行政院國家科學委員會專題研究計畫　成果報告

模曲線之定義方程式，cusp 型，及其相關問題

計畫類別：個別型計畫
計畫編號：NSC93-2115-M-009-014-
執行期間：93 年 08 月 01 日至 94 年 07 月 31 日
執行單位：國立交通大學應用數學研究所

計畫主持人：楊一帆

報告類型：精簡報告
報告附件：出席國際會議研究心得報告及發表論文
處理方式：本計畫可公開查詢

中　華　民　國 94 年 9 月 16 日

成果報告

中文摘要.

在本計畫中我們利用 generalized Dedekind eta functions 去構造模函數並利用它們給出模曲線的定義方程式。我們並更進一步地利用模曲線的定義方程去實際地算出一些有理橢圓曲線的模函數參數化。

關鍵詞. 模函數, 模曲線及其定義方程式, 橢圓曲線及其模函數參數化。

PROD. TYPE: COM
PP:1-28 (col.fig.: nil)
YAIMA2536
ED: Janagan
PAGN: Jagan – SCAN: nil
ARTICLE IN PRESS

ELSEVIER
Available online at www.sciencedirect.com
SCIENCE DIRECT®
Advances in Mathematics ■■■ (■■■■) ■■■–■■■
ADVANCES IN Mathematics
www.elsevier.com/locate/aim

Defining equations of modular curves

Yifan Yang

Department of Applied Mathematics, National Chiao Tung University, Hsinchu 300, Taiwan

Received 8 October 2004; accepted 27 May 2005
Communicated by Michael Hopkins

Abstract

We obtain defining equations of modular curves $X_0(N)$, $X_1(N)$, and $X(N)$ by explicitly constructing modular functions using generalized Dedekind eta functions. As applications, we describe a method of obtaining a basis for the space of cusp forms of weight 2 on a congruence subgroup. We also use our model of $X_0(37)$ to find explicit modular parameterization of rational elliptic curves of conductor 37.

MSC: primary 11F03; secondary 11G05; 11G18; 11G30

Keywords: ■; ■; ■

1. Background

1.1. Defining equations of modular curves

Let Γ be a congruence subgroup of $SL_2(\mathbb{R})$. The classical modular curves $X(\Gamma)$ are defined to be the quotients of the extended upper half-plane $\mathbb{H}^* = \{\tau \in \mathbb{C} : \operatorname{Im}\tau > 0\} \cup \mathbb{Q} \cup \{\infty\}$ by the action of Γ. In this note we will mainly concern ourselves with the congruence subgroups of the types

$$\Gamma_0(N) = \left\{ \gamma \in SL_2(\mathbb{Z}) : \gamma \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \bmod N \right\},$$

E-mail address: yfyang@math.nctu.edu.tw

0001-8708/$ - see front matter © 2005 Published by Elsevier Inc.
doi:10.1016/j.aim.2005.05.019

$$\Gamma_1(N) = \left\{ \gamma \in SL_2(\mathbb{Z}) : \gamma \equiv \pm \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \bmod N \right\},$$

$$\Gamma(N) = \left\{ \gamma \in SL_2(\mathbb{Z}) : \gamma \equiv \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \bmod N \right\},$$

and the modular curves $\Gamma\backslash\mathbb{H}^*$ associated with the above congruence subgroups will be denoted by $X_0(N)$, $X_1(N)$, and $X(N)$, respectively.

It turns out that a modular curve has the structure of a compact Riemann surface. Thus, a modular curve can be interpreted as a non-singular irreducible projective algebraic curve $\mathcal{C}$ (see [10, Appendix B]). Equivalently, the field of rational functions on $\mathcal{C}$ is isomorphic to the field of meromorphic functions on the modular curve. Hence, the homogeneous polynomials defining $\mathcal{C}$ are often referred to as defining equations of the corresponding modular curve. In practice, however, we find that it is more convenient to drop the non-singular condition, and call any polynomials that yield an isomorphic function field defining equations of a modular curve.

When the genus g of a modular curve is less than 5 or the curve is hyperelliptic (that is, a 2-fold covering of $\mathbb{P}^1(\mathbb{C})$ branched at $2g+2$ points), there are standard forms for defining equations. For example, if the genus is 0, the curve is isomorphic to $\mathbb{P}^1(\mathbb{C})$, and the defining equation is the zero polynomial. When the genus is 1, the curve is an elliptic curve, and an affine defining equation takes the form $y^2 + a_1xy + a_3y = x^3+a_2x^2+a_4x+a_6$. When the genus is 2 or the curve is hyperelliptic, an affine defining equation can be taken to be $y^2 = f(x)$ for some polynomial f. (Note that when the degree of f is greater than 3, the curve $y^2 = f(x)$ has a singularity at infinity.) A non-hyperelliptic curve of genus 3 has a plane quartic as a defining equation, while a non-hyperelliptic curve of genus 4 is the complete intersection of a degree 2 surface with a degree 3 surface in $\mathbb{P}^3$ (see [10]). When the genus exceeds 4, the geometry becomes more complicated, and there are no single standard forms.

When a modular curve is of the type $X_0(N)$, there is a canonical equation for it (the so-called modular equation of level N). Namely, let $j(\tau)$ be the classical modular j-function. Then the function field of $X_0(N)$ is generated by $j(\tau)$ and $j(N\tau)$, and a defining equation of $X_0(N)$ is $F_N(X,Y) = 0$, where F_N is a symmetric polynomial such that $F_N(j,Y)$ is the minimal polynomial of $j(N\tau)$ over $\mathbb{C}(j)$. This model of $X_0(N)$ is of theoretical use, but has several practical drawbacks. Firstly, the degree of F_N is very large, which means that the curve has many singular points. Secondly, the coefficients are gigantic. For example, when $N=2$, the largest coefficient in F_2 is already 157 464 000 000 000.

1.2. *Obtaining equations using the canonical embedding*

Let $\mathcal{C}$ be an algebraic curve, and let g be its genus. Let $\{\omega_1, \ldots, \omega_g\}$ be a basis of the space of holomorphic differentials. Suppose that $g > 2$. Then we can define a canonical map $\mathcal{C} \longmapsto \mathbb{P}^{g-1}$ by $P \longmapsto [\omega_1(P), \ldots, \omega_g(P)]$, where P denotes a point on $\mathcal{C}$. When the curve is non-hyperelliptic, this map is in fact injective, and we call it the canonical embedding (see [10, p. 341]).

In our modular curve setting, the above projective map is equivalent to the map $\tau \longmapsto [f_1(\tau), \dots, f_g(\tau)]$, where $\{f_1, \dots, f_g\}$ is a basis of the space $S_2(\Gamma)$ of cusp forms of weight 2 on Γ. Since any homogeneous polynomial of $f_1, \dots, f_g$ of degree k is a cusp form of weight $2k$ and $\dim S_{2k}(\Gamma)$ grows roughly in the speed of $2gk$, there is linear dependence among homogeneous polynomials of $f_1, \dots, f_g$ of the same sufficiently large degree. In many cases, these relations give a projective model of a modular curve. This approach has been adopted by Galbraith [8], Murabayashi [17], Shimura [21], and others to obtain defining equations for modular curves of the type $X_0(N)$. (Note that this method requires the knowledge of the Fourier coefficients of cusp forms of weight 2. One may obtain such information from Stein's modular form database [22], whose method of computing the Fourier coefficients in turn is originated from Merel [15,16].) This approach, however, has several drawbacks.

Firstly, ironically, the above method does not work for modular curves of genus 1 or 2, which presumably should be easier than those of higher genus, because there are not sufficient data. The method does not work for any hyperelliptic modular curve either because the map is two to one. (Note that equations of hyperelliptic modular curves $X_0(N)$ are also obtained by Galbraith [8], González [9], and Shimura [21]. Their methods are similar, except [9].) Secondly, in general, it is difficult to determine whether one has enough equations for a given curve of large genus.

1.3. Other methods of determining defining equations

Explicit equations of modular curves $X_1(N)$ have been studied by several authors. Using the fact that $X_1(N)$ can be interpreted as moduli spaces of isomorphic classes of elliptic curves with level N structures, Reichert [19] computed equations of $X_1(N)$, for $N = 11, 13, \dots, 18$, and then used them to determine torsion structures of elliptic curves over quadratic number fields. However, the computation becomes tedious as N gets large. Furthermore, the calculation is symbolic, and does not reveal what the corresponding modular functions that generate function fields are.

Explicit equations of $X_1(13)$, $X_1(16)$, and $X_1(25)$ have also been computed by Lecacheux [14], Washington [24], and Darmon [5], respectively, for the purpose of constructing cyclic extension of $\mathbb{Q}$. Their methods used the Hauptmoduls of $\Gamma_0(N)$. (The curve $X_0(13)$, $X_0(16)$, and $X_0(25)$ are all of genus 0.) Thus, the methods cannot be generalized immediately to other N.

Another method of computing equations of $X_1(N)$ is due to Ishida and Ishii [12]. They showed that the function field of $X_1(N)$ can be generated by two certain products of Weierstrass σ-functions. Thus, the relation between these two functions defines the curve $X_1(N)$. A similar method is also used to obtain defining equations of $X(N)$ by Ishida [11]. In general, though, the degree of the equations obtained in this fashion is not optimal. For example, the modular curves $X_1(14)$ and $X_1(15)$ are both of genus 1. Thus, the defining equations can be taken to be $y^2 = x^3 + ax + b$. However, the equations they obtained are of degree 4 and 5, respectively. (This, of course, can be remedied by finding suitable birational maps. But it is still something to be taken care of.)

1.4. Goals of the present note

In this note we will describe a systematic way of constructing modular functions on congruence subgroups with desired behavior at cusps using the generalized Dedekind η-functions. (See the next section for the definition of these functions.) Our method of constructing modular functions enables us to solve a variety of problems related to the theory of modular functions and modular curves, including the main theme of the present note, namely, determining defining equations of modular curves.

A distinct feature of our method is that the modular functions constructed all have poles only at infinity. (Thus, they can be regarded as analogs of Hauptmoduls for congruence subgroups of higher genus.) This feature makes the computation of defining equations relatively simple (see the discussion in Section 2). Furthermore, the equations obtained using our method are all plane curves, which may be more preferable in applications than those obtained from the canonical embedding.

Our method of finding defining equations works for curves of all types $X_0(N)$, $X_1(N)$, and $X(N)$, regardless of the genus or whether the curve is hyperelliptic. (At least in theory. To actually obtain equations for modular curves of large level in the range of hundreds, the solving of the related integer programming problem could take hours of computer time. Though, for the curves listed in the end of the article the computation takes only seconds.) Our method does not require knowledge of cusp forms of weight 2 either. On the contrary, our method in fact provides a way of finding a basis for the space of cusp forms of weight 2 on congruence subgroups. Furthermore, our model of $X_0(N)$, in many cases, can be used to determine explicitly the modular functions parameterizing a rational elliptic curve. In this note, we will work out the cases of elliptic curves of conductor 37.

The rest of the paper is organized as follows. In Section 2, we will give the definition and properties of the generalized Dedekind η-functions, and describe our method of finding defining equations of modular curves using them. In Section 3, we will give details of the applications mentioned above. In Section 4, we list defining equations up to $N = 50$ for $X_0(N)$, up to $N = 22$ for $X_1(N)$, and up to $N = 12$ for $X(N)$. (We have also computed a few more curves of higher level. They are available upon request.)

2. A new approach

Let $\mathcal{C}$ be a modular curve of non-zero genus, and let $K(\mathcal{C})$ denote the function field of $\mathcal{C}$. Our method of finding defining equations of $\mathcal{C}$ use the following basic idea, which is also used in [12]. Here, for $f \in K(\mathcal{C})$, we let $\deg_\infty f$ denote the total number of poles of f.

Lemma 1. *Suppose that X and Y are in $K(\mathcal{C})$ such that $\gcd(\deg_\infty X, \deg_\infty Y) = 1$. Then one has $K(\mathcal{C}) = \mathbb{C}(X, Y)$, and thus a defining equation of $\mathcal{C}$ can be taken to be $F(x, y) = 0$, where $F(x, y)$ is a polynomial such that $F(X, y)$ is the minimal polynomial for Y over $\mathbb{C}[X]$. Moreover, $F(x, y)$ is a polynomial of degree n in x and of degree m in y.*

Proof. Let $m = \deg_\infty X$ and $n = \deg_\infty Y$, and assume that $\gcd(m, n) = 1$. Then we have $[K(\mathcal{C}) : \mathbb{C}(X)] = m$ and $[K(\mathcal{C}) : \mathbb{C}(Y)] = n$ (see, for example, [7, p. 194]). It follows that $[K(\mathcal{C}) : \mathbb{C}(X, Y)]$ divides both m and n. Since $\gcd(m, n) = 1$, we conclude that $[K(\mathcal{C}) : \mathbb{C}(X, Y)] = 1$. That is, $K(\mathcal{C}) = \mathbb{C}(X, Y)$, $[\mathbb{C}(X, Y) : \mathbb{C}(X)] = m$, and $[\mathbb{C}(X, Y) : \mathbb{C}(Y)] = n$. Then the assertion about $F(x, y)$ follows immediately. This proves the lemma. □

As mentioned in the introduction, the functions we construct will have poles only at infinity. In this case, the polynomial $F(x, y)$ in Lemma 1 can be described as follows.

Lemma 2. *Suppose that X and Y are functions on $\mathcal{C}$ with a unique pole of orders m and n, respectively, at infinity such that $\gcd(m, n) = 1$ and that the leading Fourier coefficients are both 1. Then the polynomial $F(x, y)$ in Lemma 1 takes the form*

$$x^n - y^m + \sum_{a,b \geqslant 0, am+bn<mn} c_{a,b} x^a y^b.$$

Proof. By Lemma 1, the polynomial $F(x, y)$ takes the form $\sum_{a \leqslant n, b \leqslant m} c_{a,b} x^a y^b$. Let a_0 and b_0 be non-negative integers such that

$$a_0 m + b_0 n = \max\{am + bn : c_{a,b} \neq 0\}.$$

That is, $X^{a_0} Y^{b_0}$ has the largest degree among all terms with $c_{a,b} \neq 0$. In order to cancel the pole of order $a_0 m + b_0 n$ at infinity, there must be another pair (a_1, b_1) of non-negative integers such that $a_0 m + b_0 n = a_1 m + b_1 n$. Since $\gcd(m, n) = 1$, we have $n | (a_0 - a_1)$ and $m | (b_1 - b_0)$. Now suppose that none of the integers a_0 and a_1 is equal to zero. Then we will have $a_0 > n$ or $a_1 > n$. This contradicts to the fact from Lemma 1 that $F(x, y)$ is a polynomial of degree n in x. Therefore, we have $a_0 = 0$, $b_0 = m$ or $a_1 = n$, $b_1 = 0$. This shows that the polynomial $F(x, y)$ takes the claimed form. □

In practice, Lemma 2 means that, to find a relation between given X and Y with the prescribed properties, we can compute the Fourier expansion of $X^n - Y^m$ and use suitable products $X^a Y^b$ to cancel the poles at infinity recursively until we reach the constant term.

In light of Lemmas 1 and 2, to obtain defining equations of modular curves, it suffices to find functions with poles only at infinity. We now describe our method of constructing such functions.

2.1. Generalized Dedekind η-functions

Let $\tau \in \mathbb{H}$, and set $q = e^{2\pi i\tau}$. The ordinary Dedekind η-function is defined to be

$$\eta(\tau) = q^{1/24} \prod_{n=1}^{\infty} (1 - q^n).$$

This classical function has been extensively used to construct modular functions and modular forms on congruence groups containing $\Gamma_0(N)$. For example, a table of Hauptmoduls expressed in terms of the η-functions enabled Conway and Norton [3] to discover and describe explicitly the monstrous moonshine phenomena. However, in general, η-functions alone cannot yield all modular functions on a congruence group containing $\Gamma_0(N)$. For example, there is no way to express a Hauptmodul for $\Gamma_0^+(23) := \Gamma_0(23) + w_{23}$ in terms of $\eta(\tau)$ and $\eta(23\tau)$, where w_{23} denotes the Atkin–Lehner involution. Furthermore, when a congruence group does not contain $\Gamma_0(N)$, the associated function field has to be generated by something other than the Dedekind η-functions, and we find that generalized Dedekind η-functions are suitable for this purpose.

Following the notation by Yang [25], we fix a positive integer N, and define two classes of generalized Dedekind η-functions by

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

for g and h not congruent to 0 modulo N simultaneously and

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

for g not congruent to 0 modulo N, where $B(x) = x^2 - x + 1/6$. In Yang [25] we illustrated how to find Hauptmoduls for torsion-free genus 0 congruence subgroups of $SL_2(\mathbb{Z})$ using E_g. Moreover, generalizing the above result, we successfully determined Hauptmoduls for all genus 0 congruence subgroups of $SL_2(\mathbb{Z})$ (up to conjugation) in Chua et al. [2]. In this note we will make use of the above functions to construct modular functions that parameterize modular curves. Here, we recall the properties of E_g relevant to our consideration.

Proposition 1 (*Yang [25, Theorem 1]*). *The functions $E_{g,h}$ satisfy*

$$E_{g+N,h} = E_{-g,-h} = -\zeta^{-h} E_{g,h}, \quad E_{g,h+N} = E_{g,h}. \tag{1}$$

Moreover, let $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$. *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 $c \neq 0$,

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

where

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

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

and

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

Proposition 2 (*Yang [25, Corollary 2]*). *The functions* E_g *satisfy*

$$E_{g+N} = E_{-g} = -E_g. \tag{2}$$

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

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

and, for $c \neq 0$,

$$E_g(\gamma\tau) = \varepsilon(a, bN, c, d) e^{\pi i (g^2 ab/N - gb)} E_{ag}(\tau), \tag{3}$$

where

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

Proposition 3 (*Yang [25, Corollary 3]*). *Consider the function* $f(\tau) = \prod_g E_g(\tau)^{e_g}$, *where* g *and* e_g *are integers with* $g \not\equiv 0 \bmod N$. *Suppose that one has*

$$\sum_g e_g \equiv 0 \bmod 12, \quad \sum_g g e_g \equiv 0 \bmod 2. \tag{4}$$

Then f *is invariant under the action of* $\Gamma(N)$. *Moreover*, *if*, *in addition to* (4), *one also has*

$$\sum_g g^2 e_g \equiv 0 \bmod 2N. \tag{5}$$

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

Furthermore, *for the cases where* N *is a positive odd integer*, *conditions* (4) *and* (5) *can be reduced to*

$$\sum_g e_g \equiv 0 \bmod 12$$

and

$$\sum_g g^2 e_g \equiv 0 \bmod N,$$

respectively.

Proposition 4 (*Yang [25, Lemma 2]*). *The order of the function* E_g *at a cusp* a/c *with* $(a,c)=1$ *is* $(c,N)P_2(ag/(c,N))/2$, *where* $P_2(x) = \{x\}^2 - \{x\} + 1/6$ *and* $\{x\}$ *denotes the fractional part of a real number* x.

We now show that modular functions with poles only at infinity can be constructed using the above functions. This requires a result of Yu [26].

In [26] the cusps of $X_1(N)$ that lies above 0 on $X_0(p)$ for all primes $p|N$ are referred to as the cusps of the first type. Let $\mathcal{F}_1^0(N)$ denote the group of functions on $X_1(N)$ that have divisors supported on the cusps of the first type. Moreover, let $\mathcal{F}_1'(N)$ be the group generated by functions of the type $\prod_{h=1}^{N-1} E_{0,h}(\tau)^{e_h}$ satisfying the conditions

$$\sum_{h=1}^{N-1} h^2 e_h \equiv 0 \begin{cases} \bmod N & \text{for odd } N, \\ \bmod 2N & \text{for even } N, \end{cases}$$

and

$$\sum_{h \equiv \pm a \bmod N/p} e_h = 0 \quad \text{for all } p|N \text{ and for all congruence classes } a.$$

Then Yu proves the following result.

Proposition 5 (*Yu [26, Theorem 4]*). *We have $\mathcal{F}_1^0(N) = \mathcal{F}_1'(N)$, and they are of rank $\phi(N)/2 - 1$.*

Now observe that the action of the Atkin–Lehner involution ω_N sends the cusps of the first type to the cusps that are equivalent to ∞ under $\Gamma_0(N)$, and that, by Proposition 1,

$$E_{0,g}(-1/N\tau) = e^{-\pi ig/N} E_{g,0}(N\tau) = e^{-\pi ig/N} E_g(\tau).$$

Thus, we have the following result.

Proposition 6. *Assume $N \geqslant 3$. Let $\mathcal{F}_1^\infty(N)$ denote the group of modular functions on $\Gamma_1(N)$ that have divisors supported by the cusps lying above ∞ on $X_0(N)$, and let $\mathcal{F}_1''(N)$ denote the group generated by functions of the type $\prod_{g=1}^{N-1} E_g(\tau)^{e_g}$ satisfying*

$$\sum_{g=1}^{N-1} g^2 e_g \equiv 0 \begin{cases} \bmod N & \text{for odd } N, \\ \bmod 2N & \text{for even } N, \end{cases} \tag{6}$$

and

$$\sum_{g \equiv \pm a \bmod N/p} e_g = 0 \quad \text{for all } p|N \text{ and for all congruence classes } a. \tag{7}$$

Then one has $\mathcal{F}_1^\infty(N) = \mathcal{F}_1''(N)$, and they are of rank $\phi(N)/2 - 1$.

We remark that, by Proposition 3, conditions (6) and (7) imply that the product is a modular function on $\Gamma_1(N)$, and, by Proposition 4, condition (7) implies that the function has neither poles nor zeroes at the cusps that are not equivalent to infinity under $\Gamma_0(N)$.

We now prove a result stating that we can always find functions X and Y satisfying the assumptions in Lemma 2. The proof requires the following lemma.

Lemma 3. *Let $V \subset \mathbb{Z}^n$ be a $\mathbb{Z}$-module of rank $n-1$ such that $a_1 + \cdots + a_n = 0$ for all $v = (a_1, \ldots, a_n) \in V$. Let d be the greatest common divisor of all a_1 in $v = (a_1, \ldots, a_n) \in V$. Then there is an element$(-md, a_2, \ldots, a_n)$ in V such that $a_2, \ldots, a_n \geqslant 0$ for all sufficiently large integer m.*

Proof. We first choose any vector v_0 in V with $v_0 = (-d, b_2, \ldots, b_n)$, and let $b = \max_{2 \leqslant k \leqslant n} |b_k|$. Now consider the vector $v_1 = (1-n, 1, \ldots, 1) \in \mathbb{Z}^n$. It is contained in the subspace $W \subset \mathbb{Z}^n$ consisting of all vectors whose sums of entries are equal to zero. Since W is also of rank $n-1$, there is a positive integer a such that $av_1 \in V$. Choose a sufficient large integer k such that $ak \geqslant b$. Then both av_1 and $kav_1 + v_0$ are in

V and they are of the form $(-md, a_2, \ldots, a_n)$ with $a_2, \ldots, a_n \geqslant 0$. Then the assertion follows immediately. $\square$

Proposition 7. *The group $\mathcal{F}_1^{\infty}(N)$ contains at least two functions that have poles only at infinity and whose orders of poles are relatively prime.*

Proof. Assume that $N \geqslant 3$. By Proposition 6 and Lemma 3, it suffices to prove that the group $F_1^{\infty}(N)$ contains a function having a simple pole at infinity.

When N is a prime greater than 3, we find $(E_2^2/E_1E_3)^N$ is such a function. When N is a prime power $p^a \geqslant 8$, $a \geqslant 2$, we consider functions of the type $f_k = E_{k+N/p}^2/E_kE_{k+2N/p}$, $k \not\equiv N/p \bmod N$. It is easy to verify that the divisors are supported at cusps equivalent to infinity under $\Gamma_0(N)$. If k is an integer such that $k + 2N/p > N > k + N/p$, then the order of f_k at infinity is

$$N\left(2B_2(k/N + 1/p) - B_2(k/N) - B_2(k/N + 2/p - 1)\right)/2 = k - N/p^2 + 2N/p + N,$$

where $B_2(x) = x^2 - x + 1/6$ is the second Bernoulli polynomial. Thus, if k is an integer such that $k + 2N/p > N > k + N/p - 1$, then the function f_k/f_{k+1} has a simple pole at infinity.

When N is a product p^aq^b, $p < q$, of two prime powers, we consider the function $f_k = E_{k+N/p}E_{k+N/q}/(E_kE_{k+N/p+N/q})$, $k \not\equiv -N/p, -N/q, -N/p - N/q \bmod N$. Again, these functions have poles and zeroes only at the cusps equivalent to infinity under $\Gamma_0(N)$. When k is chosen such that $k + N/p + N/q > N > k + N/p$, then the order of f_k at infinity is

$$k + N/p + N/q - N/(pq) - N.$$

Thus, if $k + N/p + N/q > N > k + N/p - 1$, then f_k/f_{k+1} has a simple pole at infinity.

When N is a product $p_1^{a_1}p_2^{a_2}\ldots$ of at least three prime powers, the exact description of construction becomes complicated, and we shall only sketch our idea. Let P_0 denote the set of primes dividing N. For a subset P of P_0 we let c_P denote the sum $\sum_{p \in P} 1/p$. We consider the function f_k of the form

$$\begin{aligned} f_k &= \prod_{P \subset P_0} E_{k+Nc_P}^{(-1)^{|P|}} \\ &= E_k \left(\prod_p E_{k+\frac{N}{p}}\right)^{-1} \left(\prod_{p_1,p_2} E_{k+\frac{N}{p_1}+\frac{N}{p_2}}\right) \left(\prod_{p_1,p_2,p_3} E_{k+\frac{N}{p_1}+\frac{N}{p_2}+\frac{N}{p_3}}\right)^{-1} \ldots, \end{aligned}$$

where the products run over all subsets P of P_0, and let k vary. Let $m(x)$ denote the greatest integer less than or equal to x. Then the order of f_k at infinity, after simplifying, is equal to

$$C - k \sum_{P \subset P_0} m(k/N + c_P) + \sum_{P \subset P_0} N c_P m(k/N + c_P)$$
$$+ \frac{N}{2} \sum \left(m(k/N + c_P)^2 + m(k/N + c_P) \right),$$

where C is a constant depending only on N. Now choose k_1 and k_2 such that the integers $m(k_1/N + c_P) = m(k_2/N + c_P)$ for all $P \subset P_0$ with only one exception P_1, where $m(k_1/N + c_{P_1}) = 0$ and $m(k_2/N + c_{P_1}) = 1$. Then the function f_{k_2}/f_{k_1} has order

$$(k_1 - k_2) \sum_{P \neq P_1} m(k/N + c_P) - k_2 + C_1$$

at infinity, where C_1 is a constant depending only on N and P_1. Finally, if $k_1 + 1$ and $k_2 + 1$ also satisfy the property that $m((k_1 + 1)/N + c_P) = m((k_2 + 1)/N + c_P)$ for $P \neq P_1$ and $m((k_1 + 1)/N + c_{P_1}) = 0$, $m((k_2 + 1)/N + c_{P_2}) = 1$, then the function $f_{k_2+1} f_{k_1} / (f_{k_1+1} f_{k_2})$ has a simple pole at infinity. This concludes the proof of the theorem. □

Remarks. For the curves $X_1(N)$ we have computed so far, we find that it is always possible to find a product of E_g that is modular on $\Gamma_1(N)$ and have a unique pole of order m at infinity for each non-gap integer m. It is reasonable to conjecture that it is always the case, but we are unable to prove it at this point.

We also remark that since $\Gamma_1(N)$ is normal in $\Gamma_0(N)$, if f is a function on $\Gamma_1(N)$, then

$$\sum_{\gamma \in \Gamma_0(N)/\Gamma_1(N)} f(\gamma\tau)$$

is a modular function on $\Gamma_0(N)$. Thus, Proposition 7 implies that we can always find modular functions on $\Gamma_0(N)$ with a unique pole of order m at infinity for sufficiently large m. Furthermore, since $\Gamma(N)$ is conjugate to a congruence subgroup containing $\Gamma_1(N^2)$, suitable products of E_g will generate the function field on $X(N)$ as well.

In the following sections we will work out some simple examples to illustrate the procedures of constructing modular functions using our method.

2.2. *Equations for $X_1(N)$*

Let us take the genus 1 curve $X_1(11)$ for example. From Property (2) in Proposition 2 we see that there are essentially only five distinct E_g. In order to fulfill the conditions in Proposition 3 we follow the notation of Fine [6], and set $W_k = E_{4k}/E_{2k}$. (The setting of $W_k = E_{4k}/E_{2k}$ instead of E_{2k}/E_k is to get rid of the factor involving $e^{\pi i b}$ in formula (3) so that the transformation formula for W_k becomes simpler.) It is obvious that any product of W_k will satisfy condition (4) in Proposition 3 automatically. Thus, if e_k are integers such that $\sum k^2 e_k \equiv 0 \bmod 11$, then $\prod W_k^{e_k}$ is modular on $\Gamma_1(11)$. Furthermore, from Proposition 4 we see that the only poles or zeroes of W_k are at cusps equivalent to $c_j = j/11$, $j = 1, \ldots, 5$. Let $v_k(c_j)$ denote the order of W_k at c_j. The values of v_k are given in the following table.

	c_1	c_2	c_3	c_4	c_5
$11v_1$	-5	2	10	-3	-4
$11v_2$	2	-3	-4	10	-5
$11v_3$	10	-4	2	-5	-3
$11v_4$	-3	10	-5	-4	2
$11v_5$	-4	-5	-3	2	10

Thus, finding a function X with a pole of order 2 at infinity and analytic elsewhere is equivalent to solving the integer programming problem

$$\begin{aligned} -5x_1 + 2x_2 + 10x_3 - 3x_4 - 4x_5 &= -22, \\ 2x_1 - 3x_2 - 4x_3 + 10x_4 - 5x_5 &\geqslant 0, \\ 10x_1 - 4x_2 + 2x_3 - 5x_4 - 3x_5 &\geqslant 0, \\ -3x_1 + 10x_2 - 5x_3 - 4x_4 + 2x_5 &\geqslant 0, \\ -4x_1 - 5x_2 - 3x_3 + 2x_4 + 10x_5 &\geqslant 0, \end{aligned}$$

and we find that one of the solutions is $(x_1, x_2, x_3, x_4, x_5) = (3, 2, 0, 1, 2)$. Hence, we can choose

$$X = -W_1^3 W_2^2 W_4 W_5^2 = q^{-2} + 2q^{-1} + 4 + 5q + 6q^2 + 5q^3 + 3q^4 - q^5 + \cdots,$$

where $q = e^{2\pi i \tau}$. Similarly, we can choose a degree 3 function Y to be

$$Y = W_1^4 W_2 W_4 W_5^3 = q^{-3} + 3q^{-2} + 7q^{-1} + 13 + 19q + 24q^2 + 25q^3 \cdots.$$

Now consider $Y^2 - X^3$, which has a Fourier expansion

$$Y^2 - X^3 = -q^{-4} - 3q^{-3} - 9q^{-2} - 19q^{-1} - 35 - 94q + \cdots.$$

Using X^2 to cancel the pole of order 4, we find

$$Y^2 - X^3 + X^2 = q^{-3} + 3q^{-2} + 7q^{-1} + 13 + 19q + \cdots = Y.$$

Thus, a defining equation is $Y^2 - Y = X^3 - X^2$.

In general, to find an equation for $X_1(N)$ we solve integer programming problems analogous to that for $X_1(11)$ and find two modular functions X and Y with minimal orders of pole at infinity so that $\gcd(\deg_\infty X, \deg_\infty Y) = 1$. Then we compute the relation between X and Y as above.

2.3. Equations for $X_0(N)$

For curves $X_0(N)$ the basic idea is the same, though the implementation is different and in many cases we can just use the Dedekind eta function. (See [18] for properties of the Dedekind eta function.)

To construct a modular function with a pole of order k at infinity and analytic elsewhere, we first find a function F on $\Gamma_1(N)$ that has a pole of order k at infinity, poles of order $< k$ at other cusps equivalent to infinity under $\Gamma_0(N)$, and regular at any other points. Then the function

$$X = \sum_{\gamma \in \Gamma_0(N)/\Gamma_1(N)} F\big|_\gamma$$

is modular on $\Gamma_0(N)$ with the desired properties, where γ runs over a set of coset representatives of $\Gamma_0(N)/\Gamma_1(N)$. Take $X_0(11)$ for example. We solve the integer programming problem

$$\begin{aligned} -5x_1 + 2x_2 + 10x_3 - 3x_4 - 4x_5 &= -22, \\ 2x_1 - 3x_2 - 4x_3 + 10x_4 - 5x_5 &\geqslant -11, \\ 10x_1 - 4x_2 + 2x_3 - 5x_4 - 3x_5 &\geqslant -11, \\ -3x_1 + 10x_2 - 5x_3 - 4x_4 + 2x_5 &\geqslant -11, \\ -4x_1 - 5x_2 - 3x_3 + 2x_4 + 10x_5 &\geqslant -11 \end{aligned}$$

and set

$$\begin{aligned} X &= -\sum_{\gamma \in \Gamma_0(11)/\Gamma_1(11)} W_1^2 W_5^3\big|_\gamma = \sum_{\gamma \in \Gamma_0(11)/\Gamma_1(11)} \frac{E_4^2 E_2}{E_{10}^3}\bigg|_\gamma \\ &= \frac{E_4^2 E_2}{E_{10}^3} + \frac{E_8^2 E_4}{E_{20}^3} + \frac{E_{12}^2 E_6}{E_{30}^3} + \frac{E_{16}^2 E_8}{E_{40}^3} + \frac{E_{20}^2 E_{10}}{E_{50}^3} \\ &= \frac{E_4^2 E_2}{E_1^3} - \frac{E_3^2 E_4}{E_2^3} + \frac{E_1^2 E_5}{E_3^3} - \frac{E_5^2 E_3}{E_4^3} + \frac{E_2^2 E_1}{E_5^3} \\ &= q^{-2} + 2q^{-1} + 4 + 5q + 8q^2 + q^3 + \cdots. \end{aligned}$$

Likewise, we let

$$Y = \sum_{\gamma \in \Gamma_0(11)/\Gamma_1(11)} W_3^{-3} W_4 \big|_\gamma = q^{-3} + 3q^{-2} + 7q^{-1} + 12 + 17q + 26q^2 + \cdots.$$

Then the functions satisfy $Y^2 - X^3 + X^2 + 3Y + 10X + 22 = 0$, which we take as a defining equation of $X_0(11)$. (In the result section we modify the choice of Y so that the equation is in conformity with that of Birch and Swinnerton-Dyer [23] or that of Cremona [4].)

A modification of the above method is to utilize the fact that any intermediate subgroup Γ between $\Gamma_1(N)$ and $\Gamma_0(N)$ is also normal in $\Gamma_0(N)$. Thus, to find a modular function on $\Gamma_0(N)$ with a unique pole of order k at infinity, we can proceed as above with the only difference being $\Gamma_1(N)$ replaced by Γ. For example, to find a modular function on $\Gamma_0(31)$ with a unique pole of order 3 at infinity, we choose Γ to be the subgroup generated by $\Gamma_1(31)$ and $\begin{pmatrix} 5 & -1 \\ 31 & -6 \end{pmatrix}$. It is easy to verify that $W_k = E_{6k}E_{26k}E_{30k}/(E_{2k}E_{10k}E_{12k})$ is a modular function on Γ for any integer k not divisible k. There are five essentially distinct W_k, and they are W_1, W_2, W_3, W_4, and W_8. Moreover, the cusp ∞ splits into five cusps 1/31, 2/31, 3/31, 4/31, and 8/31 in Γ. The orders of W_k at those cusps are as follows:

	1/31	2/31	3/31	4/31	8/31
W_1	3	0	−4	2	−1
W_2	0	2	3	−1	−4
W_3	−4	3	−1	0	2
W_4	2	−1	0	−4	3
W_8	−1	−4	2	3	0

(8)

It follows that the function

$$\sum_{\gamma \in \Gamma_0(31)/\Gamma} W_3 W_4 W_8 \big|_\gamma$$

is invariant under $\Gamma_0(31)$ and has a unique pole of order 3 at infinity.

2.4. Equations for $X(N)$

The method is identical to that for $X_1(N)$. We take $\Gamma(7)$ for example, and let $W_k = E_{4k}/E_{2k}$. From Propositions 2 and 3 we see that W_k is a modular function on $\Gamma(7)$. Moreover, the only possible poles of W_k occur at the cusps 1/7, 2/7, and 3/7, and W_k is regular at any other points. Solving integer programming problems similar to those mentioned earlier, we set

$$X = -W_1 W_3 = q_7^{-3} + q_7^4 + q_7^{11} - q_7^{25} - q_7^{32} + \cdots,$$

and

$$Y = W_1 W_3^2 = q_7^{-5} + 2q_7^2 + 2q_7^9 + q_7^{16} - q_7^{23} + \cdots,$$

where $q_7 = e^{2\pi i\tau/7}$ is a local parameter at infinity. (Note that the gap sequence is $\{1, 2, 4\}$.) Thus, a defining equation of $X(7)$ can be taken to be $Y^3 - XY = X^5$. (Setting $Y = yx$, $X = -x$, we obtain a non-singular model $xy^3 + x^3 + y = 0$, which is the famous Klein curve.)

2.5. Remarks

Since the complexity of integer programming problems mainly depend on the number and the range of variables, the amount of time needed to find required functions depends on the level, not the type of congruence subgroups. (That is, it will be easier to find modular functions that generate the function field on $X(29)$, which is of genus 806 than that of $X_0(227)$, whose genus is only 19 because the integer programming problem for the former curve involves only 14 variables, while the latter involves 113 variables.) It seems to us that to successfully apply our methods on curves of large level, one would need to take the symmetry of the integer programming problems involved into account.

3. Applications

3.1. Cusp forms of weight 2 on congruence subgroups

An immediate application of our result is the determination of cusp forms of weight 2 on congruence subgroups.

From [20, Proposition 2.16], we know that if $\omega = f\,d\tau$ is a holomorphic differential 1-form on a modular curve $X(\Gamma)$, then f is necessarily a cusp form of weight 2 on Γ. Thus, to determine a basis for the space $S_2(\Gamma)$ of cusp forms of weight 2 on a congruence subgroup Γ, we can compute a defining equation using our method first, and compute a basis $\{\omega_1, \ldots, \omega_g\}$ for the space of holomorphic differential 1-forms. Then $\{\omega_1/d\tau, \ldots, \omega_g/d\tau\}$ generates $S_2(\Gamma)$.

Let us take $X_1(17)$ for example. The genus is 5, and the gap sequence is $1, \ldots, 4, 6$. Choose

$$\begin{aligned} X &= E_6^2 E_7 E_8/(E_1^2 E_2 E_3) = q^{-5} + 2q^{-4} + 4q^{-3} + 7q^{-2} + 11q^{-1} + \cdots, \\ Y &= E_6^2 E_7 E_8^2/(E_1^3 E_2^2) = q^{-7} + 3q^{-6} + 8q^{-5} + 16q^{-4} + 30q^{-3} + \cdots. \end{aligned}$$

A defining equation is hence

$$\begin{aligned} &Y^5 - (4X-1)Y^4 + (6X^2 - 3X)Y^3 - (X^4 + 4X^3 - 5X^2 + X)Y^2 \\ &\quad + X^3(4X-1)(X-1)Y - X^6(X-1) = 0. \end{aligned}$$

From the defining equation we deduce that the space of cusp forms of weight 2 are spanned by

$$\frac{-X(2X^2-2X^3-Y+X^2Y)q\,dX/dq}{f(X,Y)} = q-q^2-2q^3+3q^4-2q^5-q^6+\cdots,$$

$$\frac{(-5X^3+3X^4+3XY-Y^3)q\,dX/dq}{f(X,Y)} = q^2-4q^3+7q^4-5q^5-4q^6+10q^7+\cdots,$$

$$\frac{X(X^2-X^3-Y+XY)q\,dX/dq}{f(X,Y)} = q^3-2q^4+q^6-q^7+3q^8-q^9+\cdots,$$

$$\frac{-X(X-Y)^2q\,dX/dq}{f(X,Y)} = q^4-2q^5-q^6+3q^7-q^9+q^{10}+\cdots,$$

$$\frac{(X^3-X^2Y-XY+Y^2)q\,dX/dq}{f(X,Y)} = q^6-3q^7+q^8+3q^9-q^{11}-4q^{12}+\cdots,$$

where

$$f(X,Y) = 4X^5-2X^4Y-5X^4+X^3-8X^3Y+18Y^2X^2+10X^2Y$$
$$-2XY-16Y^3X-9Y^2X+5Y^4+4Y^3.$$

3.2. Modular parameterization of rational elliptic curves

The well-known Taniyama–Shimura conjecture states that every rational elliptic curve can be parameterized by modular functions. The truth of this conjecture has been established by A. Wiles and others. However, in general, it is difficult to explicitly write down modular functions that parameterize an elliptic curve. Here we will demonstrate how to obtain modular parameterization of rational elliptic curves of conductor 37 using our model of $X_0(37)$.

The modular curve $X_0(37)$ is of genus 2, and thus hyperelliptic. The hyperelliptic involution is defined over $\mathbb{Q}$, but it does not come from the normalizer of $\Gamma_0(37)$ in $SL_2(\mathbb{R})$. Let w_{37} denote the Atkin–Lehner involution and w_h the hyperelliptic involution. Then the curves $X_0(37)/w_{37}$ and $X_0(37)/(w_{37}w_h)$ are of genus 1. We now construct modular functions to parameterize these two elliptic curves.

Let Γ be the intermediate subgroup between $\Gamma_1(37)$ and $\Gamma_0(37)$ with $[\Gamma_0(37):\Gamma]=6$, and set

$$X = \frac{\eta(\tau)^2}{\eta(37\tau)^2}+37$$

and

$$Y = \sum_{\gamma\in\Gamma_0(37)/\Gamma} \frac{E_6E_8E_{14}}{E_3E_4E_7}\Big|_{\gamma} - 5X + 174.$$

Then one has

$$Y^3 + (7X - 259)Y^2 - (7X^2 - 259X)Y = X^2(X - 36)(X - 37), \tag{9}$$

which we take as the defining equation of $X_0(37)$.

From Kenku [13] we know that there are four rational points on $X_0(37)$. In the above model we can easily locate four rational points, namely, ∞, $(0, 259)$, $(36, 0)$, and $(37, 0)$. (The singular point $(0, 0)$ is not a rational point. Blowing up the point $(0, 0)$ we obtain a non-singular model $y - tx = 0$, $t^3x - x^2 + 7t^2x - 7tx + 73x - 259t^2 + 259t - 1332 = 0$. We can easily see that the point corresponding to $X = 0$, $Y = 0$ is not a rational point.) The point ∞ corresponds to the cusp ∞. Using the transformation formula for the Dedekind eta function we obtain

$$X\Big|_{w_{37}} = 37\frac{\eta(37\tau)^2}{\eta(\tau)^2} + 37, \tag{10}$$

and thus $X(0) = 37$. Hence, the rational points $(37, 0)$ corresponds to the cusp 0. The other two points $(0, 259)$ and $(36, 0)$ must be the image of the cusps under the hyperelliptic involution. Since the birational map

$$u = \frac{Y}{X}, \quad v = \frac{Y^3 + 7XY^2 - 7X^2Y + 73X^3 - 518Y^2 + 518XY - 2664X^2}{X^3},$$

$$X = \frac{74(7u^2 - 7u + 36)}{u^3 + 7u^2 - 7u - v + 73}, \quad Y = \frac{74u(7u^2 - 7u + 36)}{u^3 + 7u^2 - 7u - v + 73}$$

transforms (9) into the normal form

$$v^2 = u^6 + 14u^5 + 35u^4 + 48u^3 + 35u^2 + 14u + 1,$$

the hyperelliptic involution w_h sends the point $(37, 0)$ to $(36, 0)$ and the point ∞ to $(0, 259)$. Thus, to find explicit modular parameterization of $X_0(37)/w_{37}$ we first construct functions s and t with poles only at ∞ and $(37, 0)$ such that s has a double pole at ∞ and a pole of order at most 2 at $(37, 0)$ and t has a triple pole at ∞ and a pole of order at most 3 at $(37, 0)$. Then the functions $x = s + s\big|_{w_{37}}$ and $y = t + t\big|_{w_{37}}$ yield an equation for the elliptic curve $X_0(37)/w_{37}$. Likewise, to obtain explicit modular parameterization of $X_0(37)/(w_{37}w_h)$, we construct functions s and t with poles of order 2 and 3, respectively, at ∞ and $(36, 0)$, and then proceed as usual. For the purpose of constructing such functions, we shall first study the behavior of X and Y under w_h, w_{37}, and $w_{37}w_h$.

The involution w_h sends u to u and v to $-v$. It follows that

$$X\Big|_{w_h} = \frac{74(7u^2 - 7u + 36)}{u^3 + 7u^2 - 7u + v + 73} = \frac{37(7Y^2 - 7XY + 36X^2)}{X^3} \tag{11}$$

and

$$Y\Big|_{w_h} = \frac{74u(7u^2 - 7u + 36)}{u^3 + 7u^2 - 7u + v + 73} = \frac{37Y(7Y^2 - 7XY + 36X^2)}{X^4}. \tag{12}$$

From (10) we have

$$X\Big|_{w_{37}} = \frac{37(X - 36)}{X - 37}. \tag{13}$$

To express $Y\big|_{w_{37}}$ in terms of X and Y, we utilize Proposition 1. We have

$$E_g\Big|_{w_{37}} = E_{g,0}(37\tau)\Big|_{w_{37}} = E_{g,0}(-1/\tau) = e^{\pi i g/37} E_{0,g}(\tau).$$

From this we deduce that

$$Y\Big|_{w_{37}} = 37(q + 3q^2 + 2q^3 + 7q^4 + 11q^5 + 25q^6 + \cdots).$$

At the cusp 0, the function $X - 37$ has a triple zero, the function Y has a simple zero, and the function $Y\big|_{w_{37}}$ has a quadruple pole. Hence, $Y\big|_{w_{37}} \cdot (X-37)Y$ is a function with a unique pole of order 6 at ∞. Using the Fourier expansions of the above functions we find that

$$Y\Big|_{w_{37}} = \frac{37X(X - 36)}{Y(X - 37)}. \tag{14}$$

Therefore, by (11), (12), (13), and (14), we have

$$X\Big|_{w_{37}w_h} = \frac{(7X^2 - 7XY + 36Y^2)(X - 37)}{Y^2(X - 36)} \tag{15}$$

and

$$Y\Big|_{w_{37}w_h} = \frac{X(7X^2 - 7XY + 36Y^2)(X - 37)}{Y^3(X - 36)}. \tag{16}$$

(Alternatively, we can use divisors of the functions X, $X - 37$, and Y to guess that $Y\big|_{w_{37}} = cX(X-36)/((X-37)Y)$ for some constant c. Then, since the choice of $c = 37$ makes the map $(X, Y) \longmapsto (37(X-36)/(X-37), 37X(X-36)/((X-37)Y))$ an involution on the curve (9), we conclude that $Y\big|_{w_{37}}$ has indeed the indicated expression.)

We now construct functions to parameterize $X_0(37)/w_{37}$. For a given function f on a curve we let div f denote the divisor of the function f. In our model of $X_0(37)$ we have div $X = -3(\infty) + 2(0,0) + (0,259)$ and div $Y = -4(\infty) + 2(0,0) + (36,0) + (37,0)$. It follows that the function $s = X(X-36)/Y$ has poles of order 2 at ∞ and a simple pole at $(37,0)$, and regular everywhere. Thus, $s + s\big|_{w_{37}}$ is a function on $X_0(37)/w_{37}$ with a unique pole of order 2 at ∞. Using (9), (13), and (14), we express $s + s\big|_{w_{37}}$ as

$$s + s\Big|_{w_{37}} = \frac{X^3 - 73X^2 + 1332X + Y^2}{(X-37)Y}.$$

Furthermore, the function X has a unique pole of order 3 at ∞ on $X_0(37)$. Therefore,

$$X + X\Big|_{w_{37}} = X + \frac{37(X-36)}{X-37} = \frac{X^2 - 1332}{X-37}$$

is a function with a unique pole of order 3 at ∞ on $X_0(37)/w_{37}$. Finally, setting

$$\begin{aligned} x &= s + s\Big|_{w_{37}} + 13 = \frac{X^3 - 73X^2 + 1332X + Y^2}{(X-37)Y} + 13 \\ &= q^{-2} + 2q^{-1} + 5 + 9q + 18q^2 + 29q^3 + 51q^4 + 82q^5 + \cdots \end{aligned}$$

and

$$\begin{aligned} y &= X + X\Big|_{w_{37}} + 5x - 80 = \frac{X^2 - 1332}{X-37} + 5x - 80 \\ &= q^{-3} + 3q^{-2} + 9q^{-1} + 21 + 46q + 92q^2 + 180q^3 + 329q^4 + \cdots, \end{aligned}$$

we obtain the modular parameterization of the elliptic curve 37A1: $y^2 + y = x^3 - x$. As a check on our computation we calculate the Fourier expansion of

$$-\frac{q\,dx/dq}{2y+1} = q - 2q^2 - 3q^3 + 2q^4 - 2q^5 + 6q^6 - q^7 + 6q^9 + 4q^{10} + \cdots,$$

which is indeed the Fourier expansion of the unique normalized eigenform of weight 2 on $\Gamma_0(37) + w_{37}$.

We now construct functions to parameterize the elliptic curve $X_0(37)/(w_{37}w_h)$. Under the quotient map $X_0(37) \mapsto X_0(37)/(w_{37}w_h)$, the points ∞ and $(36,0)$ are identified together, and $(37,0)$ and $(0,259)$ together. Thus, to find a function on the quotient curve with a unique pole of order 2 at ∞, we first look for a function on $X_0(37)$ that has a double pole at ∞ and a pole of order at most 2 at $(36,0)$. From the divisors div $X = -3(\infty) + 2(0,0) + (0,259)$ and $Y = -4(\infty) + 2(0,0) + (36,0) + (37,0)$ we easily see that $X(X-37)/Y$ has the desired properties. By (15) and (16), we have

$$\frac{X(X-37)}{Y} + \frac{X(X-37)}{Y}\Big|_{w_{37}w_h} = \frac{X^3 - 66X^2 + 1073X - 7XY + 259Y - Y^2}{Y(X-36)}.$$

This is a function on $X_0(37)/(w_{37}w_h)$ with a double pole at ∞. Likewise, the function

$$X + X\Big|_{w_{37}w_h} = X + \frac{(7X^2 - 7XY + 36Y^2)(X - 37)}{Y^2(X - 36)}$$

is a function with a triple pole at ∞. Finally, setting

$$\begin{aligned} x &= \frac{X^3 - 66X^2 + 1073X - 7XY + 259Y - Y^2}{Y(X - 36)} + 8 \\ &= q^{-2} - 1 + q + 5q^2 - q^3 + 10q^4 - 4q^5 + 15q^6 + \cdots \end{aligned}$$

and

$$\begin{aligned} y &= X + \frac{(7X^2 - 7XY + 36Y^2)(X - 37)}{Y^2(X - 36)} + 2x - 72 \\ &= q^{-3} - q^{-1} + 1 - 4q - 2q^2 - 12q^3 + 4q^4 - 36q^5 + \cdots, \end{aligned}$$

we have $y^2 + y = x^3 + x^2 - 23x - 50$. This is the elliptic curve 37B1 in Cremona's table. Again, we check that

$$-\frac{q\,dx/dq}{2y + 1} = q + q^3 - 2q^4 - q^7 - 2q^9 + 3q^{11} - 2q^{12} - 4q^{13} + \cdots$$

agrees with the Fourier expansion of the normalized eigenform f of weight 2 on $\Gamma_0(37)$ with $f\big|_{w_{37}} = -f$.

We remark that the above method will certainly work for all rational elliptic curves that are in fact quotient curves of $X_0(N)$ by Atkin–Lehner involutions.

4. Results

In this section, we list equations for modular curves of small level obtained using our method. The computer softwares we used include `lp_solve`, `Ampl`, and `Maple`. The first two are used to solve the integer programming problems for finding required modular functions. (We note that the use of `Ampl` is not essential in our computation because it serves mainly as a user-solver interface. In fact, the software `lp_solve` alone will suffice for our purpose.) Once required modular functions X and Y are found, we use the computer algebra software `Maple` to determine the equation satisfied by X and Y, which by the remark following Lemma 2 is nothing more than computing the q-expansions of X and Y and finding suitable combination of X and Y to cancel the negative powers of q in the expression $X^n - Y^m$, where m and n are the orders of pole of X and Y at infinity, respectively. To give the reader a clearer idea of what kind of computation is involved, we shall work out the case $\Gamma_0(31)$ in details.

Let Γ be the congruence subgroup generated by $\Gamma_1(31)$ and the matrix $\begin{pmatrix} 5 & -1 \\ 31 & -6 \end{pmatrix}$, as given in the last paragraph of Section 2.3. Then the index of Γ in $\Gamma_0(31)$ is $[\Gamma_0(31) : \Gamma] = 5$, and a set of coset representatives is given by $\{\gamma^k : k = 0, \ldots, 4\}$, where $\gamma = \begin{pmatrix} 2 & -1 \\ 31 & -16 \end{pmatrix}$. For an integer k not divisible by 31, we let $W_k = E_{6k}E_{26k}E_{30k}/(E_{2k}E_{10k}E_{12k})$. The functions W_k are modular on Γ and have poles and zeroes only at 1/31, 2/31, 3/31, 4/31, and 8/31. There are only five essentially different W_k and their orders at the above cusps are given in (8). Moreover, the action of γ on those W_k is verified to be

$$W_1\Big|_\gamma = W_2, \quad W_2\Big|_\gamma = W_4, \quad W_4\Big|_\gamma = W_8, \quad W_8\Big|_\gamma = W_3, \quad W_3\Big|_\gamma = W_1.$$

Now the genus of $\Gamma_0(31)$ is 2. Thus we need to find modular functions X and Y on $\Gamma_0(31)$ with a pole of order 3 and 4 at infinity (or equivalently 1/31), respectively. The corresponding inequalities are

$$\begin{aligned} 3x_1 + 0x_2 - 4x_3 + 2x_4 - 1x_5 &= -m, \\ 0x_1 + 2x_2 + 3x_3 - 1x_4 - 4x_5 &\geqslant -m + 1, \\ -4x_1 + 3x_2 - 1x_3 - 0x_4 + 2x_5 &\geqslant -m + 1, \\ 2x_1 - 1x_2 + 0x_3 - 4x_4 + 3x_5 &\geqslant -m + 1, \\ -1x_1 - 4x_2 + 2x_3 + 3x_4 + 0x_5 &\geqslant -m + 1 \end{aligned}$$

with $m = 3$ and 4. We find that (using `lp_solve`) we can choose $(x_1, x_2, x_3, x_4, x_5) = (0, 0, 1, 1, 1)$ and $(0, 0, 1, 0, 0)$, respectively.

Now we set

$$\begin{aligned} X &= \sum_{k=0}^{4} W_3W_4W_8\Big|_{\gamma^k} - 10 \\ &= W_3W_4W_8 + W_1W_8W_3 + W_2W_3W_1 + W_4W_1W_2 + W_8W_2W_4 - 10 \\ &= \frac{E_4E_7E_{11}}{E_1E_5E_6} + \frac{E_8E_9E_{14}}{E_2E_{10}E_{12}} - \frac{E_3E_{13}E_{15}}{E_4E_7E_{11}} + \frac{E_1E_5E_6}{E_8E_9E_{14}} - \frac{E_2E_{10}E_{12}}{E_3E_{13}E_{15}} - 10 \\ &= q^{-3} + 2q^{-2} - 8 - q + 3q^2 + 2q^3 + q^4 + 2q^5 - 3q^7 + 2q^8 + 2q^9 - q^{10} + \cdots \end{aligned}$$

and

$$Y = \sum_{k=0}^{4} W_3\Big|_{\gamma^k} + 3X + 50$$

$$= q^{-4} + 4q^{-3} + 7q^{-2} + q^{-1} - 5 - 2q + 12q^2 + 7q^3 + 4q^4 + 6q^5 + 4q^6$$
$$-10q^7 + 10q^8 + 8q^9 - 2q^{10} + \cdots.$$

By Lemma 2, the functions X and Y satisfy

$$Y^3 - X^4 + \sum_{a,b\geqslant 0, 3a+4b<12} c_{a,b} X^a Y^b = 0$$

for some rational numbers $c_{a,b}$. To find the coefficients $c_{a,b}$, we start from the Fourier expansion

$$\begin{aligned} Y^3 - X^4 &= 4q^{-11} + 45q^{-10} + 235q^{-9} + 672q^{-8} + 948q^{-7} - 108q^{-6} - 2378q^{-5} \\ &\quad -1709q^{-4} + 5501q^{-3} + 10958q^{-2} + 2382q^{-1} \\ &\quad -11257 - 7145q + 6637q^2 + \cdots. \end{aligned}$$

From this we see that the coefficient $c_{1,2}$ must be -4. Computing the q-expansion of

$$\begin{aligned} Y^3 - X^4 - 4XY^2 &= 5q^{-10} + 51q^{-9} + 232q^{-8} + 556q^{-7} + 616q^{-6} - 22q^{-5} \\ &\quad -201q^{-4} + \cdots, \end{aligned}$$

we get $c_{2,1} = -5$. Continuing this way, we find

$$Y^3 - X^4 - 4XY^2 - 5X^2Y - 11X^3 - 31Y^2 - 31XY - 31X^2 = 0.$$

This concludes the demonstration of our method.

4.1. Equations for $X_0(N)$

In this section, we list defining equations for $X_0(N)$. Here, in general, we choose functions X and Y with leading Fourier coefficients 1. However, starting from $X_0(34)$, there are a few cases where we make a slight adjustment to make the coefficients of the equations smaller. For example, in the case $N = 34$, we choose $X = q^{-4}/17 + \cdots$ and $Y = q^{-5}/17 + \cdots$. In those cases, we will see a rational number in front of a product of Dedekind η-functions or a sum of products of generalized Dedekind η-functions.

For brevity, a product of Dedekind η-functions $\prod \eta(a_i\tau)^{b_i}$ will be abbreviated as $\prod a_i^{b_i}$. The symbol E_g is the generalized Dedekind η-function introduced in Section 2.1. The notation $\sum_k \prod E_g^{e_g}$ represents

$$\sum_{\gamma\in\Gamma_0(N)/\Gamma} E_g^{e_g}\Big|_{\gamma},$$

where Γ is the intermediate subgroup between $\Gamma_1(N)$ and $\Gamma_0(N)$ with $[\Gamma_0(N):\Gamma]=k$. (In all the cases where this notation occurs, $\Gamma_0(N)/\Gamma_1(N)$ is cyclic, and there is no ambiguity about Γ.)

Whenever the genus of $X_0(N)$ is 1, we adjust the choice of X and Y so that the equation is in agreement with Cremona's table. When the genus is greater than 1, the equation is always singular. In those cases, we adjust the functions X and Y so that the $(0,0)$ is one of the singularities, provided that this adjustment will preserve the rationality of the coefficients.

Special attention should be given to the curve $X_0(43)$. The genus is 3, and the cusp ∞ is not a Weierstrass point. Thus, up to a constant displacement, there is only one modular function with a unique pole of order 4 at ∞ with leading Fourier coefficient 1. We find that this function is

$$q^{-4}+\tfrac{1}{2}q^{-3}+\tfrac{1}{2}q^{-2}+c+\tfrac{1}{2}q+q^2+\cdots$$

whose coefficients are not all integral. We have no explanation for this phenomenon.

N	Functions	Equation
11	$X=\sum_5 \frac{E_2E_4^2}{E_1^3},\quad Y=\sum_5 \frac{E_5^4}{E_1^3E_3}+1$	$Y^2+Y=X^3-X^2-10X-20$
14	$X=\frac{2\cdot 7^7}{1\cdot 14^7}+1,\quad Y=\frac{2^8\cdot 7^4}{1^4\cdot 14^8}-3X+1$	$Y^2+XY+Y=X^3+4X-6$
15	$X=\frac{3\cdot 5^5}{1\cdot 15^5}-1,$ $Y=\frac{3^9\cdot 5^3}{1^3\cdot 15^9}-\frac{3^2\cdot 5^{10}}{1^2\cdot 15^{10}}-3X-2$	$Y^2+XY+Y=X^3+X^2-10X-10$
17	$X=\sum_8 \frac{E_3E_8}{E_1E_2}-4,\quad Y=\sum_8 \frac{E_6^2E_8}{E_2^2E_3}+1$	$Y^2+XY+Y=X^3-X^2-X-14$
19	$X=\sum_9 \frac{E_7E_8}{E_1E_6}-3,\quad Y=\sum_9 \frac{E_6^2E_8}{E_2E_3^2}+X-6$	$Y^2+Y=X^3+X^2-9X-15$
20	$X=\frac{4\cdot 10^5}{2\cdot 20^5},\quad Y=\frac{4\cdot 5^5}{1\cdot 20^5}-X-2$	$Y^2=(X+1)(X^2+4)$
21	$X=\frac{3^3\cdot 7}{1\cdot 21^3}-2,$ $Y=\frac{3^6\cdot 7^2}{1^2\cdot 21^6}-\frac{3\cdot 7^7}{1\cdot 21^7}-2X-4$	$Y^2+XY=X^3-4X-1$
22	$X=\sum_5 \frac{E_8E_9}{E_2E_3}+2,\quad Y=\frac{1}{11}\left(\frac{2^8\cdot 11^4}{1^4\cdot 22^8}-\frac{1^7\cdot 11^3}{2^3\cdot 22^7}\right)$	$Y^3+(3X-11)Y^2+X^2Y$ $=X^4-9X^3+22X^2$
23	$X=\sum_{11} \frac{E_8E_{10}}{E_1E_5}-15,$ $Y=\sum_{11} \frac{E_8E_{10}^2E_{11}^2}{E_4E_5^2E_6^2}+7X+85$	$Y^3-(7X+69)Y^2-(12X^2+230X)Y$ $=X^4+37X^3+345X^2$

24	$X=\frac{6^3\cdot 8}{2\cdot 24^3},\quad Y=\frac{4\cdot 8^2\cdot 12^5}{2\cdot 6\cdot 24^6}$	$Y^2=(X-1)(X-2)(X+2)$
26	$X=\frac{2^4\cdot 13^2}{1^2\cdot 26^4}-13,\quad Y=\sum_3\frac{E_3E_{11}}{E_1E_5}+3X+35$	$Y^3-(4X+52)Y^2-(4X^2+52X)$ $=X^4+25X^3+156X^2$
27	$X=\frac{9^4}{3\cdot 27^3},\quad Y=\frac{3^3}{27^3}$	$Y^2+Y=X^3-7$
28	$X=\frac{4^4\cdot 14^2}{2^2\cdot 28^4},\quad Y=\frac{4\cdot 14^7}{2\cdot 28^7}-1$	$Y^3+5X^2Y=X^4-7X^2$
29	$X=\sum_7\frac{E_8E_9}{E_2E_5}-4,$ $Y=\sum_7\frac{E_4E_6E_{10}E_{14}}{E_2E_3E_5E_7}+4X+25$	$Y^3-(5X+29)Y^2-X^2Y$ $=X^4+10X^3+29X^2$
30	$X=\frac{1\cdot 6^6\cdot 10^2\cdot 15^3}{2^2\cdot 3^3\cdot 5\cdot 30^6},$ $Y=\frac{6^3\cdot 10^3\cdot 15^6}{2\cdot 5^2\cdot 15^9}$ $-\frac{1\cdot 2\cdot 5\cdot 6\cdot 10\cdot 15^3}{3\cdot 30^7}-5X-20$	$Y^4+(3X+15)Y^3+(3X^3+15X^2)Y$ $=X^5+11X^4+30X^3$
31	$X=\sum_5\frac{E_4E_7E_{11}}{E_1E_5E_6}-10,$ $Y=\sum_5\frac{E_3E_{13}E_{15}}{E_1E_5E_6}+3X+50$	$Y^3-(4X+31)Y^2-(5X^2+31X)Y$ $=X^4+11X^3+31X^2$
32	$X=\frac{16^6}{8^2\cdot 32^4},\quad Y=\frac{8^4\cdot 16^2}{4^2\cdot 32^4}$	$Y^2=X^3+4X$
33	$X=\sum_{10}\frac{E_7E_{10}}{E_1E_4}+1,\quad Y=\sum_{10}\frac{E_{13}E_{16}}{E_2E_5}+1$	$Y^4+(5X^2-11X)Y^2-(4X^3-11X^2)Y$ $=X^5-11X^4+22X^3$
34	$X=\frac{1}{17}\frac{2^4\cdot 17^2}{1^2\cdot 34^4},\quad Y=\frac{1}{17}\sum_8\frac{E_{12}E_{15}}{E_2E_5}+\frac{3}{17}$	$Y^4+10XY^3+(21X^2-13X)Y^2$ $+(6X^3-14X^2+6X)Y$ $=17X^5+2X^4-3X^3+2X^2-X$
35	$X=\frac{1}{35}\sum_{12}\frac{E_8E_{14}}{E_1E_7}-\frac{19}{35},$ $Y=\frac{1}{35}\sum_{12}\frac{E_{12}E_{14}E_{15}}{E_5E_6E_7}+5X+\frac{76}{35}$	$Y^4-(6X+2)Y^3+(7X^2+2X)Y^2$ $-(12X^3+5X^2)Y$ $=35X^5+31X^4+7X^3$
36	$X=\frac{12\cdot 18^3}{6\cdot 36^3},\quad Y=\frac{12^4\cdot 18^2}{6^2\cdot 36^4}$	$Y^2=X^3+1$
37	$X=\frac{1^2}{37^2}+37,\quad Y=\sum_6\frac{E_6E_8E_{14}}{E_3E_4E_7}-5X+174$	$Y^3+(7X-259)Y^2-(7X^2-259X)Y$ $=X^4-73X^3+1332X^2$
38	$X=\frac{1}{38}\sum_9\frac{E_3E_{12}E_{15}E_{18}}{E_1E_4E_7E_{16}}-\frac{9}{38},$ $Y=\frac{1}{38}\sum_3\frac{E_2E_9E_{13}E_{14}E_{15}E_{16}}{E_3E_4E_5E_6E_{10}E_{17}}-\frac{17}{38}$	$2Y^5+(36X-87)Y^4+(148X^2+18X-148)Y^3$ $+(28X^3+217X^2+32X-84)Y^2$ $-(66X^4-12X^3-148X^2-48X+16)Y$ $=76X^6+148X^5+128X^4+24X^3$ $-36X^2-16X$

1

39	$X=\frac{1}{13}\frac{3^3\cdot 13}{1\cdot 39^3}-1,$ $Y=\frac{1}{13}\sum_{12}\frac{E_{11}E_{19}}{E_2E_7}+5X+\frac{51}{13}$	$Y^4-(3X+3)Y^3-(3X^2+3X)Y^2-(3X^3+3X^2)Y=13X^5+25X^4+12X^3$
40	$X=\frac{4^3\cdot 20}{8\cdot 40^3},\quad Y=\frac{2\cdot 8\cdot 20^4}{10\cdot 40^5}$	$Y^4+(4X^2+20X)Y^2=X^5+9X^4+20X^3$
41	$X=\sum_{10}\frac{E_{16}E_{20}}{E_2E_{18}}-16,$ $Y=\sum_{10}\frac{E_{11}E_{17}}{E_4E_5}+4X+32$	$Y^4-(6X+41)Y^3+(6X^2+41X)Y^2-(5X^3+41X^2)Y=X^5+18X^4+82X^3$
42	$X=\frac{1}{7}\frac{1\cdot 6^6\cdot 14^2\cdot 21^3}{2^2\cdot 3^3\cdot 7\cdot 42^6}-1,$ $Y=\frac{1}{7}\sum_{6}\frac{E_{16}E_{19}}{E_2E_5}+\frac{6}{7}$	$Y^6-(X+7)Y^5+(7X^2+28X+36)Y^4+(14X^3+48X^2+18X-36)Y^3+(16X^4+55X^3+18X^2-36X)Y^2+(18X^5+60X^4+48X^3)=7X^7+18X^6+12X^5$
43	$X=\frac{1}{43}\sum_{7}\frac{E_5E_8E_{13}}{E_1E_6E_7}-\frac{15}{43},$ $Y=\frac{1}{43}\sum_{7}\frac{E_2E_9E_{11}E_{12}E_{14}E_{20}}{E_1E_4E_6E_7E_{15}E_{19}}-\frac{9}{43}$	$32Y^4-(88X-1)Y^3+(166X^2+34X+5)Y^2-(147X^3+49X^2+7X)Y=43X^5-16X^4-11X^3-2X^2$
44	$X=\frac{1}{11}\frac{4^4\cdot 22^2}{2^2\cdot 44^4},\quad Y=\frac{1}{11}\sum_{5}\frac{E_{16}E_{18}}{E_4E_6}+\frac{2}{11}$	$Y^5+12X^2Y^3-14X^2Y^2+(13X^4+6X^2)Y=11X^6+6X^4+X^2$
45	$X=\frac{9^3\cdot 15}{3\cdot 45^3},$ $Y=\frac{9\cdot 15^5}{3\cdot 45^5}-\frac{1\cdot 5\cdot 9^2\cdot 15}{3\cdot 45^4}-X+1$	$Y^4+10XY^2+X^3Y=X^5-25X^2$
46	$X=\frac{1}{2}\sum_{11}\frac{E_1E_{14}E_{15}E_{16}E_{17}E_{18}}{E_5E_6E_7E_8E_9E_{22}}-\frac{19}{2},$ $Y=\sum_{11}\frac{E_{16}E_{21}}{E_2E_7}-2X-19$	$Y^6+(5X+23)Y^5+(12X^2+46X)Y^4+(23X^3+138X^2)Y^3+(22X^4+115X^3)Y^2+(26X^5+184X^4)=X^7+8X^6$
47	$X=\frac{1}{47}\sum_{23}\frac{E_{12}E_{17}E_{19}E_{21}}{E_6E_{10}E_{13}E_{15}}-\frac{17}{47},$ $Y=\frac{1}{47}\sum_{23}\frac{E_{21}E_{22}E_{23}}{E_6E_{11}E_{13}}+3X+\frac{102}{47}$	$Y^5+(2X-2)Y^4-(X^2+9X)Y^3-(14X^3+22X^2)Y^2-(40X^4+35X^3)Y=47X^6+81X^5+35X^4$
48	$X=\frac{8^7\cdot 12}{4^3\cdot 16^2\cdot 24\cdot 48^2},\quad Y=\frac{8^4\cdot 24^2}{4^2\cdot 48^4}$	$Y^4=X^5-7X^4+12X^3$
49	$X=\frac{1}{49}+2,$ $Y=\frac{E_{21}}{E_7}+\frac{E_7}{E_{14}}-\frac{E_{14}}{E_{21}}-2X+1$	$Y^2+XY=X^3-X^2-2X-1$
50	$X=\frac{2^2\cdot 25}{1\cdot 50^2}-5,$ $Y=\frac{1}{2}\left(\frac{10^4\cdot 25^2}{5^2\cdot 50^4}-\frac{1^2\cdot 10\cdot 25^3}{2\cdot 5\cdot 50^4}\right)+2X+\frac{15}{2}$	$Y^3-(2X+10)Y^2-(2X^2+5X)Y=X^4+9X^3+20X^2$

4.2. Equations for $X_1(N)$

Here the notation $\prod a_i^{b_i}$ represents $\prod E_{a_i}^{b_i}$.

N	Functions	Equation
11	$X=\frac{3\cdot4\cdot5}{1^2\cdot2}$, $Y=\frac{4^3\cdot5}{1^3\cdot2}-1$	$Y^2+Y=X^3-X^2$
13	$X=\frac{4^2\cdot5\cdot6}{1^2\cdot2\cdot3}$, $Y=\frac{4\cdot6^3}{1^3\cdot2}$	$Y^3-(X-1)Y^2-XY=X^4+X^3$
14	$X=\frac{3\cdot4^2\cdot7}{1\cdot2^2\cdot5}-1$, $Y=\frac{4\cdot5^2\cdot6}{1\cdot2^2\cdot3}-1$	$Y^2+XY+Y=X^3-X$
15	$X=\frac{4\cdot7}{1\cdot2}-1$, $Y=\frac{4\cdot5\cdot6^2}{1\cdot2\cdot3^2}-1$	$Y^2+XY+Y=X^3+X^2$
16	$X=\frac{5\cdot6\cdot7}{1\cdot2\cdot3}$, $Y=\frac{4\cdot7^2\cdot8}{1\cdot2^2\cdot3}+1$	$Y^3+(X-1)Y^2-X^2Y=X^4-X^3$
17	$X=\frac{6^2\cdot7\cdot8}{1^2\cdot2\cdot3}$, $Y=\frac{6^2\cdot7\cdot8^2}{1^3\cdot2^2}$	$Y^5-(4X-1)Y^4+(6X^2-3X)Y^3$ $-(X^4+4X^3-5X^2+X)Y^2$ $+X^3(4X-1)(X-1)Y$ $=X^6(X-1)$
18	$X=\frac{4\cdot5\cdot9}{1\cdot2\cdot3}$, $Y=\frac{5\cdot6\cdot7\cdot8}{1\cdot2\cdot3\cdot4}-1$	$Y^3+XY^2+(2X^2-2X)Y$ $=X^4-3X^3+2X^2$
19	$X=\frac{6\cdot8\cdot9^2}{1^2\cdot2\cdot3}+1$, $Y=\frac{4\cdot6^2\cdot7^2\cdot8^2\cdot9^2}{1^3\cdot2^3\cdot3^2\cdot5}$	$Y^6-(5X-3)Y^5-(3X^3-15X^2+14X-3)Y^4$ $+(X-1)(9X^4-18X^3+7X^2-1)Y^3$ $-X^2(X-1)(9X^4-20X^3+13X^2-X-2)Y^2$ $+X^4(X-1)^2(4X^3-6X^2+2X+1)Y$ $=X^7(X-1)^4$
20	$X=\frac{6\cdot8\cdot9}{1\cdot2\cdot4}$, $Y=\frac{5\cdot8\cdot9\cdot10}{1\cdot2\cdot3\cdot4}+1$	$Y^4+XY^3+X(2X-3)Y^2$ $-X(2X^2-1)Y=X^4(X-1)$
21	$X=\frac{6\cdot7\cdot8\cdot10}{1\cdot2\cdot3\cdot5}$, $Y=\frac{4\cdot7\cdot8\cdot10^2}{1^2\cdot2^2\cdot5}$	$Y^5-(6X-4)Y^4+(2X-1)(7X-6)Y^3$ $-3(X-1)(X^3+3X^2-4X+1)Y^2$ $+3X^2(X-1)^2(2X-1)Y=X^4(X-1)^3$
22	$X=\frac{7\cdot8\cdot9\cdot10}{1\cdot2\cdot3\cdot4}$, $Y=\frac{8\cdot9^2\cdot10}{1\cdot2^2\cdot3}$	$Y^6+(X+5)Y^5-(4X^2+2X-8)Y^4$ $-(2X^3+16X^2+14X-4)Y^3$ $+(6X^4+11X^3-6X^2-12X)Y^2$ $+2X^2(X+1)(X^2+6X+6)Y$ $=X^3(X+1)^2(X+2)^2$

4.3. Equations for $X(N)$

Again, the notation $\prod a_i^{b_i}$ represents $\prod E_{a_i}^{b_i}$.

N	Functions	Equation
6	$X=\dfrac{\eta(2\tau)\eta(3\tau)^3}{\eta(\tau)\eta(6\tau)^3}$, $Y=\dfrac{\eta(2\tau)^4\eta(3\tau)^2}{\eta(\tau)^2\eta(6\tau)^4}$	$Y^2=X^3+1$
7	$X=3/1,\quad Y=2\cdot 3/1^2$	$Y^3-XY=X^5$
8	$X=3/1,\quad Y=2\cdot 4/1^2$	$Y^4=X(X-1)(X+1)(X^2+1)^2$
9	$X=4/1,\quad Y=3\cdot 4/1^2$	$Y^6-X(X^3+1)Y^3=X^5(X^3+1)^2$
10	$X=\dfrac{3\cdot 4}{1\cdot 2},\quad Y=\dfrac{4^3\cdot 5}{1^2\cdot 2\cdot 3}$	$Y^{10}=X(X+1)^2(X-1)^8(X^2+X-1)^5$
11	$X=\dfrac{4\cdot 5}{1^2},\quad Y=\dfrac{4\cdot 5^2}{1^2\cdot 3}$	$Y^{10}(Y+1)^9=X^{22}-Y(Y+1)^4 \times(6Y^4+13Y^3+12Y^2+5Y+1)X^{11}$
12	$X=5/1,\quad Y=4\cdot 6/1^2$	$Y^{12}=X(X-1)^2(X+1)^6(X^2+1)^4(X^2-X+1)^3$

Acknowledgments

The integer programming problems occurring in this work were solved using the `lp_solve` software. The author would like to thank M. Berkelaar, the author of `lp_solve`, for making it freely available on the Internet. The author would also like to thanks Professor Chiang-Hsieh of the National Center for Theoretical Sciences (Taiwan) for reading earlier versions of the paper and providing valuable comments. The author's use of the Fine functions W_k and their analogs is inspired by the work of Chan et al. [1]. The author would like to thank Professor Chan of the National University of Singapore for drawing his attention to the Fine functions. Finally, the author would like to thank the anonymous referee, whose constructive criticisms and valuable comments result in a great improvement of the paper. The author is supported by the National Science Council (Taiwan) Grant 92-2119-M-009-001.

References

[1] H.H. Chan, H. Hahn, R.P. Lewis, S.L. Tan, New Ramanujan–Kolbert type partition identities, Math. Res. Lett. 9 (5–6) (2002) 801–811.
[2] K.S. Chua, M.L. Lang, Y. Yang, On Rademacher's conjecture: congruence subgroups of genus zero of the modular group, J. Algebra 277 (1) (2004) 408–428.
[3] J.H. Conway, S.P. Norton, Monstrous moonshine, Bull. London Math. Soc. 11 (3) (1979) 308–339.
[4] J.E. Cremona, Algorithms for Modular Elliptic Curves, Cambridge University Press, Cambridge, 1992.
[5] H. Darmon, Note on a polynomial of Emma Lehmer, Math. Comp. 56 (194) (1991) 795–800.
[6] N.J. Fine, On a system of modular functions connected with the Ramanujan identities, Tôhoku Math. J. 8 (2) (1956) 149–164.
[7] W. Fulton, 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.

[8] S.D. Galbraith, Equations for modular curves, Doctoral Thesis, Oxford University, 1996.

[9] J. Gonzàlez, Equations of hyperelliptic modular curves, Ann. Inst. Fourier (Grenoble) 41 (4) (1991) 779–795.

[10] R. Hartshorne, Algebraic Geometry, Graduate Texts in Mathematics, vol. 52, Springer, New York, 1977.

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

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

[13] M.A. Kenku, On the modular curves $X_0(125)$, $X_1(25)$, and $X_1(49)$, J. London Math. Soc. (2) 23 (3) (1981) 415–427.

[14] O. Lecacheux, Unités d'une famille de corps cycliques réeles de degré 6 liés à la courbe modulaire $X_1(13)$, J. Number Theory 31 (1) (1989) 54–63.

[15] L. Merel, Opérateurs de Hecke pour $\Gamma_0(N)$ et fractions continues, Ann. Inst. Fourier (Grenoble) 41 (3) (1991) 519–537.

[16] L. Merel, Universal Fourier expansions of modular forms, in: On Artin's Conjecture for Odd 2-Dimensional Representations, Lecture Notes in Mathematics, vol. 1585, Springer, Berlin, 1994, pp. 59–94.

[17] N. Murabayashi, On normal forms of modular curves of genus 2, Osaka J. Math. 29 (2) (1992) 405–418.

[18] M. Newman, Construction and application of a class of modular functions. II, Proc. London Math. Soc. 9 (3) (1959) 373–387.

[19] M.A. Reichert, Explicit determination of nontrivial torsion structures of elliptic curves over quadratic number fields, Math. Comp. 46 (174) (1986) 637–658.

[20] G. Shimura, Introduction to the arithmetic theory of automorphic functions, Publications of the Mathematical Society of Japan, vol. 11, Princeton University Press, Princeton, NJ, 1994. Reprint of the 1971 original, Kano Memorial Lectures, 1.

[21] M. Shimura, Defining equations of modular curves $X_0(N)$, Tokyo J. Math. 18 (2) (1995) 443–456.

[22] W. Stein, The Modular Forms Database. <http://modular.fas.harvard.edu/Tables, 2004>.

[23] H.P.F. Swinnerton-Dyer, B.J. Birch, Elliptic curves and modular functions, in: Modular Functions of One Variable, IV, Proceedings of the International Summer School, University Antwerp, Antwerp, 1972, Lecture Notes in Mathematics, vol. 476, Springer, Berlin, 1975, pp. 2–32.

[24] L.C. Washington, A family of cyclic quartic fields arising from modular curves, Math. Comp. 57 (196) (1991) 763–775.

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

[26] J. Yu, A cuspidal class number formula for the modular curves $X_1(N)$, Math. Ann. 252 (3) (1980) 197–216.