to the L-function of a cusp form of weight 2 on a certain modular curve $X_0(N)$. Putting it an alternative way, this means that every rational elliptic curve can be parameterized by modular functions on $X_0(N)$ for some N. In 1986 Ken Ribet proved that any non-trivial solution to $x^n + y^n = z^n$, $n \geq 3$, will give rise to an elliptic curve that is too weird to be modular. Wiles then proceeded to prove the Taniyama-Shimura conjecture for the semistable cases, and hence establsihed Fermat's Last Theorem. However, we should remark that in general it is difficult to find modular functions that parameterize a given rational elliptic curve. In this thesis we will address this problem. In particular, we will find modular functions that parameterize elliptic curves that are modular curves of type $X_0(p)$ or $X_0^+(p)$ themselves, where p are prime numbers.

Our method is basically an extension of Yang's method [16]. In [15] Y. Yang obtained transformation formulas for generalized Dedekind eta functions (see Section 2.3.3), from which he deduced criteria for a product of generalized Dedekind eta functions to be modular on $X(N)$ or $X_1(N)$. Using these simple criteria, he then devised a systematic method of finding generators of modular function fields on modular curves of type $X(N)$, $X_1(N)$, and $X_0(N)$. Since finding modular parameterizations of elliptic modular curves $X_0^+(p)$ is equivalent to finding generators of function fields on $\Gamma_0^+(p)$, this thesis can naturally be considered as a continuation of Yang's work [16]. (Here we should remark that our method works also in the cases where the levels are not primes. The main reason

why we consider only the prime cases here is that this thesis has to be submitted by a certain deadline.)

The rest of thesis is organized as follows. In Chapters 2 and 3 we will briefly review the definition and basic properties of modular curves and elliptic curves. Finally, in the last chapter of the thesis we will describe our method in more details and give the results of our computation.

Chapter 2

Modular curves and Modular forms

Almost all of this chapter are from the *Lecture Notes on Modular Forms and Modular Functions* by Y. Yang [17]. Some sources are given by T. Miyake's *Modular Forms* [10] and T.M. Apostol's *Modular Functions and Dirichlet Series in Number Theory* [1].

2.1 Congruence subgroups of $PSL_2(\mathbb{R})$

In general, we call $PSL_2(\mathbb{Z})$ the *modular group*. There are many subgroups of finite index of $PSL_2(\mathbb{Z})$. Among them, we are interested in congruence subgroup.

Definition 2.1.1 Let Γ be a discrete subgroup of $PSL_2(\mathbb{R})$ commensurable with $PSL_2(\mathbb{Z})$. If Γ contains the subgroup

$$\Gamma(N) = \left\{ \gamma \in PSL_2(\mathbb{Z}) : \gamma \equiv \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mod N \right\}$$

for some positive integer N, then Γ is a *congruence subgroup*. The smallest such positive integer N is the *level* of Γ. The group $\Gamma(N)$ is called the *principal congruence subgroup* of level N.

The following two types of congruence subgroups

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in PSL_2(\mathbb{Z}) : c \equiv 0 \mod N \right\},$$

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in PSL_2(\mathbb{Z}) : c \equiv 0, a \equiv d \equiv \pm 1 \mod N \right\}$$

are most often encountered in number theory. The congruence subgroups $\Gamma_0(N)$ are also called the *Hecke congruence subgroups* and are conjugate to

$$\Gamma^0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in PSL_2(\mathbb{Z}) : b \equiv 0 \mod N \right\}$$

in $PSL_2(\mathbb{R})$.

Proposition 2.1.2 *We have*

(1) $\Gamma_1(N)$ *is a normal subgroup of* $\Gamma_0(N)$ *and* $\Gamma_0(N)/\Gamma_1(N) \simeq \mathbb{Z}_N^\times / \pm 1$, *where* $\mathbb{Z}_N^\times$ *is the multiplicative group of residue classes modulo* N *that are relatively prime to* N.

(2) $\Gamma(N)$ *is a normal subgroup of* $PSL_2(\mathbb{Z})$ *and* $PSL_2(\mathbb{Z})/\Gamma(N) \simeq SL_2(\mathbb{Z}_N)/\pm 1$.

2.1.1 The index of a congruence subgroup in $PSL_2(\mathbb{Z})$

From the last section, we can determine the indices of the congruence groups.

Proposition 2.1.3 *We deduce that*

(1) $[\Gamma_1(N) : \Gamma(N)] = N$,
(2) $\Gamma_0(2) = \Gamma_1(2)$ *and*

$$[\Gamma_0(N) : \Gamma_1(N)] = \frac{N}{2} \prod_{p|N} \left(1 - \frac{1}{p}\right), \text{ for } N \geq 3.$$

(3)

$$[PSL_2(\mathbb{Z}) : \Gamma_0(N)] = N \prod_{p|N} (1 + 1/p),$$

where the products run over all prime divisors p of N.

2.1.2 Atkin-Lehner involutions

Let $N \geq 2$ be any positive integer.

Definition 2.1.4 Let n be a divisor of N with $\gcd(n, N/n) = 1$. The elements in

$$w_n = \left\{ \frac{1}{\sqrt{n}} \begin{pmatrix} an & b \\ cN & dn \end{pmatrix}, \ adn^2 - bcN = n \right\}$$

are the *Atkin-Lehner involutions* on $\Gamma_0(N) \setminus \mathbb{H}$. The set of $\Gamma_0(N)$ union all possible Atkin-Lehner involutions is denoted by $\Gamma_0^+(N)$.

Proposition 2.1.5 *The Atkin-Lehner involutions normalize $\Gamma_0(N)$. Furthermore, we have $\Gamma_0^+(N)/\Gamma_0(N) \simeq \mathbb{Z}_2^k$, where k is the number of distinct prime divisors of N.*

2.2 Modular curves

2.2.1 Group action of $PSL_2(\mathbb{Z})$ on $\mathbb{H}$

Recall that the linear fractional transformation of $\mathbb{H}$ is given by

$$\gamma \ : \ \tau \mapsto \frac{a\tau + b}{c\tau + d}, \ a, b, c, d \in \mathbb{R}, \ ad - bc > 0,$$

and a linear fractional transformation γ determines the matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2^+(\mathbb{R})$ up to a scalar multiplication. Hence, dividing by a suitable scalar, we may represent γ by a matrix of determinant 1. The group $SL_2(\mathbb{R})$ contains $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ and $-I = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ which act trivially, and the group $PSL_2(\mathbb{R})$ is identified with the group of linear fractional transformations. It is not difficult to check that the definition of linear fractional transformations gives a group action of $PSL_2(\mathbb{R})$ on $\mathbb{H}$.

Let Γ be a congruence subgroup of finite index of $PSL_2(\mathbb{Z})$. Then $\mathbb{H}$ and $\mathbb{H}^* = \mathbb{H} \cup \mathbb{Q} \cup \{\infty\}$ are acted on discontinuously by Γ. The set $\{\Gamma x : x \in \mathbb{H}\}$ of all orbits forms

the quotient space $\Gamma \setminus \mathbb{H}$. Note that a group action gives rise to an equivalence relation given by $x \sim y$ if and only if there is an element γ lying in Γ such that $\gamma x = y$. The equivalence class containing x is exactly Γx. The classical modular curve $\mathrm{X}(\Gamma)$ is defined by the quotient space $\Gamma \setminus \mathbb{H}^*$. For the ease of notation, we abbreviate $X(\Gamma_0(N))$ to $X_0(N)$, $X(\Gamma_1(N))$ to $X_1(N)$, and $X(\Gamma(N))$ to $X(N)$.

Now we consider the fix points of linear fractional transformations. Let $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in PSL_2(\mathbb{R})$ be a representation of a linear fractional transformation. The points fixed by γ are the roots of $c\tau^2 + (d-a)\tau - b = 0$. When $\gamma = \pm I$, every point is fixed by γ, and this identity motion forms a class by itself. When $\gamma \neq \pm I$, there are three possibilities,

(1) γ has one fixed point on $\mathbb{P}^1(\mathbb{R})$, and this γ is called *parabolic*;
(2) γ has two distinct fixed points on $\mathbb{P}^1(\mathbb{R})$, and this γ is called *hyperbolic*;
(3) γ has a pair of conjugate complex numbers as fixed points, and this γ is called *elliptic*.

These classifications can be also described in terms of the trace of γ,

Lemma 2.2.1 *Let $\gamma \in PSL_2(\mathbb{R})$. Then*

(1) γ is parabolic if and only if $\mathrm{tr}(\gamma) = 2$;
(2) γ is hyperbolic if and only if $\mathrm{tr}(\gamma) > 2$;
(3) γ is elliptic if and only if $\mathrm{tr}(\gamma) < 2$.

Definition 2.2.2 A point on $\mathbb{P}^1(\mathbb{R})$ fixed by a parabolic element is called a *cusp*, and a point in $\mathbb{H}$ fixed by an elliptic element is called an *elliptic point*.

Proposition 2.2.3 *The set of cusps of $PSL_2(\mathbb{Z})$ is $\mathbb{P}^1(\mathbb{Q})$, and the cusps are all equivalent to each other under $PSL_2(\mathbb{Z})$.*

Proposition 2.2.4 *Now we consider elliptic element and elliptic point of $PSL_2(\mathbb{Z})$*

(1) Every elliptic element of $PSL_2(\mathbb{Z})$ has order 2 or 3.

(2) An element of $PSL_2(\mathbb{Z})$ has order 2 if and only if its trace is 0. An element has order 3 if and only if its trace has absolute value 1.

(3) Every elliptic element of order 2 is conjugate to $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ in $PSL_2(\mathbb{Z})$. Every elliptic element of order 3 is conjugate to either $\begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$ or $\begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}$.

(4) $PSL_2(\mathbb{Z}) \setminus \mathbb{H}$ has only two inequivalent elliptic points. One is represented by i, which is of order 2; the other is represented by $e^{\pi i/3}$, which is of order 3. That is ,if $\tau \in \mathbb{H}$ is of order 2, then τ is equivalent to i; if it is of order 3, it is equivalent to $e^{\pi i/3}$.

2.2.2 Cusps and Elliptic points of congruence subgroups

Here we discuss the cusps and elliptic points of congruence subgroups.

Lemma 2.2.5 *Let Γ be a congruence subgroup of $PSL_2(\mathbb{Z})$, then the set of cusps of Γ is exactly $\mathbb{P}^1(\mathbb{Q})$.*

Definition 2.2.6 Let Γ be a congruence subgroup of $PSL_2(\mathbb{Z})$. Let $a/c \in \mathbb{P}^1(\mathbb{Q})$ be a cusp. The smallest positive integer m such that the matrix

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \begin{pmatrix} 1-acm & a^2m \\ -c^2m & 1+acm \end{pmatrix} \tag{2.1}$$

falls in Γ is called the *width* of the cusp a/c.

Remark. In fact, a cusp a/c is fixed by the matrix describing in (2.1).

Proposition 2.2.7 *A set of inequivalent cusps for $\Gamma_0(N)$ is given by*

$$\left\{ \frac{a}{c} : c|N,\ a = 0, \ldots, \gcd(c, N/c) - 1,\ \gcd(a, c) = 1 \right\}.$$

Hence the number of inequivalent cusps is

$$\sum_{c|N} \phi(\gcd(c, N/c)).$$

The number of inequivalent cusps for $\Gamma_1(N)$, $N \geq 3$, is

$$\frac{1}{2} \sum_{c|N} \phi(c)\phi(N/c),$$

where ϕ is the Euler totient function.

Proposition 2.2.8 *The number v_2 of inequivalent elliptic points of order 2 for $\Gamma_0(N)$ is equal to the number of solutions of $x^2 + 1 = 0$ in $\mathbb{Z}_N$. That is, when $4|N$, $v_2 = 0$ and*

$$\text{when } 4 \nmid N,\ v_2 = \prod_{p|N,\, p \text{ odd prime}} \left(1 + \left(\frac{-1}{p}\right)\right).$$

The number v_3 of inequivalent elliptic points of order 3 for $\Gamma_0(N)$ is equal to the number of solutions of $x^2 + x + 1 = 0$ in $\mathbb{Z}_N$. That is, when $9|N$, $v_3 = 0$, and

$$\text{when } 9 \nmid N,\ v_3 = \prod_{p|N,\, p \text{ odd prime}} \left(1 + \left(\frac{-3}{p}\right)\right),$$

where $\left(\frac{a}{b}\right)$ is the Legendre symbols.

Proposition 2.2.9 *When $N \geq 4$, the congruence subgroups $\Gamma_1(N)$ are torsion-free. When $N \geq 2$, the principal congruence subgroups $\Gamma(N)$ are torsion-free.*

2.2.3 Genus

Let Γ be a subgroup of $PSL_2(\mathbb{Z})$ of index m. We now determine the genus of $X(\Gamma)$. Let v_2, v_3, v_∞ be the numbers of Γ-inequivalent elliptic points of order 2, elliptic points of order 3, and cusps, respectively. Then the genus $g(\Gamma)$ of $X(\Gamma)$ is given by the formula

$$g(\Gamma) = 1 + \frac{m}{12} - \frac{v_2}{4} - \frac{v_3}{3} - \frac{v_\infty}{2}.$$

2.3 Modular forms and Modular functions

2.3.1 Definitions

Let $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2^+(\mathbb{R})$. For an integer k and a meromorphic function $f : \mathbb{H} \mapsto \mathbb{C}$ we let the notation $f(\tau)\big|\,[\gamma]_k$ denote the *slash operator*

$$f(\tau)\big|\,[\gamma]_k = (\det\gamma)^{k/2}(c\tau+d)^{-k} f\left(\frac{a\tau+b}{c\tau+d}\right).$$

The factor $c\tau+d$ is called the *automorphy factor*. If the weight k is clear from the context, we often write simply $f\big|_\gamma$.

Definition 2.3.1 Let Γ be a subgroup of $PSL_2(\mathbb{Z})$ of finite index, and k be an even integer. A holomorphic function $f : \mathbb{H} \mapsto \mathbb{C}$ is called a *modular form* of weight k with respect to Γ if

(1) $f(\tau)\big|\,[\gamma]_k = f(\tau)$ for all $\tau \in \mathbb{H}$ and $\gamma \in \Gamma$, that is,

$$f(\tau) = (c\tau+d)^{-k} f\left(\frac{a\tau+b}{c\tau+d}\right).$$

(2) $f(\tau)$ is holomorphic at every cusp.

In addition to (1) and (2), if the function also satisfies

(3) f vanishes at every cusp,

then the function f is a *cusp form* of weight k with respect to Γ.

Let $a/c \in \mathbb{P}^1(\mathbb{Q})$ be a cusp and choose $\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in PSL_2(\mathbb{Z})$. Then a function f satisfies condition (1) if and only if the function $g(\tau) = f\big|\,[\sigma]_k$ is invariant under the action of $\sigma^{-1}\Gamma\sigma$ since

$$\big(f\big|\,[\sigma]\big)\,\big|\,[\sigma^{-1}\gamma\sigma] = \big(f\big|\,[\gamma]\big)\,\big|\,[\sigma] = f\big|\,[\sigma], \text{ for all } \gamma \in \Gamma.$$

In particular, $g(\tau)$ is invariant under the substitution $\tau \mapsto \tau + h$, where h is the width of the cusp a/c. Let $\sum_{n\in\mathbb{Z}} a_n e^{2\pi i n\tau/h}$ be the Fourier expansion of $g(\tau)$. Then we say f is holomorphic at a/c provided that $a_n = 0$ for all $n < 0$, or equivalently, that g is bounded in a neighborhood of a/c. Moreover, condition (3) means that $a_n = 0$ for all $n \le 0$ for each cusp a/c.

Definition 2.3.2 A meromorphic modular form of weight 0 is called a *modular function*. That is a modular function on Γ is a meromorphic function $f : \mathbb{H} \to \mathbb{P}^1(\mathbb{C})$ such that $f(\gamma\tau) = f(\tau)$ for all $\gamma \in \Gamma$.

It is clear that modular functions form a field.

2.3.2 Dedekind eta function $\eta(\tau)$

The Dedekind eta function plays a central role in number theory. It was introduced by Dedekind in 1877 and provides another convenient way of constructing modular forms and modular functions.

Definition 2.3.3 Let $\tau \in \mathbb{H}$, and write $q = e^{2\pi i\tau}$. The *Dedekind eta function* $\eta(\tau)$ is defined by

$$\eta(\tau) = q^{1/24}\prod_{n=1}^{\infty}(1-q^n) = e^{\pi i\tau/12}\prod_{n=1}^{\infty}(1-e^{2\pi in\tau}).$$

Proposition 2.3.4 *For*

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}),$$

the transformation formula for $\eta(\tau)$ is given by, for $c = 0$,

$$\eta(\tau + b) = e^{\pi ib/12}\eta(\tau),$$

and, for $c > 0$,

$$\eta(\gamma\tau) = \epsilon(a,b,c,d)\sqrt{\frac{c\tau+d}{i}}\eta(\tau)$$

with

$$\varepsilon(a,b,c,d) = \begin{cases} \left(\dfrac{d}{c}\right) i^{(1-c)/2} e^{\pi i\left(bd(1-c^2)+c(a+d)\right)/12}, & \text{if } c \text{ is odd,} \\ \left(\dfrac{c}{d}\right) e^{\pi i\left(ac(1-d^2)+d(b-c+3)\right)/12}, & \text{if } d \text{ is odd,} \end{cases} \tag{2.2}$$

where $\left(\dfrac{d}{c}\right)$ is the Legendre-Jacobi symbol.

Proposition 2.3.5 *Let N be a positive integer. If*

$$f(\tau) = \prod_{h|N}\eta(h\tau)^{e_h}$$

satisfies

(1)

$$e = \sum_{h|N} e_h \equiv 0 \mod 4,$$

(2)

$$\prod_{h|N} h^{e_h} \text{ is a square of a rational number,}$$

(3)

$$\sum_{h|N} e_h h \equiv 0 \mod 24,$$

(4)

$$\sum_{h|N} e_h N/h \equiv 0 \mod 24,$$

then $f(\tau)$ is a meromorphic modular form of weight $\frac{1}{2}e$ on $\Gamma_0(N)$.

2.3.3 Generalized eta functions

In this section, what we discuss are refered to the paper [15] *Transformation formulas for generalized Dedekind eta functions* by Y. Yang.

Definition 2.3.6 Let N be a positive integer. For $\tau \in \mathbb{C}$ with $\operatorname{Im}\tau > 0$, we set $q = e^{2\pi i\tau}$. Let g and h be arbitrary real numbers not congruent to 0 modulo N simultaneously. We define the generalized Dedekind eta functions $E_{g,h}(\tau)$ by

$$E_{g,h}(\tau) = q^{B(g/N)/2}\prod_{m=1}^{\infty}\left(1-\zeta^h q^{m-1+g/N}\right)\left(1-\zeta^{-h}q^{m-g/N}\right).$$

Let g be an arbitrary real number not congruent to 0 modulo N. We define the generalized Dedekind eta function $E_g(\tau)$ by

$$E_g(\tau) = q^{NB(g/N)/2}\prod_{m=1}^{\infty}\left(1-q^{(m-1)N+g}\right)\left(1-q^{mN-g}\right).$$

Where $\zeta = e^{2\pi i/N}$ and $B(x) = x^2 - x + 1/6$.

Proposition 2.3.7 *The functions $E_{g,h}$ satisfy*

$$E_{g+N,h} = E_{-g,-h} = -\zeta^{-h}E_{g,h}, \qquad E_{g,h+N} = E_{g,h}. \tag{2.3}$$

Moreover, let $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in PSL_2(\mathbb{Z})$. Then we have, for $c = 0$,

$$E_{g,h}(\tau + b) = e^{\pi i b B(g/N)}E_{g,bg+h}(\tau),$$

and, for $c > 0$,

$$E_{g,h}(\gamma\tau) = \varepsilon(a,b,c,d)e^{\pi i\delta}E_{g',h'}(\tau),$$

where

$$\varepsilon(a,b,c,d) = \begin{cases} e^{\pi i\left(bd(1-c^2)+c(a+d-3)\right)/6}, & \text{if } c \text{ is odd,} \\ -ie^{\pi i\left(ac(1-d^2)+d(b-c+3)\right)/6}, & \text{if } d \text{ is odd,} \end{cases}$$

$$\delta = \frac{g^2ab + 2ghbc + h^2cd}{N^2} - \frac{gb + h(d-1)}{N},$$

and

$$(g'\ h') = (g\ h)\begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Using the fact that

$$N\gamma\tau = \frac{a(N\tau)+bN}{c(N\tau)+d} = \begin{pmatrix} a & bN \\ c & d \end{pmatrix}(N\tau)$$

and the special class of generalized Dedekind eta functions $E_g(\tau) = E_{g,0}(N\tau)$, we have

Proposition 2.3.8 *The functions E_g satisfy*

$$E_{g+N} = E_{-g} = -E_g.$$

Moreover, let $\gamma = \begin{pmatrix} a & b \\ cN & d \end{pmatrix} \in \Gamma_0(N)$. *Then we have, for* $c = 0$,

$$E_g(\tau + b) = e^{\pi i b N B(g/N)} E_g(\tau),$$

and, for $c \neq 0$,

$$E_g(\gamma\tau) = \varepsilon(a, bN, c, d) e^{\pi i (g^2 ab/N - gb)} E_{ag}(\tau),$$

where

$$\varepsilon(a,b,c,d) = \begin{cases} e^{\pi i \left(bd(1-c^2)+c(a+d-3)\right)/6}, & \text{if } c \text{ is odd}, \\ -ie^{\pi i \left(ac(1-d^2)+d(b-c+3)\right)/6}, & \text{if } d \text{ is odd}. \end{cases}$$

Proposition 2.3.9 *Consider the function* $f(\tau) = \prod_g E_g(\tau)^{e_g}$, *where* g *and* e_g *are integers. Suppose that one has*

$$\sum_g e_g \equiv 0 \mod 12, \qquad \sum_g g e_g \equiv 0 \mod 2. \tag{2.4}$$

Then f *is invariant under the action of* $\Gamma(N)$. *Moreover, if, in addition to (2.4), one also has*

$$\sum_g g^2 e_g \equiv 0 \mod 2N. \tag{2.5}$$

Then f *is a modular function on* $\Gamma_1(N)$.

Furthermore, for the cases where N *is a positive odd integer, the conditions (2.4) and (2.5) can be reduced to*

$$\sum_g e_g \equiv 0 \mod 12 \tag{2.6}$$

and

$$\sum_g g^2 e_g \equiv 0 \mod N, \tag{2.7}$$

respectively.

Proposition 2.3.10 *The order of the function* E_g *at a cusp* a/c *with* $\gcd(a, c) = 1$ *is*

$$\frac{1}{2}\gcd(c, N) P_2(ag/\gcd(c, N)),$$

where $P_2(x) = \{x\}^2 - \{x\} + \frac{1}{6}$ *and* $\{x\}$ *denotes the* fractional part *of a real number* x.

Proposition 2.3.11 *Observe that the action of the Atkin-Lehner involution* ω_N *sends the cusps to the cusps that are equivalent to* ∞ *under* $\Gamma_0(N)$. *Then we have*

$$E_{0,g}\left(\frac{-1}{N\tau}\right) = -ie^{\pi i g/N} E_{g,0}(N\tau) = -ie^{\pi i g/N} E_g(\tau).$$

2.4 Petersson Inner Product and Hecke Operators

2.4.1 Petersson inner product

Let Γ be a subgroup of $PSL_2(\mathbb{Z})$ of finite index. The vector space

$$S_k(\Gamma) = \{f : f \text{ is a cusp form of wight k on } \Gamma\}$$

is equipped with an inner product, called the Petersson inner product.

Definition 2.4.1 Let D be a fundamental domain for Γ. Then the *Petersson inner product* of $f, g \in S_k(\Gamma)$ is defined as

$$\langle f, g \rangle_\Gamma = \frac{1}{[PSL_2(\mathbb{Z}) : \Gamma]} \iint_D y^k f(\tau) \overline{g(\tau)} \frac{dxdy}{y^2},$$

where for $\tau \in \mathbb{H}$ we write $\tau = x + iy$.

The Petersson inner product is defined only on $S_k(\Gamma)$ because if f and g are not cusp forms then the integral may not be finite. However, the integral will converge whenever at least one of f and g is a cusp form. We remark that

(1) The hyperbolic measure $dxdy/y^2$ is invariant under the substitution $\tau \mapsto \gamma\tau$ for any $\gamma \in GL_2^+(\mathbb{R})$.

(2) The factor $1/[PSL_2(\mathbb{Z}) : \Gamma]$ is inserted so that the inner product $\langle f, g \rangle$ will remain the same if we consider f and g as modular forms on a smaller subgroup Γ'.

(3) The Petersson inner product is independent of the choice of the fundamental domain D.

2.4.2 Hecke Operators on modular forms on $\Gamma_0(N)$

To define the Hecke operators T_n on $\Gamma_0(N)$ it is necessary to distinguish the cases $\gcd(n, N) = 1$ from the cases $\gcd(n, N) \neq 1$. When n is a positive integer relatively prime to N, we consider the sets

$$\mathcal{M}_n^{(N)} = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{Z}) : ad - bc = n \right\} / \pm 1.$$

When $n = p$ is a prime divisor of N, we consider the set

$$\mathcal{M}_p^{(N)} = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{Z}) : ad - bc = p,\ N|c,\ p|d, \gcd(a, N) = 1 \right\} / \pm 1$$

instead. Then the modular group $\Gamma_0(N)$ acts on $\mathcal{M}_n^{(N)}$ by multiplication from left. We denote the set of orbits (equivalence classes) by $\mathcal{S}_n^{(N)}$.

Proposition 2.4.2 *Let $\sigma \in \Gamma_0(N)$. Then $\phi_\sigma : \mathcal{S}_n^{(N)} \to \mathcal{S}_n^{(N)}$ given by $\phi_\sigma([\gamma]) = [\gamma\sigma]$ is a well-defined permutation on the elements of $\mathcal{S}_n^{(N)}$.*

Proposition 2.4.3 *Let n be a positive integer relatively prime to N. A complete set of representatives of orbits in $\mathcal{S}_n^{(N)}$ is*

$$\left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} : ad = n,\ a > 0,\ b = 0, \ldots, d-1 \right\}.$$

When $n = p$ is a prime divisor of N, a set of representatives of $\mathcal{S}_p^{(N)}$ is

$$\left\{ \begin{pmatrix} 1 & b \\ 0 & p \end{pmatrix} : b = 0, \ldots, p-1 \right\}.$$

Definition 2.4.4 Let k be an even integer and n a positive integer. Write n in the form $mp_1^{e_1}\dots p_r^{e_r}$ such that $\gcd(m,N)=1$ and $p_i|N$ are prime divisors of N. Then the nth Hecke operator T_n on the space of modular forms of weight k is defined by

$$T_n = T_m T_{p_1}^{e_1}\dots T_{p_r}^{e_r},$$

where

$$T_h f = h^{k/2-1}\sum_{[\gamma]\in \mathcal{S}_h^{(N)}} f\Big|\,[\gamma]_k.$$

Proposition 2.4.5 *The Hecke operators T_n are linear transformations on the space of modular forms on $\Gamma_0(N)$. Moreover, if f is a cusp form, then so is $T_n f$.*

Proposition 2.4.6 *For all positive integers m and n with $\gcd(m,n)=1$ we have*

$$T_{mn} = T_m T_n.$$

Furthermore, suppose that m and n are positive integers such that both of them are relatively prime to N. Then we have

$$T_m T_n = \sum_{d|\gcd(m,n)} d^{k-1} T_{mn/d^2} = T_n T_m.$$

In the following contents we will determine the adjoints T_n^* of the Hecke operators T_n with respect to the Petersson inner product. For convenience, throughout this section the notation $\langle\cdot,\cdot\rangle$ without any subscript denotes the inner product on the space of modular forms on $PSL_2(\mathbb{Z})$, while $\langle\cdot,\cdot\rangle_\Gamma$ carries the usual meaning.

Proposition 2.4.7 *Let n be a positive integer relatively prime to N. The Hecke operators T_n are self-adjoint (also called hermitian) with respect to the Petersson inner product. That is, we have*

$$\langle T_n f, g\rangle = \langle f, T_n g\rangle.$$

for all modular forms f and g of weight k on $\Gamma_0(N)$.

Since T_n are self-adjoint, an elementary result in linear algebra asserts that the eigenvalues of T_n are all real.

Proposition 2.4.8 *For all positive integers n with $\gcd(n,N)=1$, the eigenvalues of T_n are all real.*

Now we have a family of self-adjoint linear operators T_n that are commuting with each other on an inner product space. By a well-known theorem in linear algebra, These linear operators T_n are simultaneously diagonalizable. In other words, the vector space has a basis consisting entirely of simultaneous eigenvectors.

Proposition 2.4.9 *There is a decomposition of the vector space $S_k(\Gamma_0(N))$ into a direct sum*

$$S_k(\Gamma_0(N)) = \oplus V_i$$

of orthogonal subspaces V_i such that each V_i is a simultaneous eigenspace for all T_n with $\gcd(n,N)=1$.

Moreover, if f is an eigenform in V_i, then so is $T_p f$ for $p|N$. Therefore, each T_p, $p|N$, stabilizes V_i. However, in general, V_i may not have a basis consisting of simultaneous eigenforms for all T_n. There does not exist a basis whose elements are all simultaneous eigenforms for all T_n. Nevertheless, if $f = \sum_{n=1}^{\infty} c_n q^n$ is a simultaneous eigenforms for all T_n, then f still enjoys the property that $T_n f = c_n f$.

In general, let f be a non-vanishing modular form of weight k on $PSL_2(\mathbb{Z})$.

Definition 2.4.10 If f is a simultaneous eigenform for all Hecke operators T_n on $PSL_2(\mathbb{Z})$, then we say f is a *simultaneous eigenform* or a *Hecke eigenform*. If the Fourier expansion of f has leading coefficient 1, then f is *normalized*.

Proposition 2.4.11 *The space $S_k(PSL_2(\mathbb{Z}))$ of cusp forms of weight k on $PSL_2(\mathbb{Z})$ is spanned by simultaneous eigenforms.*

2.4.3 Properties of Hecke eigenforms

Throughout this section we let k be a positive even integer and d be the dimension of $S_k(PSL_2(\mathbb{Z}))$. We assume that $\{f_1, \ldots, f_d\}$ is a basis of $S_k(PSL_2(\mathbb{Z}))$ consisting of Hecke eigenforms. In this section we will study properties of f_i.

Proposition 2.4.12 *Let f be a Hecke eigenform, and assume that the Fourier expansion of f is $c_1 q + c_2 q^2 + \cdots$. Then $c_1 \neq 0$.*

Recall that we say a Hecke eigenform is normalized if the leading Fourier coefficient is 1, the Fourier coefficients of a normalized Hecke eigenform are multiplicative.

Proposition 2.4.13 *Let f be a normalized Hecke eigenform with a Fourier expansion $q + c_2 q^2 + c_3 q^3 + \cdots$. Then $T_n f = c_n f$ for all positive integers n.*

Proposition 2.4.14 *If f is a normalized Hecke eigenform with a Fourier expansion $q + c_2 q^2 + c_3 q^3 \cdots$, then we have*

$$c_m c_n = \sum_{d|\gcd(m,n)} d^{k-1} c_{mn/d^2}$$

for all positive integers m and n. In particular, if $\gcd(m,n) = 1$, then $c_{mn} = c_m c_n$.

Proposition 2.4.15 *Let $f \neq g$ be two normalized Hecke eigenforms. Then f and g are orthogonal with respect to the Petersson inner product.*

2.4.4 Newforms and oldforms

Some of the cusp forms in $S_k(\Gamma_0(N))$ actually have level smaller than N. Namely, if M is an integer dividing N, then any cusp forms on $\Gamma_0(M)$ is also a cusp form on $\Gamma_0(N)$.

Proposition 2.4.16 *Let M be a positive integer dividing N, and $f(\tau)$ be a cusp form on $\Gamma_0(M)$. Then for any $h|(N/M)$, the function $f(h\tau)$ is a cusp form on $\Gamma_0(N)$. Moreover, if $f(\tau)$ is a simultaneous eigenform for all T_n with $\gcd(n,N) = 1$, then so is $f(h\tau)$.*

Definition 2.4.17 If $f(\tau) \in S_k(\Gamma_0(N))$ satisfies $f(\tau) = g(h\tau)$ for some simultaneous eigenform $g(\tau) \in S_k(\Gamma_0(M))$ with $M|N$, $M < N$, and $h|(N/M)$, then $f(\tau)$ is called an *oldform*. The subspace spanned by all oldforms is called the space of oldforms and is denoted by $S_k^{\text{old}}(\Gamma_0(N))$. The orthogonal complement is called the space of *newforms* and is denoted by $S_k^{\text{new}}(\Gamma_0(N))$.

Proposition 2.4.18 *Each of $S_k^{old}(\Gamma_0(N))$ and $S_k^{new}(\Gamma_0(N))$ is stable under T_n for all n with $\gcd(n, N) = 1$.*

Proposition 2.4.19 *The subspace $S_k^{new}(\Gamma_0(N))$ has a basis consisting of simultaneous eigenforms for all T_n with $\gcd(n, N) = 1$.*

Definition 2.4.20 Let $f \in S_k^{\text{new}}(\Gamma_0(N))$. If f is a non-vanishing simultaneous eigenform for all T_n with $\gcd(n, N) = 1$, then f is a *newform*.

In fact, more about $S_k^{\text{new}}(\Gamma_0(N))$ is true. To facilitate further discussion. Let us recall a result of Atkin and Lehner.

Proposition 2.4.21 (Atkin-Lehner) *Let $f(\tau) = \sum_{n=1}^{\infty} c_n q^n$ be a cusp form on $\Gamma_0(N)$. If there exists a positive integer M such that whenever $\gcd(n, M) = 1$ the coefficient a_n vanishes, then f lies in the space of oldforms.*

Proposition 2.4.22 *Let $f(\tau) = \sum_{n=1}^{\infty} c_n q^n$ be a newform on $\Gamma_0(N)$. Then $c_1 \neq 0$.*

Proposition 2.4.23 *Let $S_k^{new}(\Gamma_0(N)) = \oplus V_i$ be the decomposition of $S_k^{new}(\Gamma_0(N))$ into a direct sum of simultaneous eigenspaces for all T_n with $\gcd(n, N) = 1$. Then each V_i has dimension 1.*

Before we state our last results in this chapter, let us recall that the Atkin-Lehner involutions

$$w_n = \left\{ \frac{1}{\sqrt{n}} \begin{pmatrix} an & b \\ cN & dn \end{pmatrix},\ n|N,\ \gcd(n, N/n) = 1,\ adn^2 - bcN = n \right\},$$

normalize $\Gamma_0(N)$. Thus if f is a modular form of weight k on $\Gamma_0(N)$, then so is $f\big|\,[w_n]_k$. For the ease of notation, given a modular form on $\Gamma_0(N)$, we write

$$W_n f = f\big|\,[w_n].$$

We remark that since $w_n^2 \in \Gamma_0(N)$, the coset $\Gamma_0(N)w_n$ is all the same for a fixed n, regardless of which w_n we choose. Therefore, the definition of W_n does not depend on the representative w_n.

Proposition 2.4.24 *If m is a positive integer such that $\gcd(m, N) = 1$, then $T_m W_n = W_n T_m$.*

Proposition 2.4.25 *The space of newforms is spanned by cusp forms that are simultaneous eigenforms for all Atkin-Lehner involutions and all Hecke operators.*

Remark. Since $w_n^2 \in \Gamma_0(N)$, we have $W_n^2 f = f$. Thus, the eigenvalues of W_n must be 1 or -1.

Finally we study the eigenvalue of T_p, $p|N$, associated with a newform.

Proposition 2.4.26 *Let $f = \sum_{n=1}^{\infty} c_n q^n$ be a normalized newform on $\Gamma_0(N)$. Let p be a prime divisor of N. If $p^2|N$, then $c_p = 0$. If p^2 does not divide N, then $c_p = -\epsilon p^{k/2-1}$, where ϵ is the eigenvalue of W_p associated with f.*

Chapter 3

Elliptic Curves

An *elliptic curve* is a pair (E, O), where E is a smooth projective curve of genus 1 and O is a basepoint of E.

Let K be any perfect field. The elliptic curve (E, O) is said to be defined over K if the curve is defined over K, which is also denoted by E/K, and O is a rational point on E defined over K. Every such curve can be written as the locus in $\mathbb{P}^2$ of a cubic equation with only one point on the line at infinity. That is, after scaling X and Y, as an equation of the form

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3.$$

Here $O = [0, 1, 0]$ and $a_i \in \overline{K}$. And there exists a morphism

$$+ : E \times E \to E \text{ defined by } (P_1, P_2) \mapsto P_1 + P_2$$

giving the group law such that the set of rational points on E with identity O (point at infinity) forms an abelian group.

3.1 Definitions

In this chapter, we consider the special case $K = \mathbb{Q}$.

A cubic curve in normal form looks like

$$y^2 = f(x) = x^3 + ax^2 + bx + c.$$

Assuming that the roots of $f(x)$ are distinct, that is, this curve is nonsingular. Then such a curve is an elliptic curve, and every point on an elliptic curve has a well-defined tangent line. The reason is as follows. If we write the equation as $F(x, y) = y^2 - f(x) = 0$ and take the partial derivatives,

$$\frac{\partial F}{\partial x} = -f'(x), \text{ and } \frac{\partial F}{\partial y} = 2y.$$

We can see that there is no point on the curve at which the partial derivatives vanish simultaneously, since the curve is nonsingular. The details can be found in *Rational Points on Elliptic Curves* by J.H. Silverman [13].

If this curve is singular, we classify the singular points depending on its tangent directions.

Definition 3.1.1 Let P be a singular point on the curve $F(x, y) = 0$. We say that P is a *node* if there are two distinct tangent directions at P. P is a *cusp* if there is one tangent direction at P.

3.1.1 Minimal Weierstrass Equation

We may assume that each elliptic curve have a *Weierstrass equation* of the form

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

And this equation has an associated *discriminant*

$$\begin{aligned}\Delta = &-(a_1^2 + 4a_2)^2(a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2) - 8(2a_4 + a_1a_3)^3 \\ &- 27(a_3^2 + 4a_6)^2 + 9(a_1^2 + 4a_2)(2a_4 + a_1a_3)(a_3^2 + 4a_6).\end{aligned}$$

If we replace the variables (x, y) by $(x/u^2, y/u^3)$, then each a_i in the Weierstrass equation $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ becomes u^ia_i and the discriminant is $u^{12}\Delta$. In this way, we can choose u such that u^ia_i are all integers.

Let E' be a new equation

$$E' : y^2 + b_1xy + b_3y = x^3 + b_2x^2 + b_4x + b_6$$

of this elliptic curve E form changing variables such that b_i are all integers. Let Δ' be the discriminant of E'. For each prime p, define $v_p(\Delta')$ as the power of p such that $p^{v_p(\Delta')} \mid \Delta'$ but $p^k \nmid \Delta'$ if $k > v_p(\Delta')$.

Definition 3.1.2 A Weierstrass equation is called a *minimal Weierstrass equation* E' for E at p if $v_p(\Delta')$ is minimized subject to the condition $b_i \in \mathbb{Z}$.

If we define

$$v_p(\Delta) = \min_{E'} v_p(\Delta'),$$

then the *minimal discriminant* of E is defined by

$$D = \prod_p p^{v_p(\Delta)}.$$

Definition 3.1.3 A Weierstrass equation is called a *global minimal Weierstrass equation* for E if E is simultaneously minimal at all primes of $\mathbb{Q}$. The discriminant Δ of this global minimal Weierstrass equation is equal to the minimal discriminant D of $E/\mathbb{Q}$.

Proposition 3.1.4 ([12], Corollary 8.3) *Every elliptic curve $E/\mathbb{Q}$ has a global minimal Weierstrass equation.*

We remark that we can find a global minimal Weierstrass equation for $E/\mathbb{Q}$ by finding local minimal equations(e.g. by using Tate's algorithm).

3.1.2 Reduction

The *reduction* of E modulo p, denoted $\widetilde{E}$, is then the curve over $\mathbb{Z}_p$ defined by the equation

$$\widetilde{E} : y^2 + \widetilde{a_1}xy + \widetilde{a_3}y = x^3 + \widetilde{a_2}x^2 + \widetilde{a_4}x + \widetilde{a_6},$$

where $\widetilde{a_i}$ denotes reduction modulo p. The curve $\widetilde{E}$ may be singular; its non-singular part is denoted $\widetilde{E}^{ns}$.

Definition 3.1.5 We say that

(1) E has *good (stable) reduction* if $\widetilde{E}$ is non-singular.

(2) E has *multiplicative (semi-stable) reduction* if $\widetilde{E}$ has a node. And the reduction is called *split* if the tangent directions are defined over $\mathbb{Z}_p$, otherwise it is *non-split*.

(3) E has *additive (unstable) reduction* if $\widetilde{E}$ has a cusp.

In cases (2) and (3), E is naturally said to have *bad reduction*.

3.1.3 Conductor

The minimal discriminant is a measure of the bad reduction of E. Another such measure is the *conductor* of $E/\mathbb{Q}$.

Definition 3.1.6 The *conductor* of $E/\mathbb{Q}$ is defined by

$$N(E/\mathbb{Q}) = \prod_p p^{f_p(E/\mathbb{Q})},$$

where the exponents $f_p(E/\mathbb{Q})$ are given by

$$f_p(E/\mathbb{Q}) = \begin{cases} 0, & \text{if } E \text{ has good reduction at } p, \\ 1, & \text{if } E \text{ has multiplicicative reduction at } p, \\ 2+\delta_p, & \text{if } E \text{ has additive reduction at } p, \end{cases}$$

where $\delta_p = 0$ if $p \nmid 6$.

Further, f_p may be computed by using *Ogg's formula*[11].

3.1.4 L-Series

The L-series of an elliptic curve is a generating function which records information about the reduction of the curve modulo every prime.

Let E be an elliptic curve. Set $q = p^k$, for some prime p.

Definition 3.1.7 Let $E(\mathbb{F}_{q^r})$ be the set of points on E with coordinates in $\mathbb{F}_{q^r}$. The *zeta function* of E over $\mathbb{F}_{q^r}$ is given by the formal power series

$$Z(E/\mathbb{F}_q; T) = \exp\left(\sum_{r=1}^{\infty} (\#E(F_{q^r}))\frac{T^r}{r}\right), \text{ where } \exp(u) = \sum_{k=0}^{\infty} \frac{u^k}{k!}.$$

Proposition 3.1.8 *[12] There is an integer a so that*

$$Z(E/\mathbb{F}_q; T) = \frac{1 - aT + qT^2}{(1-T)(1-qT)} = \frac{(1-\alpha T)(1-\beta T)}{(1-T)(1-qT)} \text{ with } |\alpha| = |\beta| = \sqrt{q}.$$

Further more

$$Z(E/\mathbb{F}_q; T) = Z(E/\mathbb{F}_q; 1/(qT)).$$

For each prime p, if E has good reduction at p, let $a_p = p + 1 - \#\widetilde{E}(\mathbb{F}_p)$. The *local factor* of the L-series of E at p is $L_p(T) = 1 - a_pT + pT^2$. We extend the definition of $L_p(T)$ to the case that E has bad reduction by setting

$$L_p(T) = \begin{cases} 1 - T, & \text{if } E \text{ has split multiplicicative reduction at } p, \\ 1 + T, & \text{if } E \text{ has non-split multiplicicative reduction at } p, \\ 1, & \text{if } E \text{ has additive reduction at } p. \end{cases}$$

In all cases, the relation $L_p(1/p) = \#\widetilde{E}(\mathbb{F}_p)/p$ holds.

Definition 3.1.9 We make substitution $T = p^{-s}$ in $Z(E/\mathbb{F}_p; T)$, and define *Hasse-Weil L-series* $L(E, s)$ by

$$L(E, s) = \frac{\zeta(s)\zeta(s-1)}{\Pi_p Z(E/\mathbb{F}_p; p^{-s})},$$

where $\zeta(s)$ is the *Riemann zeta function* defined by

$$\zeta(s) = \sum_{n \in \mathbb{N}} \frac{1}{n^s}, \text{ for } Re(s) > 1$$

and we can express $\zeta(s)$ as

$$\zeta(s) = \prod_{primes\, p} \frac{1}{1 - p^{-s}}.$$

Thus, we have

$$L(E/\mathbb{Q}, s) = \prod_p \frac{1}{1 - a_p p^{-s} + p^{1-2s}} = \prod_p L_p(p^{-s})^{-1}.$$

3.2 Taniyama-Shimura Conjecture

The conjecture says that every rational elliptic curve $y^2 = f(x) = x^3 + ax^2 + bx + c$ is a modular form in disguise.

Proposition 3.2.1 Taniyama-Shimura Conjecture

Let $E/\mathbb{Q}$ be an elliptic curve of conductor N, let $L(E, s) = \sum c_n n^{-s}$ be its Hasse-Weil L-series,and let $f(\tau) = \sum c_n e^{2\pi i n\tau}$ be the inverse Mellin transform of $L(E, s)$.

1. *$f(\tau)$ is a cusp form of weight 2 on $\Gamma_0(N)$, for some positive integer N.*
2. *For each prime $p \nmid N$, let $T(p)$ be the corresponding Hecke operator; and let W be the operator $(Wf)(\tau) = f(-1/N\tau)$. Then*

   $$T(p)f = c_p f \text{ and } Wf = wf,$$

   where $w = \pm 1$ is the sign of the functional equation

   $$\xi_E(s) = w\xi_E(2 - s), \text{ where } \xi_E(s) = (2\pi)^{-s} N^{s/2} \Gamma(s) L(E, s), \text{ for } s \in \mathbb{C},$$

   with the well-know Gamma-function $\Gamma(s)$.
3. *Let ω be an invariant differential on $E/\mathbb{Q}$. There exists a morphism $\phi : X_0(N) \to E$, defined over $\mathbb{Q}$, such that $\phi^*(\omega)$ is a multiple of the differential form on $X_0(N)$ represented by $f(\tau)d\tau$.*

Chapter 4

Modular parameterizations

In this chapter we will obtain modular parameterization of elliptic curves that are modular curves of the form $X_0(p)$ and $X_0^+(p) = X(\Gamma_0^+(p)) = X_0(p)/\omega_p$, where the levels p are primes. In Section 4.1 we will determine all such curves, and then describe methods to obtain parameterizations in Section 4.2. Afterward, we work out several examples to illustrate the procedures. Finally, we will tabulate the results in Section 4.3.

4.1 Genera of $X_0(p)$ and $X_0^+(p)$

First we observe that the genus of an elliptic curve is 1, so we need to find the modular curves $X_0(p)$ and $X_0^+(p)$ of genus 1.

Since $X_0(p)$ is a Riemann surface, from the Riemann Hurwitz's formula, we have

$$g(\Gamma_0(p)) = 1 + \frac{m}{12} - \frac{v_2}{4} - \frac{v_3}{3} - \frac{v_\infty}{2},$$

which is given in section 2.2.3. Using Propositions 2.1.3, 2.2.7, and 2.2.8,

$$g(\Gamma_0(p)) = \begin{cases} \lfloor p/12 \rfloor - 1, & \text{if } p \equiv 1 \bmod 12, \\ \lfloor p/12 \rfloor, & \text{if } p \equiv 5, 7 \bmod 12, \\ \lfloor p/12 \rfloor + 1, & \text{if } p \equiv 11 \bmod 12, \end{cases}$$

the formula becomes simplifier. Hence we can deduce that only when $p = 11$, 17 and 19, the modular curves $X_0(p)$ are of genus 1.

P. Zograf [18] proved that

$$g(\Gamma_0^+(p)) + 1 > 3\chi(\Gamma_0^+(p))/64,$$

where

$$\chi(\Gamma) = \frac{\mathrm{Vol}(\Gamma\backslash\mathbb{H})}{6\mathrm{Vol}(PSL_2(\mathbb{Z})\backslash\mathbb{H})}.$$

For $\Gamma_0^+(p)$, the value of $\chi(\Gamma_0^+(p))$ is $(p+1)/12$. Thus, we only need to determine the genera of $X_0^+(p)$ for $p \leq 511$. To find the genus of $X_0^+(p)$, we use the Fricke's formula that the number of fixed points of the involution ω_p on $\Gamma_0(p)$ is

$$\nu(p) = \begin{cases} h(-4p), & \text{if } p \equiv 1 \bmod 4, \\ h(-4p) + h(-p), & \text{if } p \equiv 3 \bmod 4, \end{cases}$$

where $h(d)$ is the number of

$$\left\{ax^2+bxy+cy^2 \,:\, b^2-4ac=d\right\}/SL_2(\mathbb{Z}).$$

(The general formula for $\Gamma_0^+(N)$ can be seen in [9].) Now the class numbers $h(-p)$ and $h(-4p)$ can be easily computed using Kronecker's class number relations

$$\sum_{n^2<4N} H(4N-n^2)=\sum_{d|N}\max(d,N/d)+\begin{cases}1/6, & \text{if } N \text{ is a square,}\\ 0, & \text{else,}\end{cases}$$

with the initial values $H(1)=H(2)=0$, $H(3)=1/3$. Here $H(d)$ denotes the Hurwitz class number, and is essentially $h(-d)$. In fact, when $d\neq n^2, 3n^2$, we have $H(d)=h(-d)$. Finally the Riemann-Hurwitz formula yields

$$g(\Gamma_0(p))=2(g(\Gamma_0^+(p))-1)+1+\nu(p)/2.$$

From this we deduce that only when $p=37$, 43, 53, 61, 79, 83, 89, 101, and 131, the genus of $g(\Gamma_0^+(p))$ is 1.

4.2 Methods for finding modular parameterizations

In [16] Y. Yang gave a general method of finding defining equations of modular curves of the type $X_0(N)$, $X_1(N)$, and $X(N)$. Here we will first review his method for $X_0(p)$, and then we will refine the method to obtain modular parameterizations for $X_0^+(p)$ that have genus 1. We will also describe an alternative method using the fact that the holomorphic 1-forms on a modular curve are actually cusp forms of weight 2 in disguise.

4.2.1 Equations for $X_0(p)$

In [16], it was shown that for any positive integer N it is always possible to find modular functions X and Y that generate the function field on $X_0(N)$ using the generalized Dedekind eta functions.

To be more explicit, recall the basic fact that the congruence subgroup $\Gamma_1(N)$ is a normal subgroup of $\Gamma_0(N)$. Let Γ be an intermediate subgroup between $\Gamma_0(N)$ and $\Gamma_1(N)$. We have the fact that Γ is a normal subgroup of $\Gamma_0(N)$. Thus, if $f(\tau)$ is a modular function on Γ, then the function

$$\sum_{\gamma\in\Gamma_0(N)/\Gamma} f(\gamma\tau)$$

is modular on $\Gamma_0(N)$. Furthermore, assume that f has only poles at cusps that are equivalent to ∞ under $\Gamma_0(N)$. Assume also that the order of f at ∞ is m, while at the other poles the orders are less than m. Then the above function has exactly one pole of order m at ∞ and is holomorphic at any other point of $X_0(N)$. Thus, the problem of finding generators of the function field on $X_0(N)$ reduces to that of finding modular functions on $\Gamma_1(N)$ that have the required analytic behaviors. In [16], Yang demonstrated a method how one can achieve this using generalized Dedekind eta functions. Here we will work out the case $N=17$ to demonstrate the whole procedure.

First of all, let us set $W_k=E_{4k}/E_{2k}$. The purpose of this setting is to get rid of the factor involving $e^{\pi ib}$ in Proposition 2.3.8. Then any product of W_k will satisfy

condition (2.6) in Proposition 2.3.9 automatically. Thus, if e_k are integers such that $\sum_k k^2 e_k = 0 \bmod 17$, then $\prod_k W_k^{e_k}$ is modular on $\Gamma_1(17)$. Furthermore, it is easy to see that the infinite products defining E_k converge absolutely for any $\tau \in \mathbb{H}$. Thus, the only possible poles or zeroes of E_k are all at cusps. In fact, using Proposition 2.3.10, we see that the poles and zeroes can happen at cusps $k/17$, $17 \nmid k$.

There are eight distinct W_k, $k = 1 \dots 8$. The cusp ∞ of $X_0(17)$ splits into eight inequivalent cusps $k/17$, $k = 1 \dots 8$, in $X_1(17)$. The orders of W_k at these cusps, multiplied by 17, are as follows.

	3/17	8/17	7/17	4/17	5/17	2/17	6/17	1/17
W_3	−7	−12	28	14	−10	−5	−11	3
W_8	−12	28	14	−10	−5	−11	3	−7
W_7	28	14	−10	−5	−11	3	−7	−12
W_4	14	−10	−5	−11	3	−7	−12	28
W_5	−10	−5	−11	3	−7	−12	28	14
W_2	−5	−11	3	−7	−12	28	14	−10
W_6	−11	3	−7	−12	28	14	−10	−5
W_1	3	−7	−12	28	14	−10	−5	−11

We need a function F with a pole of order 2 at infinity and poles of order less than 2 at other cusps equivalent to infinity under $\Gamma_0(17)$, and holomorphic at any other points. To find F is equivalent to solving the integer programming problem

$$\begin{array}{rrrrrrrrl}
-7x_1 & -12x_2 & +28x_3 & +14x_4 & -10x_5 & -5x_6 & -11x_7 & +3x_8 & \geq -17, \\
-12x_1 & +28x_2 & +14x_3 & -10x_4 & -5x_5 & -11x_6 & +3x_7 & -7x_8 & \geq -17, \\
28x_1 & +14x_2 & -10x_3 & -5x_4 & -11x_5 & +3x_6 & -7x_7 & -12x_8 & \geq -17, \\
14x_1 & 10x_2 & -5x_3 & -11x_4 & +3x_5 & -7x_6 & -12x_7 & +28x_8 & \geq -17, \\
-10x_1 & -5x_2 & -11x_3 & +3x_4 & -7x_5 & -12x_6 & +28x_7 & +14x_8 & \geq -17, \\
-5x_1 & -11x_2 & +3x_3 & -7x_4 & -12x_5 & +28x_6 & +14x_7 & -10x_8 & \geq -17, \\
-11x_1 & +3x_2 & -7x_3 & -12x_4 & +28x_5 & +14x_6 & -10x_7 & -5x_8 & \geq -17, \\
3x_1 & -7x_2 & -12x_3 & +28x_4 & +14x_5 & -10x_6 & -5x_7 & -11x_8 & = -34.
\end{array}$$

We find one of the solutions is $(x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8) = (0, 1, 0, 0, 0, 0, 1, 2)$. That is,

$$F = W_8 W_6 W_1^2 = q^{-2} + q^{-1} + 2 + 2q + q^2 + 2q^3 + q^4 + q^5 + q^6 - q^7 + \cdots,$$

where $q = e^{2\pi i \tau}$. Thus, if we choose

$$\begin{aligned}
X &= \sum_{\gamma \in \Gamma_0(17)/\Gamma_1(17)} F|_\gamma \\
&= \sum_{\gamma \in \Gamma_0(17)/\Gamma_1(17)} \left. \frac{E_{10}{E_4}^2}{E_2 E_{16} E_{12}} \right|_\gamma \\
&= -\frac{E_{13}{E_{12}}^2}{E_6 E_{14} E_2} + \frac{E_{12}{E_{15}}^2}{E_{16} E_9 E_{11}} + \frac{E_2{E_{11}}^2}{E_{16} E_{14} E_{10}} - \frac{E_6{E_{16}}^2}{E_8 E_{13} E_{14}} \\
&\quad - \frac{E_{16}{E_3}^2}{E_9 E_{10} E_{12}} - \frac{E_3{E_8}^2}{E_4 E_{15} E_7} + \frac{E_9{E_7}^2}{E_{12} E_{11} E_4} + \frac{E_{10}{E_4}^2}{E_2 E_{16} E_{12}} \\
&= q^{-2} + q^{-1} + 3 + q + 2q^2 + 2q^3 + 3q^4 - 4q^5 + 4q^6 - 2q^7 - q^8 + \cdots,
\end{aligned}$$

then X is modular on $\Gamma_0(17)$ with those properties which we want, where γ runs over a set of coset representatives of $\Gamma_0(17)/\Gamma_1(17)$. Similarly, we can choose a degree 3 function

Y to be

$$\begin{aligned} Y =& \sum_{\gamma\in\Gamma_0(17)/\Gamma_1(17)} \frac{E_{10}{E_6}^3E_8}{E_4E_{14}^3E_{12}}\bigg|_\gamma \\ =& q^{-3}-2q^{-2}-2q^{-1}+8-2q^2-7q^3-2q^4+15q^5-6q^6+\cdots. \end{aligned}$$

Then the functions satisfy

$$Y^2+7XY-31Y=X^3-19X^2+123X-264.$$

Now let

$$\begin{aligned} x =& X-2=\sum_{\gamma\in\Gamma_0(17)/\Gamma_1(17)} \frac{E_{10}{E_4}^2}{E_2E_{16}E_{12}}\bigg|_\gamma-2, \\ y =& Y+3x-9=\sum_{\gamma\in\Gamma_0(17)/\Gamma_1(17)} \frac{E_{10}{E_6}^3E_8}{E_4E_{14}^3E_{12}}\bigg|_\gamma+3x-9. \end{aligned}$$

We have an elliptic curve $y^2+xy+y=x^3-x^2-x-14$, which is a minimal Weierstrass equation. This concludes the demonstration of the case $X_0(17)$. For other two $X_0(p)$ of genus 1, the same method also applies. We list the results in Section 4.3.

4.2.2 Equations for $X_0^+(p)$

For curves $X_0^+(p)$ the basic idea is the same. Since the curves $X_0^+(p)$ are assumed to be of genus one, there are two modular functions x and y on $X_0^+(p)$ such that they have poles only at the cusp ∞ with orders 2 and 3, respectively. Now consider x and y as modular functions on $\Gamma_0(p)$. Since the Atkin-Lehner involutions ω_p on $X_0(p)$ sends the cusps ∞ and 0 to each other, the function x has double poles at cusps ∞ and 0, and the function y has triple poles only at cusps ∞ and 0. Thus, our goal here is to find modular functions that satisfy these requirement. One way to achieve this is as follows.

Suppose that s is a modular function on $\Gamma_0(p)$ such that s has a double pole at ∞, a pole of order less than or equal to 2 at 0, and holomorphic at any other points. Then the function

$$x=s+s|_{\omega_p},$$

considered as a function on $\Gamma_0^+(p)$ will have a pole of order 2 at ∞. Similarly, if t is a modular function on $\Gamma_0(p)$ with a triple pole at ∞, a pole of order less than or equal to 3 at 0, then a possible choice of y is

$$y=t+t|_{\omega_p}.$$

We take $X_0^+(61)$ for example. Now we construct modular functions to parameterize this elliptic curve.

Let Γ be the intermediate subgroup between $\Gamma_1(61)$ and $\Gamma_0(61)$ with $[\Gamma_0(61):\Gamma]=6$. Then Γ is generated by $\Gamma_1(61)$ and $\begin{pmatrix}3 & 2\\ 61 & 41\end{pmatrix}$, and

$$W_k=E_{6k}E_{18k}E_{54k}E_{40k}E_{2k}/E_{3k}E_{9k}E_{27k}E_{20k}E_k$$

is a modular function on Γ for any positive integer k. There are six distinct W_k, and they are W_2, W_4, W_8, W_5, W_{10}, and W_1. Moreover, the cusp ∞ splits into six inequivalent

cusps 2/61, 4/61, 8/61, 5/61, 10/61, and 1/61 in Γ. The orders of W_k at these cusps are as follows.

	2/61	4/61	8/61	5/61	10/61	1/61
W_2	-4	4	-7	13	0	-6
W_4	4	-7	13	0	-6	-4
W_8	-7	13	0	-6	-4	4
W_5	13	0	-6	-4	4	-7
W_{10}	0	-6	-4	4	-7	13
W_1	-6	-4	4	-7	13	0

It follows that

$$\sum_{\gamma\in\Gamma_0(61)/\Gamma}\left.\frac{E_{30}E_{32}E_{26}E_{44}E_{10}}{E_{46}E_{16}E_{48}E_{22}E_{56}}\right|_\gamma$$

is a modular function on $\Gamma_0(61)$ and has a unique pole of order 7 at infinity.

Now we set

$$X(\tau)=\frac{\eta(\tau)^2}{\eta(61\tau)^2}$$

and

$$Y(\tau)=\sum_{\gamma\in\Gamma_0(61)/\Gamma}\left.\frac{E_{30}E_{32}E_{26}E_{44}E_{10}}{E_{46}E_{16}E_{48}E_{22}E_{56}}(\tau)\right|_\gamma+9,$$

where X and Y have pole at infinity of order 5 and 7, respectively. Then we have

$$Y^5-23XY^4+149X^2Y^3-9(X^4+31X^3+61X^2)Y^2+33(X^5+X^4+61X^3)Y=X^3(X^2+X+61)^2,$$

which we takes as the defining equation of $X_0(61)$.

The points ∞ and $(0,0)$ correspond to the cusps ∞ and 0, respectively. This is because if we use the transformation formula for the Dedekind eta function (Proposition 2.3.4), then we get that

$$X(\tau)|_{\omega_{61}}=61\frac{\eta(61\tau)^2}{\eta(\tau)^2}=\frac{61}{X(\tau)} \tag{4.1}$$

and thus $X(0)=0$.

From Proposition 2.3.11, we deduce that

$$Y(\tau)|_{\omega_{61}}=61q^3(1+3q+10q^2+24q^3+57q^4+120q^5+246q^6+\cdots). \tag{4.2}$$

If we consider the Fourier expansions of these functions, then we obtain that the function $Y|_{\omega_{61}}X^2$ has a pole at cusp ∞ of order 7, so we use the function Y to cancel it. Thus, we have

$$Y|_{\omega_{61}}=\frac{61Y}{X^2}. \tag{4.3}$$

To find modular parameterization of $X_0^+(61)$, we need to construct functions s and t with poles only at cusps ∞ and 0 such that s has double poles at cusps ∞ and 0, and t has triple poles at cusps ∞ and 0. According to equations (4.1), (4.2) and (4.3), since the Atkin-Lehner involution ω_{61} sends the cusps ∞ and 0 to each other, we have

$$\begin{aligned}
&\mathrm{div}(X)=-5(\infty)+5(0,0),\\
&\mathrm{div}(Y)=-7(\infty)+3(0,0)+2(\alpha,0)+2(\beta,0),\\
&\mathrm{div}(X|_{\omega_{61}})=5(\infty)-5(0,0),\\
&\mathrm{div}(Y|_{\omega_{61}})=3(\infty)-7(0,0)+2(\alpha,0)+2(\beta,0),
\end{aligned}$$

where $\mathrm{div}(f)$ means the divisor of the function f, and α, β are the roots of $X^2+X+61=0$.

Thus, the function $X_{\omega_{61}}Y = 61Y/X$ has double poles only at ∞ and 0. Using the equations (4.1) and (4.3), we can find that

$$\left.\frac{Y}{X}\right|_{\omega_{61}} = \frac{61Y}{X^2} \times \frac{X}{61} = \frac{Y}{X},$$

that is, Y/X is invariant under Atkin-Lehner involutions.

Also, one has

$$\mathrm{div}(X^2+X+61) = -10(\infty) + 2(\alpha,0) + 2(\beta,0) + \text{ other six simlpe zeros.}$$

Hence the function $(X^2+X+61)/Y$ has triple poles only at ∞ and 0. Similarly, we can show that $(X^2+X+61)/Y$ is invariant under Atkin-Lehner involutions by directly computation.

By setting $s = Y/X$ and $t = (X^2+X+61)/Y$, we have

$$t^2 + 9st - 33t + 270 = s^3 - 23s^2 + 149s,$$

which we takes as the defining equation of $X_0^+(61)$. Let

$$\begin{aligned} x =& s - 1 = \frac{Y}{X} - 1, \\ y =& t + 4x - 12 = \frac{X^2+X+61}{Y} + 4x - 12. \end{aligned}$$

Hence we have modular parameterization of the elliptic curve $y^2 + xy = x^3 - 2x + 1$.

4.2.3 An alternative method for $X_0^+(p)$

In this section we describe an alternative method for finding modular parameterizations of elliptic curves of the type $X_0^+(p)$, where p is one of the primes 37, 43, 53, 61, 79, 83, 89, 101, and 131.

First of all, for such a given modular curves $X_0^+(p)$, there are two pieces of information available to us in the tables of [3] (The tables can be seen in the web site http://modular.fas.harvard.edu/Tables/. [14]). One piece of information is the equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

of the elliptic curve given in Table 1 of [3]. The other is the Fourier expansion

$$q + b_2q^2 + b_3q^3 + \cdots$$

of the unique normalized Hecke eigenform given in Table 3. Now let x be a modular function on $\Gamma_0^+(p)$ with a unique pole of order 2 at infinity with leading coefficient 1 and y be a function with a triple at infinity with leading coefficient 1. We may assume that they satisfy the equation $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$. Furthermore, recall that if Γ is a subgroup of $PSL_2(\mathbb{Z})$ of finite index, there is an isomorphism $\omega = fd\tau$ between two vector spaces $\{f$: meromorphic modular forms of weight 2 on $\Gamma\}$ and $\{\omega$: meromorphic differential 1-forms on $X(\Gamma)\}$. By this one-to-one correspondence, ω is holomorphic on $X(\Gamma)$ if and only if f vanishes at every cusps on $X(\Gamma)$. Thus, if ω is a holomorphic differential 1-form on $X_0^+(p)$, then $\omega/d\tau$ is a cusp form of weight 2 on $X_0^+(p)$,

where τ denotes the standard local parameter of $X_0^+(p)$. Since the holomorphic 1-form of $y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6$ is given by

$$\frac{dx}{2y+a_1x+a_3},$$

we have

$$-\frac{qdx/dq}{2y+a_1x+a_3}=q+\sum_{n=2}^{\infty}b_nq^n.$$

This relation, together with $y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6$, uniquely determine the Fourier expansions of x and y.

Let us take the curve $X_0^+(43)$ for example. According to Table 1 of [3], it has an equation

$$y^2+y=x^3+x^2.$$

Furthermore, from Table 3 of [3], we find that $b_2=-2$, $b_3=-2$, $b_5=-4$, $b_7=0$, $b_{11}=3$, and so on. Using Proposition 2.4.14, we then deduce that the unique normalized Hecke eigenform on $\Gamma_0^+(43)$ has the Fourier expansion

$$q-2q^2-2q^3+2q^4-4q^5+4q^6+q^9+8q^{10}+3q^{11}-4q^{12}+\cdots.$$

Thus, assuming that

$$x=q^{-2}+c_{-1}q^{-1}+c_0+\cdots,\qquad y=q^{-3}+d_{-2}q^{-2}+d_{-1}q^{-1}+\cdots,$$

and solving

$$\begin{cases}\dfrac{-qdx/dq}{2y+1}=q-2q^2-2q^3+2q^4-4q^5+4q^6+q^9+8q^{10}+3q^{11}-4q^{12}+\cdots,\\ y^2+y=x^3+x^2,\end{cases}$$

for the coefficients c_i and d_i, we conclude that

$$x=q^{-2}+2q^{-1}+4+7q+13q^2+20q^3+33q^4+50q^5+77q^6+112q^7+166q^8+\cdots$$

and

$$y=q^{-3}+3q^{-2}+8q^{-1}+16+34q+63q^2+115q^3+197q^4+336q^5+549q^6+885q^7+\cdots.$$

The remaining task is to find a closed form representation for x and y.

Observe that x, considered as a modular function on $\Gamma_0(43)$, has two double poles at ∞ and 0 and holomorphic at any other points. Thus, if f is a modular function with a double zero at 0 and having poles only at ∞, then the function xf has only poles at ∞, and we can express it as a sum of functions having poles only at ∞. We now work out the details in the following computation.

Let Γ be the intermediate subgroup between $\Gamma_1(43)$ and $\Gamma_0(43)$ with $[\Gamma_0(43):\Gamma]=7$, and set

$$X=\sum_{\gamma\in\Gamma_0(43)/\Gamma}\frac{E_{34}E_{32}E_{20}E_{12}E_{14}E_2}{E_{24}E_{28}E_4E_6E_{36}E_{42}}-\frac{E_{26}E_{16}E_{10}E_{12}E_{14}E_2}{E_{36}E_{42}E_6E_{32}E_{20}E_{34}}\bigg|_\gamma-16,$$

$$Y=\sum_{\gamma\in\Gamma_0(43)/\Gamma}\frac{E_{26}E_{16}E_{10}E_{12}E_{14}E_2}{E_{36}E_{42}E_6E_{32}E_{20}E_{34}}\bigg|_\gamma+7,$$

$$Z = \sum_{\gamma \in \Gamma_0(43)/\Gamma} \left. \frac{E_{24}E_{28}E_4}{E_6E_{36}E_{42}} \right|_\gamma - 18,$$

and

$$V = \sum_{\gamma \in \Gamma_0(43)/\Gamma} \left. \frac{E_{22}E_{40}E_{18}E_{26}E_{16}E_{10}E_{12}E_{14}E_2}{E_{32}E_{20}E_{34}E_{30}E_8E_{38}E_6E_{36}E_{42}} \right|_\gamma - 15.$$

The Fourier expansions for them are

$$\begin{aligned} X =& 2q^{-4} + q^{-4} + q^{-2} - 12 + q + 2q^2 + 2q^3 + q^4 + 2q^6 - 2q^7 + 4q^9 + \cdots, && (4.4)\\ Y =& q^{-5} - 2q^{-3} - q^{-2} - 2q^{-1} + 4 + 2q + 2q^3 - 3q^4 - 2q^5 + 2q^7 - q^9 + \cdots, && (4.5)\\ Z =& q^{-6} + q^{-5} + q^{-4} + q^{-2} - 16 + 2q + 3q^2 + 2q^3 + q^4 + 4q^6 + 3q^8 + \cdots, && (4.6) \end{aligned}$$

and

$$V = q^{-7} + q^{-6} + q^{-5} - q^{-4} + 2q^{-1} - 12 + q^2 - 2q^3 + 2q^5 + \cdots. \quad (4.7)$$

Now we consider the behavior of X, Y, Z and V under ω_{43}. We can deduce that

$$\begin{aligned} X|_{\omega_{43}} =& 43(q + 3q^2 + 7q^3 + 16q^4 + 32q^5 + 63q^6 + 117q^7 + \cdots),\\ Y|_{\omega_{43}} =& 43(q^2 + 4q^3 + 12q^4 + 31q^5 + 71q^6 + 154q^7 + 314q^8 + \cdots),\\ Z|_{\omega_{43}} =& 43(2q + 8q^2 + 24q^3 + 65q^4 + 159q^5 + 366q^6 + 794q^7 + 1654q^8 + \cdots), \end{aligned}$$

and

$$V|_{\omega_{43}} = 43(3q + 13q^2 + 47q^3 + 141q^4 + 385q^5 + 963q^6 + 2270q^7 + 5074q^8 + \cdots).$$

Thus, the modular function X has pole of order 4 at cusp ∞ and zero of order 1 at cusp 0, the modular function Y has pole of order 5 at cusp ∞ and zero of order 2 at cusp 0, the modular function Z has pole of order 6 at cusp ∞ and zero of order 1 at cusp 0, and the modular function V has pole of order 7 at cusp ∞ and zero of order 1 at cusp 0 on $\Gamma_0(43)$. It follows that the function

$$xY = q^{-7} + 2q^{-6} + 2q^{-5} + 2q^{-4} + q^{-3} + 2q^{-2} + 2q^{-1} + 3 + 3q + 6q^2 + \cdots,$$

has only a pole at ∞, and thus can be represented as a linear sum of X, Y, Z, and V. To be precise, we use the function V to cancel the pole of order 7 at cusp ∞. Then we have

$$xY - V = q^{-6} + q^{-5} + 3q^{-4} + q^{-3} + 2q^{-2} + 15 + 3q + 5q^2 + 4q^3 + 2q^4 + 6q^6 - 2q^7 + 3q^8 + \cdots,$$

which is a function with pole at cusp ∞ of order 6. We then use Z, Y, and X to cancel q^{-6}, q^{-5}, and q^{-4} sequentially. We arrive at

$$x = (X + V + Z + 43)/Y.$$

By a similar procedure, we find that

$$y = (2Zx - Vx + Z + 2V + Y - 2X)/(3Y - Z + 2X).$$

Hence we have modular parameterization of the rational elliptic curve $y^2 + y = x^3 + x^2$.

For the other $X_0^+(p)$ of genus 1, these two methods also apply. We list the results in Section 4.3.

4.3 Results

N	Functions	Elliptic Curve
11	$x=\sum_5 \frac{E_2{E_4}^2}{{E_{10}}^3}, y=\sum_5 \frac{{E_5}^4}{{E_1}^3E_3}+1$	$y^2+y=x^3-x^2-10x-20$
17	$x=\sum_8 \frac{E_{10}{E_4}^2}{E_2E_{16}E_{12}}-2, y=\sum_8 \frac{E_{10}{E_6}^3E_8}{E_4E_{14}^3E_{12}}+3x-9$	$y^2+xy+y=x^3-x^2-x-14$
19	$x=\sum_9 \frac{E_{12}E_8}{E_{18}E_6}-3, y=\sum_9 \frac{{E_6}^2E_8}{E_2{E_{16}}^2}+x-6$	$y^2+y=x^3+x^2-9x-15$
37	$X=\frac{\eta(\tau)^2}{\eta(37\tau)^2}, Y=\sum_6 \frac{E_6E_8E_{14}}{E_3E_4E_7}-11$ $x=\frac{-47X^2+X^3+6Y^2-7XY+185Y+222X}{X(Y+185)}$ $y=37/X+X+5x-7$	$y^2+y=x^3-x$
43	$X=\sum_7 \frac{E_{34}E_{32}E_{20}E_{12}E_{14}E_2}{E_{24}E_{28}E_4E_6E_{36}E_{42}}-9-Y$ $Y=\sum_7 \frac{E_{26}E_{16}E_{10}E_{12}E_{14}E_2}{E_{36}E_{42}E_6E_{32}E_{20}E_{34}}+7$ $Z=\sum_7 \frac{E_{24}E_{28}E_4}{E_6E_{36}E_{42}}-18$ $V=\sum_7 \frac{E_{22}E_{40}E_{18}E_{26}E_{16}E_{10}E_{12}E_{14}E_2}{E_{32}E_{20}E_{34}E_{30}E_8E_{38}E_6E_{36}E_{42}}-15$ $x=(X+V+Z+43)/Y,$ $y=\frac{2Zx-Vx+Z+2V+Y-2X}{3Y-Z+2X}$	$y^2+y=x^3+x^2$
53	$X=\sum_{13} \frac{E_{24}E_{22}E_{36}E_{20}}{E_{12}E_{42}E_{18}E_{10}}-4,$ $Y=\sum_{13} \frac{E_{14}E_4E_{24}E_{22}}{E_{46}E_2E_{12}E_{42}}, Z=\sum_{13} \frac{E_{24}E_{22}}{E_{16}E_{50}}-16$ $x=\frac{3Y(Y-53)+5Z(Z-53)+2173}{(53+3X)X}$ $+\frac{-9Y+29X-25Z+547}{53+3X}$ $y=\frac{(x-7)Z+(x-3)Y+37}{X}+10-3x$	$y^2+xy+y=x^3-x^2$
61	$X=\frac{\eta(\tau)^2}{\eta(61\tau)^2}, Y=\sum_6 \frac{E_{30}E_{32}E_{26}E_{44}E_{10}}{E_{46}E_{16}E_{48}E_{22}E_{56}}+9$ $x=\frac{Y}{X}-1, y=\frac{X^2+X+61}{Y}+4x-12$	$y^2+xy=x^3-2x+1$

N	Functions	Elliptic Curve
79	$X_9 = \sum_{13} \frac{E_{54}E_{22}E_{32}}{E_{24}E_{56}E_{78}} - 16$ $X_{10} = \sum_{13} \frac{E_{42}E_{60}E_{18}E_{56}E_{78}E_{24}}{E_{72}E_{10}E_{76}E_{34}E_{26}E_8} - 24$ $X_{12} = \sum_{13} \frac{E_{54}E_{22}E_{32}}{E_{62}E_{66}E_4} - 20$ $X_{13} = \sum_{3} \frac{E_{54}E_{36}E_{24}E_{16}E_{42}E_{28}E_{34}E_{30}E_{20}E_{66}E_{44}E_{76}E_2}{E_{52}E_{18}E_{12}E_8E_{58}E_{14}E_{62}E_{64}E_{10}E_{46}E_{22}E_{38}E_{78}} - 7$ $X_{15} = \sum_{3} \frac{E_{54}E_{36}E_{24}E_{16}E_{42}E_{28}E_{34}E_{30}E_{20}E_{66}E_{44}E_{76}E_2}{E_{50}E_{72}E_{48}E_{32}E_{74}E_{56}E_{68}E_{60}E_{40}E_{26}E_{70}E_6E_4} - 10$ $x = \frac{X_{15} + X_{13} + X_{12} - 2X_{10} + X_9}{X_{13} - 2X_{12} + X_{10}}$ $y = \frac{X_{13} - X_{10} + X_9}{X_{10} - X_9} - x$	$y^2 + xy + y = x^3 + x^2 - 2x$

N	Functions	Elliptic Curve
83	$X_{19} = \sum_{41} \frac{E_{38}E_{10}E_{70}E_{62}E_{56}E_{40}E_{24}E_{66}E_{18}}{E_{76}E_{78}E_{48}E_{20}E_4E_{50}E_{74}E_6E_{26}} - 215$ $Y_{19} = \sum_{41} \frac{E_{38}E_{46}E_{20}E_{30}E_{82}E_{28}E_{66}E_{18}E_{12}}{E_{76}E_{78}E_{48}E_{60}E_{80}E_{68}E_4E_{50}E_{74}} - 37$ $X_{20} = \sum_{41} \frac{E_{46}E_{20}E_{42}E_{16}E_{28}E_{66}E_{18}E_{12}E_{52}}{E_{60}E_{10}E_{80}E_{62}E_4E_{14}E_{50}E_{74}E_{26}} - 111$ $Y_{20} = \sum_{41} \frac{E_{38}E_{46}E_{20}E_{30}E_{82}E_{16}E_{28}E_{66}E_{18}E_{12}E_{52}}{E_{64}E_{76}E_{78}E_{48}E_{60}E_{80}E_{62}E_{68}E_4E_{50}E_{74}} - 400$ $Z_{20} = \sum_{41} \frac{E_{48}E_{44}E_{22}E_{40}E_{74}E_4E_{16}E_{52}}{E_{46}E_{10}E_{80}E_{62}E_{14}E_{70}E_{72}E_2} + 12$ $U_{20} = \sum_{41} \frac{E_{48}E_{44}{E_{64}}^2E_{62}E_{40}}{E_{16}E_{80}E_{14}E_{52}E_{10}E_{70}} + 13$ $V_{20} = \sum_{41} \frac{E_{38}E_{48}E_{58}E_{68}E_{44}E_{22}E_{40}E_{74}E_4E_{16}E_{52}}{E_{64}E_{76}E_{78}E_{54}E_{34}E_{24}E_{46}E_{80}E_{62}E_{72}E_2} - 208$ $T_{20} = \sum_{41} \frac{E_{38}E_{64}E_{44}E_{62}E_{40}E_{30}E_{26}E_{82}}{E_{76}E_{78}E_{70}E_{68}E_{16}E_{52}E_{80}E_{42}} + 79$ $X_{21} = \sum_{41} \frac{E_{38}E_{44}E_{46}E_{20}E_{72}E_2E_{16}E_{28}E_{12}E_{52}}{E_{64}E_{76}E_{78}E_{24}E_{56}E_{22}E_{80}E_{62}E_4E_{74}} + 27$ $Y_{21} = \sum_{41} \frac{E_{38}E_{14}E_{70}E_{54}E_{34}E_{36}E_{44}E_{46}E_{20}E_6E_{42}}{E_{64}E_{76}E_{78}E_{48}E_{56}E_{66}E_{18}E_{22}E_{60}E_{80}E_{62}} - 508$ $Z_{21} = \sum_{41} \frac{E_{38}E_{54}E_{34}E_{44}E_{20}E_{28}E_{12}}{E_{76}E_{78}E_{48}E_{56}E_{80}E_{68}E_{58}} + 86$ $V_{21} = \sum_{41} \frac{E_{48}E_{44}E_{64}E_{40}}{E_{80}E_{14}E_{10}E_{70}} - 12$ $U_{21} = \sum_{41} \frac{E_{38}E_{44}E_{40}E_{30}E_{26}E_{82}}{E_{76}E_{78}E_{70}E_{68}E_{80}E_{42}} + 42$ $T_{21} = \sum_{41} \frac{E_{38}E_{64}E_{44}E_{22}E_{62}E_{40}E_{74}E_4}{E_{76}E_{78}E_{16}E_{52}E_{46}E_{80}E_{72}E_2} - 162$ $X_{22} = \sum_{41} \frac{E_{54}E_{34}E_{44}E_{20}E_{42}E_{16}E_{28}E_{12}E_{52}}{E_{56}E10E_{80}E_{62}E_{58}E_{30}E_{82}E_{14}E_{26}} - 240$ $Y_{22} = \sum_{41} \frac{E_{54}E_{34}E_{44}E_{20}E_{38}E_{16}E_{28}E_{12}E_{52}}{E_{64}E76E_{78}E_{48}E_{56}E_{80}E_{62}E_{68}E_{58}} - 405$ $Z_{22} = \sum_{41} \frac{E_{48}E_{44}E_{40}E_{16}E_{52}}{E_{10}E80E_{62}E_{14}E_{70}} - 40$ $U_{22} = \sum_{41} \frac{E_{38}E_{44}E_{22}E_{40}E_{74}E_4}{E_{76}E_{78}E_{46}E_{80}E_{72}E_2} - 125$ $V_{22} = \sum_{41} \frac{{E_{64}}^2{E_{62}}^2E_{38}E_{44}E_{40}}{{E_{52}}^2{E_{16}}^2E_{76}E_{78}E_{80}} - 585$	$y^2 + xy + y = x^3 + x^2 + x$

N	Functions	Elliptic Curve
83	$X_{18} = T_{20} - X_{20}$ $X_{17} = X_{20} - U_{20}$ $X_{16} = Y_{20} - Z_{20} + Y_{19} + X_{18} - X_{17}$ $Y_{16} = V_{22} - X_{22} - X_{18} - X_{17}$ $X_{15} = X_{20} - Z_{20} + X_{19} + 2X_{18} + 3X_{16}$ $Y_{15} = X_{20} - V_{20} + Y_{19} + 2X_{18} + 2X_{17} + 3X_{16}$ $X_{14} = Z_{21} - U_{21} + X_{20} + 2Y_{19} + 2X_{18} + 2X_{17} + 2X_{16}$ $Y_{14} = Z_{21} - Y_{21} - 2U_{21} + 2T_{21} + 2X_{20} + X_{19} + 3X_{18} + 2X_{17} + Y_{16}$ $Z_{14} = (X_{15} - Y_{15})/2$ $Y_{13} = (V_{21} - Z_{21} - Y_{19} - X_{17} + X_{16} - X_{15} + 3X_{14})/21$ $R_{13} = Y_{22} - V_{22} + 2U_{22} - 2Z_{22} + X_{21} - 3X_{20} - X_{19} - 2X_{18} - X_{16} + 2X_{15} - Y_{15} - X_{14} - Y_{14} - 4Z_{14}$ $T_{13} = (V_{21} - Z_{21} - Y_{19} - X_{17} + X_{16} - Y_{15} + X_{14})/2$ $U_{13} = 4Y_{15} - 4X_{15} + 3X_{14} + 5Y_{14}$ $Y_{12} = 3(Z_{21} - X_{21} + X_{20} + X_{19} - X_{18} + 2X_{17} - 8X_{16} + 7X_{15} - 34X_{14} + 301Y_{13}) - R_{13} + T_{13}$ $Z_{12} = 4X_{22} - 2U_{22} - 2V_{22} - 2X_{21} + 3Y_{20} + 2X_{20} - 3U_{20} - 4X_{19} + X_{18} - 12X_{17} - X_{16} - 5X_{15} + 58Z_{14} - 22R_{13}$ $V_{12} = 21(X_{21} - Z_{21} - X_{20} - X_{19} + X_{18} - 2X_{17} + 8X_{16} - 7X_{15} + 34X_{14} - 301Y_{13})/2 + R_{13} - V_{13}$ $X_{11} = 10X_{15} - 10Y_{15} - 3X_{14} - 17Y_{14} - 65T_{13} + Z_{12} + 3Y_{12}$ $Z_{11} = (X_{15} - Y_{15} - 2Y_{14} - 11T_{13} - 17Y_{12})/4$ $X_{10} = (2U_{22} - Y_{22} - Z_{22} - X_{20} - X_{18} - X_{17} + 2X_{16} - 4X_{15} + 24X_{14} - 210Y_{13})/25$ $Y_9 = (5X_{21} - 11U_{21} + 6T_{21} - X_{19} + 7X_{18} - 4X_{17} + 20X_{16} - 59X_{15} + 52Y_{15} + 17X_{14} + 98Y_{14} + 5R_{13} + 393T_{13} - U_{13} + 290Y_{12} - 77/2X_{11} + 48035/2X_{10})/48$ $R_9 = (2T_{13} - 2R_{13} - 2V_{12} - 18Y_{12} + X_{11} - Z_{11} - 2157/4X_{10})/4$ $X_8 = 5(R_9 - Y_9)/313$ $x = \frac{-Y_{19} - 2X_{18} + 2X_{17} - 6X_{16} + 11X_{15} - 62Z_{14} - 39T_{13}}{X_{16} - X_{17}} \frac{-464Y_{12} - 391/2X_{11}15131/2X_{10} + 109580R_9}{X_{16} - X_{17}} \frac{-15055231/10X_8 + 498}{X_{16} - X_{17}}$ $y = \frac{4X_{19} + 2X_{18} + 6X_{17} + 3X_{16} + 84X_{15} - 472Z_{14}}{3X_{16} - 2X_{15}} \frac{-496R_{13} + 181(V_{12} - Z_{12}) - 9240Y_{12} - 326X_{11}}{3X_{16} - 2X_{15}} \frac{-937109/2X_{10} + 739424R_9 - 20418507/2X_8}{3X_{16} - 2X_{15}} \frac{-x(X_{17} + 4X_{15} + 1826) + 10292}{3X_{16} - 2X_{15}}$	$y^2 + xy + y = x^3 + x^2 + x$

N	Functions	Elliptic Curve
89	$X_{11} = \sum_{12} \frac{E_{26}E_6E_{46}E_{38}}{E_{76}E_{86}E_{66}E_{70}} + 4,$ $Y_{11} = \sum_{12} \frac{E_{26}E_6E_{32}E_{20}}{E_{76}E_{86}E_{78}E_{18}} - 32,$ $X_{12} = \sum_{12} \frac{E_{24}E_{74}E_{46}E_{38}E_{42}E_4}{E_8E_{84}E_{52}E_{12}E_{66}E_{70}} - 1$ $X_{13} = \sum_{11} \frac{E_{28}E_{32}E_{62}E_{20}}{E_{74}E_{68}E_{24}E_2} - 4$ $X_{14} = \sum_{11} \frac{E_{44}E_{26}E_{72}E_6E_{28}E_{32}E_{62}E_{20}}{E_{22}E_{76}E_{36}E_{86}E_{14}E_{16}E_{58}E_{10}} - 32$ $x = (X_{13} + X_{12})/X_{11}$ $y = (X_{14} + X_{13} + X_{12} + 2Y_{11} + 89)/X_{11} - 1$	$y^2 + xy + y = x^3 + x^2 - x$

N	Functions	Elliptic Curve
101	$X_{14} = \sum_{10} \frac{E_{40}E_{46}E_{38}E_{74}E_{26}}{E_{20}E_{78}E_{82}E_{64}E_{88}} - 17$ $X_{15} = \sum_{10} \frac{E_{62}E_{60}E_{32}E_{44}E_{10}E_{28}E_{12}E_{34}E_{72}E_{2}}{E_{56}E_{24}E_{68}E_{58}E_{4}E_{14}E_{6}E_{84}E_{36}E_{100}} - 41$ $Y_{15} = \sum_{10} \frac{E_{90}E_{48}E_{66}E_{86}E_{8}E_{40}E_{46}E_{38}E_{74}E_{26}}{E_{28}E_{12}E_{34}E_{72}E_{2}E_{78}E_{82}E_{64}E_{88}E_{20}} - 36$ $X_{16} = \sum_{10} \frac{E_{22}E_{96}E_{70}E_{30}E_{16}E_{62}E_{60}E_{32}E_{44}E_{10}}{E_{28}E_{12}E_{34}E_{72}E_{2}E_{42}E_{18}E_{50}E_{94}E_{98}}$ $\frac{E_{40}E_{46}E_{38}E_{74}E_{26}E_{84}E_{36}E_{100}E_{14}E_{6}}{{E_{78}}^2{E_{82}}^2{E_{64}}^2{E_{88}}^2{E_{20}}^2} + 41$ $Z_{17} = \sum_{10} \frac{E_{56}E_{24}E_{68}E_{58}E_{4}E_{62}E_{60}E_{32}E_{44}E_{10}}{E_{28}E_{12}E_{34}E_{72}E_{2}E_{70}E_{30}E_{16}E_{22}E_{96}}$ $\frac{E_{50}E_{94}E_{98}E_{42}E_{18}}{E_{20}E_{78}E_{82}E_{64}E_{88}} - 1$ $V_{17} = \sum_{10} \frac{E_{62}E_{60}E_{32}E_{44}E_{10}E_{78}E_{82}E_{64}E_{88}E_{20}}{E_{28}E_{12}E_{34}E_{72}E_{2}E_{90}E_{48}E_{66}E_{86}E_{8}} + 14$ $Y_{18} = \sum_{10} \frac{E_{40}E_{46}E_{38}E_{74}E_{26}}{E_{28}E_{12}E_{34}E_{72}E_{2}} - 133$ $Z_{18} = \sum_{10} \frac{E_{56}E_{24}E_{68}E_{58}E_{4}E_{62}E_{60}E_{32}E_{44}E_{10}}{E_{70}E_{30}E_{16}E_{22}E_{96}E_{20}E_{78}E_{82}E_{64}E_{88}} - 14$ $V_{18} = \sum_{10} \frac{E_{56}E_{24}E_{68}E_{58}E_{4}E_{22}E_{96}E_{70}E_{30}E_{16}}{E_{28}E_{12}E_{34}E_{72}E_{2}E_{90}E_{48}E_{66}E_{86}E_{8}}$ $\frac{E_{40}E_{46}E_{38}E_{74}E_{26}}{E_{76}E_{54}E_{52}E_{80}E_{92}} + 17$ $X_{13} = \sum_{10} \frac{E_{40}E_{46}E_{38}E_{74}E_{26}}{E_{70}E_{30}E_{16}E_{22}E_{96}} \frac{E_{40}E_{46}E_{38}E_{74}E_{26}}{E_{90}E_{48}E_{18}E_{66}E_{8}}$ $+ X_{14} + 24$ $X_{12} = X_{15} - Y_{15} + 2X_{14}$ $X_{11} = Z_{17} - V_{17} - X_{16} - 2X_{15} + 4X_{14} - 5X_{13}$ $X_{10} = (V_{18} - Y_{18} + Z_{17} - X_{16} + X_{15} + 3X_{14} - X_{13}$ $+ 2X_{12} + X_{11})/6$ $X_9 = (V_{18} - Z_{18} + V_{17} - X_{16} + X_{15} - X_{14} + 3X_{13}$ $- X_{12} - 5X_{11} - 33X_{10})/18$ $x = \frac{X_{15} - X_{12} - X_{14} - X_{11} - 3X_{10}}{X_{13}} + 2$ $y = \frac{3X_{12} + X_{16} + X_{15} + 101 + 6X_{11} + 39X_{10} + 27X_9}{X_{13}} + 1$	$y^2 + y = x^3 + x^2 - x - 1$

N	Functions	Elliptic Curve
131	$X_{18} = \sum_{13} \frac{E_{18}E_{50}E_{94}E_{30}E_4E_{68}E_{44}E_{64}E_{26}E_{14}E_{104}E_{56}E_{10}E_{86}}{E_{122}E_{106}E_{84}E_{116}E_2E_{52}E_{28}E_{126}E_{88}E_{128}E_{102}E_{66}E_{96}E_{92}}$ $\frac{E_6}{E_{110}} - 33$ $X_{20} = \sum_{5} \frac{E_{52}E_{92}E_{62}E_{112}E_{84}E_{68}E_{80}E_{60}E_{86}E_{130}E_{32}E_{24}E_{18}}{E_{96}E_{72}E_{54}E_{106}E_{14}E_{76}E_{74}E_{10}E_{58}E_{22}E_{82}E_4E_{128}} - 79$ $Y_{20} = \sum_{13} \frac{E_{58}E_{130}E_{70}E_{78}E_{42}}{E_{22}E_{34}E_{32}E_{118}E_{124}} - 44$ $Z_{20} = \sum_{13} \frac{E_{36}E_{100}E_{74}E_{60}E_{96}E_8E_{92}E_{110}E_{102}E_{66}}{E_{16}E_{72}E_{62}E_{114}E_{120}E_{54}E_{112}E_{20}E_{90}E_{12}} - 50$ $X_{24} = \sum_{13} \frac{E_{36}E_{100}E_{74}E_{60}E_{68}E_{44}E_{64}E_{26}E_8E_{14}E_{104}E_{56}E_{10}E_{86}}{E_{32}E_{118}E_{124}E_{34}E_{22}E_{126}E_{88}E_{52}E_{28}E_{108}E_{38}E_{40}E_{82}E_{24}}$ $\frac{E_6}{E_{128}} - 87$ $Y_{24} = \sum_{13} \frac{E_{36}E_{100}E_{74}E_8E_{60}}{E_{122}E_{106}E_{84}E_{116}E_2} - 50$ $Z_{24} = \sum_{13} \frac{E_{18}E_{50}E_{94}E_{30}E_4E_{102}E_{66}E_{96}E_{92}E_{110}}{E_{122}E_{106}E_{84}E_{116}E_2E_{54}E_{112}E_{20}E_{90}E_{12}} + 21$ $V_{24} = \sum_{13} \frac{E_{108}E_{38}E_{40}E_{82}E_{24}E_{58}E_{130}E_{70}E_{78}E_{42}}{E_{122}E_{106}E_{84}E_{116}E_2E_{68}E_{44}E_{64}E_{26}E_{14}} - 28$ $R_{24} = \sum_{13} \frac{E_{36}E_{100}E_{74}E_{60}E_8E_{102}E_{66}E_{96}E_{92}E_{110}E_{58}E_{130}E_{70}E_{78}}{E_{106}E_{84}E_2E_{112}E_{20}E_{90}E_{12}E_{76}E_{122}E_{116}E_{54}E_{80}E_{98}E_{48}}$ $\frac{E_{42}}{E_{46}} - 116$ $Q_{24} = \sum_{13} \frac{E_{54}E_{112}E_{20}E_{90}E_{12}E_{76}E_{80}E_{98}E_{48}E_{46}}{E_{18}E_{50}E_{94}E_4E_{72}E_{30}E_{62}E_{114}E_{120}E_{16}} - 23$ $X_{25} = \sum_{13} \frac{E_{68}E_{44}E_{64}E_{26}E_{14}E_{104}E_{56}E_{10}E_{86}E_6}{E_{32}E_{118}E_{124}E_{34}E_{22}E_{126}E_{88}E_{128}E_{52}E_{28}} - 50$ $Y_{25} = \sum_{13} \frac{E_{122}E_{106}E_{84}E_{116}E_{68}E_{44}E_{64}E_{26}E_{14}E_{108}E_{38}E_{40}E_{24}}{E_{32}E_{118}E_{124}E_{34}E_{22}E_{126}E_{88}E_{128}E_{52}E_{28}E_{18}E_{50}E_{94}}$ $\frac{E_{82}E_2}{E_{30}E_4} - 28$ $R_{25} = \sum_{13} \frac{E_{108}E_{38}E_{40}E_{82}E_{24}}{E_{122}E_{106}E_{84}E_{116}E_2} - 98$ $T_{25} = \sum_{13} \frac{E_{18}E_{50}E_{94}E_{30}E_4E_{68}E_{44}E_{64}E_{26}E_{14}}{E_{122}E_{106}E_{84}E_{116}E_2E_{54}E_{112}E_{20}E_{90}E_{12}} - 125$ $X_{21} = X_{24} - V_{24}$ $X_{22} = V_{24} - T_{24}$ $X_{23} = Z_{24} - X_{24}$ $X_{19} = Z_{20} - X_{20}$ $X_{17} = X_{20} - Y_{20} - X_{18}$ $X_{16} = X_{24} - Q_{24} + X_{23} - X_{22} + X_{19} + 4X_{18} + X_{17}$ $X_{15} = Q_{24} - Y_{24} + X_{20} + X_{19} + X_{18} - 2X_{16}$ $X_{14} = (Y_{16} - X_{16} - 2X_{15})/6$ $X_{13} = 3(Y_{25} - R_{25} + 2X_{24} + 4X_{23} - 3X_{22} + X_{21} + 3X_{20}$ $+ 9X_{19} + 16X_{18} + 8X_{17} - 3X_{16} + 7X_{15} + 31X_{14})/5$	$y^2 + y = x^3 - x^2 + x$

N	Functions	Elliptic Curve
131	$x = \frac{3X_{25} - 3T_{25} + 3X_{23} + 6X_{20} + 18X_{19} + 18X_{18} + 21X_{17}}{3(Z20 - X18)} \frac{+6X_{16} + 27X_{15} + 102X_{14} - 5X_{13}}{3(Z20 - X18)}$ $y = \frac{8R_{25} - 3Y_{25} - 5T_{25} + 2X_{24} - 2Y_{24} - 12Q_{24} + R_{24} - 4X_{23}}{X_{18} + Y_{20} - X_{20}} \frac{-8X_{21} + 6X_{20} - 2Y_{20} - 3Z_{20} - 5X_{18}}{X_{18} + Y_{20} - X_{20}}$	$y^2 + y = x^3 - x^2 + x$

Bibliography

[1] T.M. Apostol, 1976. *Modular Functions and Dirichlet Series in Number Theory*, Spring-Verlag.

[2] G. Cornell, J.H. Silverman and Glenn Stevens, 1997. *Modular Forms and Fermat's Last Theorem*, Spring-Verlag.

[3] J. E. Cremona, 2002. *Algorithms for modular elliptic curves*, Cambridge University Press, Cambridge.

http://www.maths.nott.ac.uk/personal/jec/book/fulltext/index.html

[4] W. Fulton, 1969. *Algebraic curves*, Advanced Book Classics. Addison-Wesley Publishing Company Advanced Book Program, Redwood City, CA, 1989. An introduction to algebraic geometry, Notes written with the collaboration of Richard Weiss, Reprint of 1969 original.

[5] R. Hartshorne, 1977. *Algebraic geometry*, Springer-Verlag, New York, 1977. Graduate Texts in Math, No. 52.

[6] N. Ishida, 1998. *Generators and equations for modular function fields of principal congruence subgroups*, Acta Arith. 85 (3) (1998), 197-207.

[7] N. Ishida and N. Ishii, 2002. *Generators and defining equation of the modular function field of the group* $\Gamma_1(N)$, Acta Arith. 101 (4) (2002), 303-320.

[8] N. Koblitz, 1984. *Introduction to Elliptic Curves and Modular Forms*, Springer-Verlag.

[9] P. G. Kluit, 1976. *On the normalizer of* $\Gamma_0(N)$, Modualr function of one variable, V (Proc. Second Internat. Conf. Univ. Bonn. Bonn., 1976), Lecture Notes in Math., Vol.601. Springer, Berlin, (1977), 239-246.

[10] T. Miyake, 1989. *Modular Forms*, Springer-Verlag.

[11] A.Ogg, 1967. *Elliptic curves and wild ramification*, Am. J. of Math. 89 (1967), 1-21.

[12] J.H. Silverman, 1986. *The Arithmetic of Elliptic Curves*, Spring-Verlag, Graduate Texts in Math.

[13] J.H. Silverman, 1992. *Rational Points on Elliptic Curves*, Spring-Verlag.

[14] W. A. Stein. *The modular form database*, http://modular.fas.harvard.edu/Tables/.

[15] Y. Yang, 2004. *Transformation formulas for generalized Dedekind eta functions*, Bull. London Math. Soc.36 (5) (2004) 671-682.

[16] Y. Yang, . *Defining equations of modular curves*, Adv. Math. (to appear)

[17] Y. Yang, 2005. *Lecture Notes on Modular Forms and Modular Functions.*

[18] P. Zograf, 1991. *A spectral proof of Rademacher's conjecture for congruence subgroups of the modualr group*, Math. Ann. 252 (3) (1980), 197-216.