國立臺灣大學理學院數學系

碩士論文

Department of Mathematics

College of Science

National Taiwan University

Master's Thesis

具 N 階點之橢圓曲線的參數表示

Explicit parametrizations of elliptic curves with N-torsions

林侑勳

Yuw-Hsun Lin

指導教授: 楊一帆 博士

Advisor: Yi-Fan Yang Ph.D.

中華民國 114 年 6 月

June, 2025

doi:10.6342/NTU202501859

國立臺灣大學碩士學位論文

口試委員會審定書

MASTER'S THESIS(DOCTORAL DISSERTATION) ACCEPTANCE CERTIFICATE
NATIONAL TAIWAN UNIVERSITY

具 N 階點之橢圓曲線的參數表示

Explicit parametrizations of elliptic curves with N-torsions

本論文係林侑勳君（R11221014）在國立臺灣大學數學系完成之碩士學位論文，於民國 114 年 6 月 25 日承下列考試委員審查通過及口試及格，特此證明

指導教授：

口試委員：　　李庭諭

所　　長：

doi:10.6342/NTU202501859

Acknowledgements

回顧研究所這三年，就像走過一座迷宮。

我曾經夢想成為一名數學研究者。當我收到錄取台大數學所的通知時，我無比興奮。那時的我，期待能在這裡遇見志同道合的朋友，接受教授的指導，鍛鍊研究能力，最終成為一名學者——或許，本來應該如此。

但我的碩士生涯並不如想像中順利。面對艱深的課業，我曾經熬夜苦撐；面對尋找指導教授與研究方向，我曾徬徨不前。在層層壓力下，我迷惘、逃避，也曾懷疑自己是否已經搞砸了人生。

然而，正是在這些困頓之中，我開始直視內心真正的聲音，並重新省思自己想走的路。雖然我選擇不再以成為數學家為目標，但這三年的歷程讓我更認識自己，也找到繼續走下去的方法。從迷失到完成這份論文，我學會了，即使未來還會有挑戰，我也能一步一步跨過去。

我要誠摯地感謝我的指導教授楊一帆教授，謝謝您在我最迷惘的時候，願意接納我、指導我、包容我，讓我有機會完成這份作品。也感謝我的家人與朋友，謝謝你們在我情緒低落時不離不棄，聆聽我、支持我、陪伴我。感謝學校心理輔導中心的老師，在我困惑無助時，教我理解自己、與自己和解。

我也想感謝數學，感謝它曾經是我生命中的指引，陪我走過許多階段。這篇論文，算是一個暫時的句點，我會懷抱著對知識的熱情繼續走下去。

最後，我想感謝我自己。謝謝你沒有放棄，哪怕走得跌跌撞撞，也仍然堅持了下來，讓這一切得以完成。

doi:10.6342/NTU202501859

doi:10.6342/NTU202501859

摘要

本論文探討帶有 N 階點的橢圓曲線組成之模空間，其中 N 為 4 到 20 之間的整數。目標是將橢圓曲線之 Tate 標準形式的係數，以明確的模函數表示。這些模函數由廣義戴德金 η 函數組成，並且生成由對應模群 $\Gamma_1(N)$ 的模函數組成的體。

關鍵字：模形式

doi:10.6342/NTU202501859

doi:10.6342/NTU202501859

Abstract

In this thesis, we study the moduli space of elliptic curves with a specified N-torsion, for $4 \leq N \leq 20$. Our focus is on expressing the coefficients of the Tate normal form of elliptic curves in terms of explicit modular functions. These modular functions are specific generators for the field of modular functions on $\Gamma_1(N)$ constructed from Generalized η-functions.

Keywords: Modular Form, Tate Normal Form

doi:10.6342/NTU202501859

doi:10.6342/NTU202501859

Contents

doi:10.6342/NTU202501859

doi:10.6342/NTU202501859

List of Tables

doi:10.6342/NTU202501859

doi:10.6342/NTU202501859

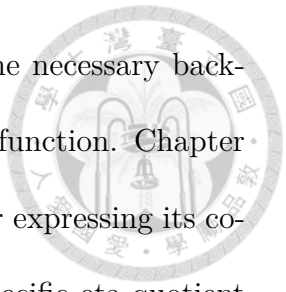
Chapter 1

Introduction

The study of elliptic curves and their moduli spaces plays a critical role in modern number theory. The moduli space $Y_1(N)$, the quotient space of the complex upper plane under the action of the matrix group $\Gamma_1(N)$ using Möbius transformation, is important for understanding elliptic curves over $\mathbb{C}$ since it provides a parametrization for the elliptic curves with a specified N-torsion point. A useful tool for studying these curves is the Tate normal form, which simplifies the representation of elliptic curves with torsion points. With this tool, we are able to narrow our focus to two coefficients, which are modular functions on $\Gamma_1(N)$ [1]. On the other hand, Yang [7][8] gave a table of generators. In this thesis, we aim to express the coefficients of the Tate normal form in terms of the generators given by the table.

This work builds on the properties of modular forms and the relationship between the Dedekind eta function and modular functions. By expressing the coefficients in this way, we provide a clear method for relating the Tate normal form to known generators of modular forms.

doi:10.6342/NTU202501859



This work is organized as follows. In Chapter 2, we review the necessary background on elliptic curves, modular forms, and the Dedekind eta function. Chapter 3 introduces the Tate normal form and formulates our method for expressing its coefficients using modular generators. Chapter 4 introduces the specific eta-quotient generators for fields of modular functions on $\Gamma_1(N)$ given by Yifan Yang [7][8], and Chapter 5 presents the computed expressions for each N in the range $4 \leq N \leq 20$.

doi:10.6342/NTU202501859

Chapter 2

Preliminaries

2.1 Complex Elliptic Curves

In this section, we denote the complex projective plane by $\mathbb{P}^2(\mathbb{C})$, which is defined to be the set of all equivalence classes of $\mathbb{C}^3\setminus\{(0,0,0)\}$ under the equivalence relation $\sim$ defined by

$$(z_1,z_2,z_3)\sim(z_1',z_2',z_3')\Leftrightarrow(z_1,z_2,z_3)=\lambda(z_1',z_2',z_3') \text{ for some } \lambda\neq 0.$$

Also we denote the set $(a:b:c)$ to be the equivalence class containing $(a,b,c)\in\mathbb{C}^3\setminus\{(0,0,0)\}$.

An elliptic curve over $\mathbb{C}$ is a nonsingular projective curve consisting of the zeros of the algebraic equation

$$Y^2Z+a_1XYZ+a_3YZ^2=X^3+a_2X^2Z+a_4XZ^2+a_6Z^3,\ a_1,\ldots,a_6\in\mathbb{C}$$

called the Weierstrass Form and the point $O=(0:1:0)\in\mathbb{P}^2(\mathbb{C})$ at infinity. In the following text, an elliptic curve would always mean an elliptic curve over $\mathbb{C}$. A

doi:10.6342/NTU202501859

curve is said to be nonsingular if the tangent line is well defined at each point on the curve. The nonsingularity condition imposes a restriction on the elliptic curve. To be precise, set

$$b_2 = a_1^2 + 4a_2,\ b_4 = 2a_4 + a_1a_3,\ b_6 = a_3^2 + 4a_6,$$

$$b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2,$$

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6.$$

Then the curve defined by the Weierstrass form is nonsingular if and only if $\Delta \neq 0$ (III.1.4 in [6]). For simplicity, the Weierstrass form is usually written as

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,\ a_1, \ldots, a_6 \in \mathbb{C}$$

in nonhomogeneous coordinates $x = X/Z$ and $y = Y/Z$.

The elliptic curve is also a curve with an additive group structure and identity $O = (0 : 1 : 0)$.

Theorem 2.1.1. (III.2.3, [6]) Let E be an elliptic curve defined by

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

Let $P = (x_P, y_P),\ Q = (x_Q, y_Q) \in E$. If $x_P = x_Q$ and $y_P + y_Q + a_1x_1 + a_3 = 0$, we have $P + Q = O$. Otherwise, set

$$\lambda = \begin{cases} \dfrac{y_Q - y_P}{x_Q - x_P}, & \text{if } x_P \neq x_Q, \\ \dfrac{3x_P^2 + 2a_2x_P + a_4 - a_1y_P}{2y_P + a_1x_P + a_3}, & \text{if } x_P = x_Q, \end{cases}$$

doi:10.6342/NTU202501859

$$\nu = \begin{cases} \dfrac{y_P x_Q - y_Q x_P}{x_Q - x_P}, & \text{if } x_P \neq x_Q, \\ \dfrac{-x_P^3 + a_4 x_P + 2a_6 - a_3 y_P}{2y_P + a_1 x_P + a_3}, & \text{if } x_P = x_Q. \end{cases}$$

and we define the addition $P + Q = (x_{P+Q}, y_{P+Q})$ by

$$\begin{cases} x_{P+Q} = \lambda^2 + a_1\lambda - a_2 - x_P - x_Q, \\ y_{P+Q} = -(\lambda + a_1)x_{P+Q} - \nu - a_3. \end{cases}$$

Then, the set of points on E forms a group under this addition.

Next, we define the isomorphism between elliptic curves.

Definition. A morphism $\phi : E_1 \to E_2$ is a function $\phi = (\phi_0, \phi_1, \phi_2)$ such that ϕ_1, ϕ_2, ϕ_3 are homogeneous polynomials of X, Y, Z with coefficients in K of the same degree. An isogeny $\phi : E_1 \to E_2$ is a morphism satisfying $\phi(O) = O$ and $\phi(E_1) = E_2$. Two elliptic curves E_1 and E_2 are said to be isomorphic if there are isogenies $\phi : E_1 \to E_2$ and $\psi : E_2 \to E_1$ such that $\phi \circ \psi$ and $\psi \circ \phi$ are identity maps on E_1 and E_2 respectively.

It can also be shown that an isogeny from E_1 to E_2 is also a group homomorphism. (III.4.8 [6]) Therefore, when two elliptic curves E_1 and E_2 are said to be isomorphic, they are also isomorphic in the sense of group isomorphism.

Recall that the Weierstrass form of an elliptic curve is written as

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \ a_1, \ldots, a_6 \in \mathbb{C}.$$

By the substitution $y \mapsto \frac{1}{2}(y - a_1x - a_3)$, E can be simplified to the elliptic curve

doi:10.6342/NTU202501859

of the form

$$E_1 : y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6,\ b_2, b_4, b_6 \in \mathbb{C}.$$

Furthermore, by the substitution $x \mapsto \left(\frac{x-3b_2}{36}, \frac{y}{216}\right)$, E_1 becomes the elliptic curve of the form

$$E_2 : y^2 = 4x^3 - Ax - B,\ A, B \in \mathbb{C}.$$

Observe that the point O at infinity is fixed by the substitution. Clearly, the three elliptic curves E, E_1 and E_2 are isomorphic to each other. Therefore, every elliptic curve is isomorphic to a elliptic curve defined by the equation of the form $y^2 = 4x^3 + Ax + B,\ A, B \in \mathbb{C}$.

Another property of elliptic curves is their relation to complex tori, which we define as below:

Definition. Let ω_1 and ω_2 be two nonzero complex numbers such that ω_1/ω_2 is not a real number. A lattice Λ with period ω_1, ω_2 is the set

$$\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 = \left\{n\omega_1 + m\omega_2 | (n, m) \in \mathbb{Z}^2\right\}.$$

The quotient $\mathbb{C}/\Lambda$, the set of cosets of Λ in $\mathbb{C}$, is called a complex torus.

An important function defined on the complex torus $\mathbb{C}/\Lambda$ is the Weierstrass $\wp$-function $\wp(z; \Lambda)$ defined by

$$\wp(z; \Lambda) := \frac{1}{z^2} + \sum_{\omega \in \Lambda \setminus \{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right),\ z \in \mathbb{C}$$

doi:10.6342/NTU202501859

The Laurent series of $\wp(z;\Lambda)$ at $z=0$ is

$$\wp(z;\Lambda) = \frac{1}{z^2} + \sum_{k=1}^{\infty} G_{2k+2}(\Lambda) z^{2k}$$

where $G_{2k}(\Lambda) = \sum_{\substack{\omega\in\Lambda \\ \omega\neq 0}} \omega^{2k}$ is called the Eisenstein series of weight $2k$. Also, the Weierstrass $\wp$-function satisfies

$$\wp'(z;\Lambda)^2 = 4\wp(z;\Lambda)^3 - g_2(\Lambda)\wp(z;\Lambda) - g_3(\Lambda) \tag{2.1}$$

$$= 4(\wp(z;\Lambda) - \wp(\frac{\omega_1}{2};\Lambda))(\wp(z;\Lambda) - \wp(\frac{\omega_2}{2};\Lambda))(\wp(z;\Lambda) - \wp(\frac{\omega_1+\omega_2}{2};\Lambda)) \tag{2.2}$$

for $z \notin \Lambda$, where $g_2(\Lambda) := 60G_4(\Lambda)$ and $g_3(\Lambda) = 140G_6(\Lambda)$ (P21–23,[2]). Moreover, the complex torus $\mathbb{C}/\Lambda$ is in one-to-one correspondence to the elliptic curve

$$E_\Lambda : y^2 = 4x^2 - g_2(\Lambda)x - g_3(\Lambda),$$

through the map

$$\phi : \mathbb{C} \to E \subset \mathbb{P}^2(\mathbb{C}), \begin{cases} z \mapsto (\wp(z) : \wp'(z) : 1) \\ 0 \mapsto (0:1:0) \end{cases}$$

(VI.3,6, [6]). We call E_Λ the elliptic curve corresponding to Λ. Two elliptic E_1 and E_2 corresponding to Λ_1 and Λ_2 respectively are isomorphic if and only if $\Lambda_1 = \alpha\Lambda_2$ for some nonzero $\alpha \in \mathbb{C}$ (VI.4.1.1 [6]). Therefore, every elliptic curve E_Λ corresponding to Λ with period ω_1, ω_2 is isomorphic to the elliptic curve E_τ corresponding to $\mathbb{Z}+\mathbb{Z}\tau$. Without loss of generality, we may assume the imaginary part of τ is positive. Also,

doi:10.6342/NTU202501859

every elliptic curve defined by

$$y^2 = 4x^3 - Ax - B,\ A, B \in \mathbb{C},$$

is an elliptic curve corresponding to some lattice Λ (VI.5.1 [6]). Combining all the results, we may conclude that every elliptic curve is isomorphic to some elliptic curve E_τ corresponding to $\mathbb{Z} + \mathbb{Z}\tau$ with τ having the positive imaginary part.

Finally, we end this section with a result of the moduli space of elliptic curves. For $N \geq 2$, An N-torsion point P on the elliptic curve E is a point on E such that $\underbrace{P + P + \cdots + P}_{N} = O$. We define an equivalence relation on the set of pairs (E, P), where E is a complex elliptic curve and P is an N-torsion point on E, as follows: (E_1, P_1) and (E_2, P_2) if there is an isomorphism $\phi : E_1 \mapsto E_2$ such that $\phi(P_1) = P_2$. Let $S_1(N)$ be the set of equivalence classes of pairs (E, P). We write $[E, P]$ to represent an equivalence class containing the pair (E, P). Next, we set

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

and set $\mathbb{H} = \{a + bi \in \mathbb{C} : b > 0\}$ to be the upper half plane. The matrix group $\Gamma_1(N)$ acts on $\mathbb{H}$ by the Möbius transformation.

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \tau = \frac{a\tau + b}{c\tau + d}, \quad \tau \in \mathbb{H}.$$

We write $\Gamma_1(N)\tau = \{\gamma\tau : \gamma \in \Gamma_1(N)\}$ for $\tau \in \mathbb{H}$ and set $Y_1(N)$ to be the quotient space of orbits under $\Gamma_1(N)$. Then we have the following nontrivial result:

Theorem 2.1.2 (Theorem 1.5.1,[4]). Let $\Lambda_\tau = \mathbb{Z} + \mathbb{Z}\tau$ for $\tau \in \mathbb{H}$. The set $S_1(N)$

doi:10.6342/NTU202501859

can be written as $S_1(N) = \{[E_\tau, \wp(1/N; \Lambda_\tau)] : \tau \in \mathbb{H}\}$. Two equivalent classes $[E_\tau, \wp(1/N; \Lambda_\tau)]$ and $[E_{\tau'}, \wp(1/N; \Lambda_{\tau'})]$ are the same if and only if $\Gamma_1(N)\tau = \Gamma_2(N)\tau'$. In other words, there is a one-to-one correspondence defined by

$$\psi : S_1(N) \to Y_1(N), \quad [E_\tau, \wp(1/N; \Lambda_\tau)] \mapsto \Gamma_1(N)\tau.$$

2.2 Tate Normal Form

Let E be an elliptic curve defined by the Weierstrass form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,\ a_1, \ldots, a_6 \in \mathbb{C},$$

and let $P = (x_0, y_0)$ be an N-torsion point on E. We can transform the Weierstrass form into the Tate normal form by the following procedure: By the substitution $(x, y) \mapsto (x + x_0, y + y_0)$, we can transform E into an isomorphic elliptic curve E' defined by the Weierstrass form

$$y^2 + a_1'xy + a_3'y = x^3 + a_2'x^2 + a_4'x,\ a_1', \ldots, a_4' \in \mathbb{C}, \tag{2.3}$$

with an N-torsion point $P = (0, 0)$ on E'. For an elliptic curve with Weierstrass form above and N-torsion point above, we have the following lemma:

Lemma 1. If P is an N-torsion point with $N \geq 3$, then $a_3' \neq 0$.

Proof. Suppose that $a_3' = 0$. Suppose $Q = (0, y_Q)$ is on E. By applying Q to the equation above, we have $y_Q^2 = 0$, which implies $y_Q = 0$ and $P = Q$. Therefore, $(0, 0)$ is the only point with x -coordinate 0. By the addition formula (Theorem 2.1.1), we have $P + P = O$ and thus P is a 2-torsion point, which is a contradiction to our

doi:10.6342/NTU202501859

assumption. Therefore, $a_3' \neq 0$. □

Next by substituting $(x, y) \mapsto (x, y + \frac{a_4'}{a_3'}x)$, we further transform E' to the isomorphic elliptic curve with Weierstrass form

$$y^2 + b_1xy + b_3y = x^3 + b_2x^2,\ b_1, b_2, b_3 \in \mathbb{C}, \tag{2.4}$$

with N-torsion point $P = (0, 0)$. For the elliptic curve with the Weierstrass form above, we have the following lemma.

Lemma 2. If P is an N-torsion point with $N \geq 4$, then $b_2 \neq 0$.

Proof. Suppose that $b_2 = 0$. Let $Q = (x_Q, 0)$ be a point on E. By applying Q to (2.4), we have $x_Q^3 = 0$, which implies that $x_Q = 0$ and $P = Q$. Therefore, P is the only point with y -coordinate 0. Since $N \geq 4$, we have $b_3 \neq 0$ by the previous lemma. By direct computation, we have $P+P = (0, -b_3)$ and $P+P+P = O$, which implies that P is a 3 -torsion point, which is a contradiction. Thus, $b_2 \neq 0$. □

Let $u = b_3/b_2 \neq 0$. Note that $b_3u^3 = b_2u^4$. By the substitution $(x, y) \mapsto (u^2x, u^3y)$, E'' can be transformed into the isomorphic elliptic curve E''' with Weierstrass form

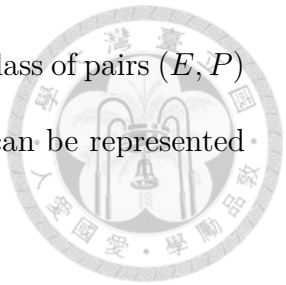
$$u^6y^2 + b_1u^5xy + b_3u^3y = u^6x^3 + b_2u^4x^2, \tag{2.5}$$

with N-torsion point $P = (0, 0)$. Write $1 + g = b_1u^{-1}$ and $f = b_3u^{-3} = b_2u^{-2}$ ($f \neq 0$). Then, the equation can rewritten as

$$y^2 + (1 + g)xy + fy = x^3 + fx^2,$$

which is called the Tate normal form. We have the following theorem from [1].

doi:10.6342/NTU202501859



Theorem 2.2.1. Suppose that $N \geq 4$. Then every isomorphism class of pairs (E, P) with E an elliptic curve and $P \in E$ a torsion point of order N can be represented by a unique pair of the form

$$E : y^2 + (1+g)xy + fy = x^3 + fx^2, \ P = (0,0),$$

with $f, g \in \mathbb{C}$ and $f \neq 0$.

Finally, we end this section with a result from [1], which gives a full set of representatives for the set of isomorphism classes of pairs (E, P) with E an elliptic curve and P an N-torsion point on E for $N \geq 4$. Note that the functions $\tau \mapsto \wp(1/N;\tau)$, $\tau \mapsto \wp(2/N;\tau)$ are modular forms of weight 2 on $\Gamma_1(N)$ and $\tau \mapsto \wp'(1/N;\tau)$, $\tau \mapsto \wp'(2/N;\tau)$ are modular forms of weight 3 on $\Gamma_1(N)$.

Theorem 2.2.2. Let $N \geq 4$ and let $S_1(N)$ be the set of isomorphism classes of pairs (E, P) with E an elliptic curve and P an N-torsion point on E. Then,

$$S_1(N) := \{[E_\tau, (0,0)]\}, \ E_\tau : y^2 + (1+g(\tau))xy + f(\tau)y = x^3 + f(\tau)x^2, \ \tau \in \mathbb{H},$$

where

$$f(\tau) = \frac{(\wp(1/N;\tau) - \wp(2/N;\tau))^3}{\wp'(1/N;\tau)^2},$$
$$g(\tau) = \frac{\wp'(2/N;\tau)}{\wp'(1/N;\tau)},$$

are modular functions on $\Gamma_1(N)$.

doi:10.6342/NTU202501859

2.3 Modular Forms and Modular Functions

Set

$$GL_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| a, b, c, d \in \mathbb{Z},\ ad - bc = \pm 1 \right\},$$

$$SL_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| a, b, c, d \in \mathbb{Z},\ ad - bc = 1 \right\},$$

and $PSL_2(\mathbb{Z}) = SL_2(\mathbb{Z})/\{\pm I\}$. The group $GL_2(\mathbb{Z})$ acts on $\mathbb{C}$ through Möbius transformation, which is defined by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \tau = \frac{a\tau + b}{c\tau + d}, \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{Z}),\ \tau \in \mathbb{C}.$$

This action of $GL_2(\mathbb{Z})$ leads to a classification of matrices.

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

(a) γ is elliptic if and only if $|a + d| < 2$,

(b) γ is parabolic if and only if $|a + d| = 2$,

(c) γ is hyperbolic if and only if $|a + d| > 2$.

doi:10.6342/NTU202501859

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

$$\gamma\tau = \tau \Leftrightarrow \frac{a\tau + b}{c\tau + d} = \tau,$$

$$\Leftrightarrow c\tau^2 + (d-a)\tau - b = 0.$$

The discriminant of the quadratic equation is

$$(d-a)^2 + 4bc = (d-a)^2 + 4(ad-1) = (d+a)^2 - 4.$$

Therefore, we have the following theorem

Theorem 2.3.1. (Theorem 1.3.1, [5]) Let $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$.

(a) γ is elliptic if and only if γ has two complex fixed points τ and its complex conjugate $\overline{\tau}$ with $\tau \in \mathbb{H}$,

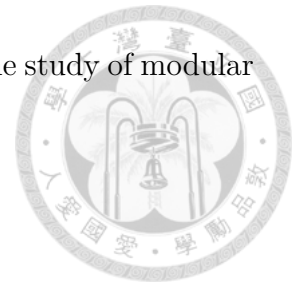
(b) γ is parabolic if and only if γ has exactly one fixed point in $\mathbb{P}^1(\mathbb{Q}) = \mathbb{Q} \cup \{\infty\}$,

(c) γ is hyperbolic if and only if γ has two real fixed point in in $\mathbb{P}^1(\mathbb{R}) := \mathbb{R} \cup \{\infty\}$.

This further gives us a classification of points in the upper half plane $\mathbb{H}$.

Definition. Let Γ be a subgroup of $SL_2(\mathbb{Z})$. An elliptic point is a fixed point of some elliptic matrix of Γ. A cusp of Γ is a fixed point of some parabolic matrix of Γ (including the point at infinity).

doi:10.6342/NTU202501859



Next, we review some matrix group that is frequently used in the study of modular forms. For a positive integer $N \geq 2$, we define

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \middle| c \equiv 0 (\text{mod } N) \right\},$$

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \middle| c \equiv 0 (\text{mod } N), a, d \equiv 1 (\text{mod } N) \right\},$$

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \middle| b, c \equiv 0 (\text{mod } N), a, d \equiv 1 (\text{mod } N) \right\}.$$

These are the most common examples of congruence subgroups.

Definition. A congruence subgroup Γ of $SL_2(\mathbb{Z})$ is a subgroup of $SL_2(\mathbb{Z})$ that contains $\Gamma(N)$ for some positive integer N. The smallest such N is called the level of Γ.

For a congruence subgroup Γ of $SL_2(\mathbb{Z})$, we denote $\overline{\Gamma}$ to be the subgroup $\pm\Gamma/\pm I$ of $PSL_2(\mathbb{Z})$. Note that

$$[PSL_2(\mathbb{Z}) : \overline{\Gamma}] = \begin{cases} [SL_2(\mathbb{Z}) : \Gamma], & \text{if} - I \in \Gamma, \\ \frac{1}{2}[SL_2(\mathbb{Z}) : \Gamma], & \text{if } -I \notin \Gamma. \end{cases}$$

Therefore,

$$[PSL_2(\mathbb{Z}) : \overline{\Gamma}_0(N)] = [SL_2(\mathbb{Z}) : \Gamma_0(N)],$$

doi:10.6342/NTU202501859

$$[PSL_2(\mathbb{Z}) : \overline{\Gamma}_1(N)] = \begin{cases} [SL_2(\mathbb{Z}) : \Gamma_1(N)], & \text{if } N = 2, \\ \frac{1}{2}[SL_2(\mathbb{Z}) : \Gamma_1(N)], & \text{if } N \geq 3, \end{cases}$$

$$[PSL_2(\mathbb{Z}) : \overline{\Gamma}(N)] = \begin{cases} [SL_2(\mathbb{Z}) : \Gamma(N)], & \text{if } N = 2, \\ \frac{1}{2}[SL_2(\mathbb{Z}) : \Gamma(N)], & \text{if } N \geq 3. \end{cases}$$

For calculating the index of subgroup, we have the following theorem:

Theorem 2.3.2 (Theorem 4.2.5, [5]). For an integer $N \geq 2$,

(a) $[PSL_2(\mathbb{Z}) : \overline{\Gamma}(N)] = \begin{cases} \frac{1}{2}[SL_2(\mathbb{Z}) : \Gamma(N)] = \frac{1}{2}N^3 \prod_{p|N}(1 - 1/p^2), & N > 2, \\ [SL_2(\mathbb{Z}) : \Gamma(2)] = 6, & N = 2. \end{cases}$

(b) $[PSL_2(\mathbb{Z}) : \overline{\Gamma}_0(N)] = [SL_2(\mathbb{Z}) : \Gamma_0(N)] = N \prod_{p|N}(1 + 1/p)$.

(c) $[PSL_2(\mathbb{Z}) : \overline{\Gamma}_1(N)] = \begin{cases} \frac{1}{2}[SL_2(\mathbb{Z}) : \Gamma_1(N)] = \frac{1}{2}N^2 \prod_{p|N}(1 - 1/p^2), & N > 2, \\ [SL_2(\mathbb{Z}) : \Gamma_1(2)] = 3, & N = 2. \end{cases}$

The product $\prod_{p|N}$ runs through all primes p that divide N.

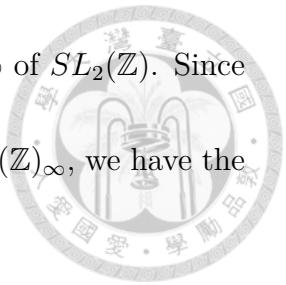
Let $\overline{\mathbb{H}} = \mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})$. For $N \geq 2$, we set $X_0(N)$, $X_1(N)$ and $X(N)$ to be the quotient space of orbits of $\overline{\mathbb{H}}$ under the action of $\Gamma_0(N)$, $\Gamma_1(N)$ and $\Gamma(N)$ respectively.

Remark. For $X_1(N)$, there exists a model over $\mathbb{Q}$ where the cusp corresponding to 0 is $\mathbb{Q}$-rational ([3]).

Recall that a cusp $\alpha \in \mathbb{P}(\mathbb{Q})$ of a subgroup Γ of $SL_2(\mathbb{Z})$ is a fixed point of a parabolic matrix of Γ. Let $\gamma \in SL_2(\mathbb{Z})$ be a matrix in $SL_2(\mathbb{Z})$ such that $\gamma \cdot \infty = \alpha$. Then, for $\delta \in SL_2(\mathbb{Z})$ with $\delta \cdot \alpha = \alpha$, we know that $(\gamma^{-1}\delta\gamma) \cdot \infty = \infty$. Let Γ_α (Γ_∞ respectively) be the stabilizer subgroup of α of Γ (∞ respectively). Then $\gamma^{-1}\Gamma_\alpha\gamma$ is

doi:10.6342/NTU202501859

a subgroup of Γ_∞. Let $SL_2(\mathbb{Z})_\infty$ be the stabilizer subgroup of ∞ of $SL_2(\mathbb{Z})$. Since $SL_2(\mathbb{Z})_\infty$ is generated by $\pm\begin{pmatrix} 1 & 1 \\ & \\ 0 & 1 \end{pmatrix}$ and Γ_∞ is a subgroup of $SL_2(\mathbb{Z})_\infty$, we have the following definition:



Definition. Let γ, α, and Γ be defined as above. The width of a cusp α of Γ is the smallest integer h such that

$$\gamma^{-1}\begin{pmatrix} 1 & h \\ & \\ 0 & 1 \end{pmatrix}\gamma \in \Gamma \quad \text{or} \quad -\gamma^{-1}\begin{pmatrix} 1 & h \\ & \\ 0 & 1 \end{pmatrix}\gamma \in \Gamma.$$

Then α is said to be regular if $\gamma^{-1}\begin{pmatrix} 1 & h \\ & \\ 0 & 1 \end{pmatrix}\gamma \in \Gamma$, and α is said to be irregular if $-\gamma^{-1}\begin{pmatrix} 1 & h \\ & \\ 0 & 1 \end{pmatrix}\gamma \in \Gamma$.

Note that the definition of h is independent of the choice of γ since if γ_1 and γ_2 are two matrices in $SL_2(\mathbb{Z})$ such that $\gamma_1 \cdot \infty = \gamma_2 \cdot \infty = \alpha$, $\gamma_1^{-1}\gamma_2 \in \Gamma_\alpha$. Also, two $\overline{\Gamma}$-equivalent cusps α_1 and α_2 (i.e. $\alpha_1 = \sigma \cdot \alpha_2$ for some $\sigma \in \Gamma$) have the same width. Here we cite a result for cusps of $\Gamma_1(N)$. The cusp ∞ is written as $1/0$ and $\gcd(0, N) = N$ for all integers N.

Theorem 2.3.3. (Theorem 4.2.9, [5]) Let $N \geq 4$ be an natural number.

(a) Let $a_1/c_1,\ a_2/c_2 \in \mathbb{P}(\mathbb{Q})$ be two cusps written in lowest terms. Then, a_1/c_1 and a_2/c_2 are $\overline{\Gamma_1}(N)$-equivalent if and only if there is $r \in \{\pm 1\}$ such that $c_1 \equiv rc_2 (\text{mod } N)$ and $a_1 \equiv ra_2 (\text{mod } \gcd(c_1, N))$.

(b) $\Gamma_1(N)$ has no elliptic points.

doi:10.6342/NTU202501859

(c) For $N \geq 5$, $\Gamma_1(N)$ has no irregular cusps. $\Gamma_1(4)$ has one orbits of irregular cusps (represented by $1/2$), and two orbits of regular cusps (represented by 0 and ∞).

(d) Let a/c be a cusp written in lowest terms. For $N \geq 5$, the width of a/c of $\Gamma_1(N)$ is $N/\gcd(c, N)$. The three orbits $[0]$, $[1/2]$ and $[\infty]$ of $\Gamma_1(4)$ have width 4, 1, and 1 respectively.

Next we proceed to define the modular forms and modular functions. Let $f : \mathbb{H} \to \mathbb{C}$ be a complex valued function on $\mathbb{H}$. For all integer matrix $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with positive determinant, and integer k, we define the slash operator of weight k of γ on f by

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

By direct computation, it is clear that

$$f|_k(\gamma_1\gamma_2) = (f|_k\gamma_1)|_k\gamma_2,$$

for all 2×2 integer matrices γ_1, γ_2 with positive determinant and integer k.

The modular form is defined as below:

Definition. Let Γ be a congruence group and k be a nonnegative integer. A function $f : \mathbb{H} \to \mathbb{C}$ is a modular form of weight k on Γ if

(a) f is holomorphic on $\mathbb{H}$,

(b) $(f|_k\gamma)(\tau) = f(\tau)$ for all $\gamma \in \Gamma$ and $\tau \in \mathbb{H}$,

doi:10.6342/NTU202501859

(c) f is holomorphic at every cusp of Γ (definition given later).

If the function f also vanishes at every cusp of Γ, then the function f is called the cusp form of weight k on Γ.

A classical example of a modular form is the Eisenstein series $G_{2k}(\tau), k \geq 1$ with respect to $\mathbb{Z} + \mathbb{Z}\tau$, which is a modular form of weight $2k$ on $SL_2(\mathbb{Z})$. The modular function is defined as below:

Definition. Let Γ be a congruence group. A function $f : \mathbb{H} \to \mathbb{C}$ is a modular function on Γ if

(a) f is meromorphic on $\mathbb{H}$,

(b) $f(\gamma\tau) = f(\tau)$ for all $\gamma \in \Gamma$ and $\tau \in \mathbb{H}$,

(c) f is meromorphic at every cusp of Γ (definition given below).

We define a function on $\mathbb{H}$ to be holomorphic or meromorphic at cusps as follows:

Definition. Let $\alpha \in \mathbb{P}^1(\mathbb{Q})$ and $\sigma \in SL_2(\mathbb{Z})$ be a matrix such that $\sigma\infty = \alpha$. Then the function $(f|_k\sigma)(\tau)$ admits a Fourier expansion of the form

$$(f|_k\sigma)(\tau) = \sum_{n\in\mathbb{Z}} a_n e^{2\pi i n\tau/h},$$

where h is the width of the cusp α(P.38–39, [5]). Let n be the smallest integer such that $a_n \neq 0$. Then $f(\tau)$ is said to be

(a) meromorphic at α if $n > -\infty$.

doi:10.6342/NTU202501859

(b) holomorphic at α if $n \geq 0$.

(c) vanishing at α if $n > 0$.

It is standard to set $q = e^{2\pi i\tau}$ and $q_h = e^{2\pi i/h}$ in the Fourier series of modular forms and modular functions. Thus, the Fourier series of modular forms and modular functions written in this way is also called the q-expansion.

2.4 Valence Formula

Now we review the valence formula and set bounds for the number of zeros for modular form of weight k on $\Gamma_1(N)$. Let $\overline{\mathbb{H}} = \mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})$. Let f be a meromorphic function on $\mathbb{H}$. For $\tau_0 \in \mathbb{H}$, define $v_{\tau_0}(f)$ to be the unique integer v such that $f(\tau)/(\tau - \tau_0)^v$ is holomorphic and nonzero at $\tau_0 \in \mathbb{H}$. If $\tau_0 \in \mathbb{P}^1(\mathbb{Q})$, let $\sigma \in SL_2(\mathbb{Z})$ be a matrix that satisfies $\sigma\infty = \tau_0$. Then, $f|_k\sigma$ admits a Fourier expansion of the form

$$(f|_k\sigma)(\tau) = \sum_{n\in\mathbb{Z}} a_n e^{2\pi i n\tau/h},$$

where h is the width of τ_0. Then $v_{\tau_0}(f)$ is defined to be the smallest integer n such that $a_n \neq 0$.

Theorem 2.4.1. (Theorem 5.6.11, [2])Let Γ be a subgroup of $SL_2(\mathbb{Z})$ of finite order. Let f be a modular function of weight k on Γ, which is not identically 0. Then,

$$\sum_{\tau\in\Gamma\backslash\overline{\mathbb{H}}} \frac{v_\tau(f)}{e_\tau} = [PSL_2(\mathbb{Z}) : \overline{\Gamma}]\frac{k}{12},$$

where $e_\tau = |\{\gamma \in \overline{\Gamma} : \gamma\tau = \tau\}|$ and $e_\tau = 1$ if $\tau \in \mathbb{P}^1(\mathbb{Q})$.

By the valence formula and the fact that $\Gamma_1(N),\ N \geq 4$ does not have elliptic

doi:10.6342/NTU202501859

points (Theorem 4.2.9, [5]), we can deduce that

Corollary 2.4.1.1. Let f be a modular form of weight k on $\Gamma_1(N)$ for some $N \geq 4$. For $\tau \in \overline{\mathbb{H}}$, we have

$$v_{\tau_0}(f) \leq [SL_2(\mathbb{Z}) : \Gamma_1(N)]\frac{k}{12} = \frac{1}{2}N^2 \prod_{p|N}(1 - \frac{1}{p^2}),$$

The product $\prod_{p|N}$ runs through all primes p that divide N.

Finally, we end this section with a theorem for a criterion of equality based on equality of the q-expansions.

Corollary 2.4.1.2 (Corollary 5.6.14, [2])**.** Let k be an integer, let h be a positive integer and let Γ be a subgroup of $SL_2(\mathbb{Z})$ of finite index. Set $m = [PSL_2(\mathbb{Z}) : \overline{\Gamma}]$. If two modular forms $f_i(\tau) = \sum_{n\geq 0} a_n^{(i)} q_h^n,\ q_h = e^{2\pi i\tau/h},\ i = 1, 2$ of weight k on Γ satisfy $a_n^{(1)} = a_n^{(2)}$ for all $1 \leq n \leq 1 + \frac{mk}{12}$, then $f_1 = f_2$.

2.5 Transformation Formula for $\wp(s\tau + t; \tau)$

Recall that the Weierstrass $\wp$-function $\wp(z; \tau)$ corresponding to $\Lambda_\tau = \mathbb{Z} + \mathbb{Z}\tau$ and its first derivative with respect to z is defined by

$$\wp(z;\tau) = \frac{1}{z^2} + \sum_{\omega\in\Lambda_\tau\setminus\{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right),\ z \in \mathbb{C},\ \tau \in \mathbb{H},$$

and

$$\wp'(z;\tau) = -\frac{2}{z^3} - 2\sum_{\omega\in\Lambda_\tau\setminus\{0\}} \frac{1}{(z-\omega)^3},\ z \in \mathbb{C},\ \tau \in \mathbb{H}.$$

We have the following transformation formula:

Theorem 2.5.1. Let $N \geq 4$, $s, t \in \mathbb{Q}$ and $\tau \in \mathbb{H}$ and set $P_{s,t}(\tau) = \wp(s\tau + t; \tau)$ and

doi:10.6342/NTU202501859

$Q_{s,t}(\tau) = \wp'(s\tau + t; \tau)$. Then, for $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$, we have

$$(P_{s,t}|_2\gamma)(\tau) = P_{as+ct,bs+dt}(\tau),\ (Q_{s,t}|_3\gamma)(\tau) = Q_{as+ct,bs+dt}(\tau).$$

Proof. Note that for $z \in \mathbb{Z}$ and $\tau \in \mathbb{H}$

$$\wp(z;\tau) = \frac{1}{z^2} + \sum_{\substack{(m,n)\in\mathbb{Z}^2 \\ (m,n)\neq(0,0)}}^{\infty} \left(\frac{1}{(z - m\tau - n)^2} - \frac{1}{(m\tau + n)^2} \right),$$

$$\wp'(z;\tau) = -\frac{2}{z^3} - 2 \sum_{\substack{(m,n)\in\mathbb{Z}^2 \\ (m,n)\neq(0,0)}}^{\infty} \frac{1}{(z - m\tau - n)^3}.$$

For $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$, set $m' = am + cn$, $n' = bm + dn$, $s' = as + ct$ and $t' = bs + dt$ and we have

$$\begin{aligned} \frac{1}{s\gamma\tau + t - m - n\gamma\tau} &= \frac{c\tau + d}{(as + ct)\tau + (bs + dt) - (am + cn)\tau - (bm + dn)} \\ &= \frac{1}{s'\tau + t' - m'\tau - n'}, \\ \frac{1}{m\gamma\tau + n} &= \frac{c\tau + d}{(am + cn)\tau + (bm + dn)} \\ &= \frac{c\tau + d}{m'\tau + n'}, \\ \frac{1}{s\gamma\tau + t} &= \frac{c\tau + d}{s'\tau + t'}. \end{aligned}$$

Since $ad - bc = 1$, (a, c) and (b, d) are pairs of relatively prime integers. Therefore, as

doi:10.6342/NTU202501859

(m,n) runs through $\mathbb{Z}^2\setminus\{(0,0)\}$, (m',n') also runs through $\mathbb{Z}^2\setminus\{(0,0)\}$. Therefore,

$$\begin{aligned}
P_{s,t}(\gamma\tau) &= \frac{1}{(s\gamma\tau+t)^2}+\sum_{\substack{(m,n)\in\mathbb{Z}^2\\(m,n)\neq(0,0)}}^{\infty}\left(\frac{1}{(s\gamma\tau+t-m-n\gamma\tau)^2}-\frac{1}{(m\gamma\tau+n)^2}\right)\\
&= \frac{(c\tau+d)^2}{(s'\tau+t')^2}+\sum_{\substack{(m',n')\in\mathbb{Z}^2\\(m',n')\neq(0,0)}}^{\infty}\left(\frac{(c\tau+d)^2}{(s'\tau+t'-m'-n'\tau)^2}-\frac{(c\tau+d)^2}{(m'\tau+n')^2}\right)\\
&= (c\tau+d)^2P_{s',t'}(\tau),\\
Q_{s,t}(\gamma\tau) &= \frac{-2}{(s\gamma\tau+t)^3}-2\sum_{\substack{(m,n)\in\mathbb{Z}^2\\(m,n)\neq(0,0)}}^{\infty}\frac{1}{(s\gamma\tau+t-m-n\gamma\tau)^3}\\
&= \frac{-2(c\tau+d)^3}{(s'\tau+t')^3}-2\sum_{\substack{(m',n')\in\mathbb{Z}^2\\(m',n')\neq(0,0)}}^{\infty}\frac{(c\tau+d)^3}{(s'\tau+t'-m'-n'\tau)^3}\\
&= (c\tau+d)^3Q_{s',t'}(\tau).
\end{aligned}$$

Therefore,

$$(P_{s,t}|_2\gamma)(\tau)=P_{as+ct,bs+dt}(\tau),\ (Q_{s,t}|_3\gamma)(\tau)=Q_{as+ct,bs+dt}(\tau).$$

□

From this theorem, it can be deduced that for $a\not\equiv 0(\mathrm{mod}\ N)$, $\wp(a/N;\tau)$ and $\wp'(a/N;\tau)$ are modular forms of weight 2 and 3 respectively ([1]). Also, it is easy to see that

$$\begin{aligned}
\wp(a/N;-\frac{1}{N\tau}) &= \tau^2\wp(a\tau;N\tau),\\
\wp'(a/N;-\frac{1}{N\tau}) &= \tau^3\wp(a\tau;N\tau).
\end{aligned}$$

Finally, we write the q-expansion of Weierstrass $\wp$-function $\wp(z;\tau)$ with respect to $\mathbb{Z}+\mathbb{Z}\tau$, $\tau\in\mathbb{H}$, which will be useful later.

doi:10.6342/NTU202501859

Theorem 2.5.2. (Theorem 2.1.11, [2]) Let $\tau \in \mathbb{H}$ and let $q = e^{2\pi i\tau}$. Then,

$$\wp(z;\tau) = (2\pi i)^2 \left(\frac{1}{12} + \frac{e^{2\pi iz}}{(1-e^{2\pi iz})^2} + \sum_{n=1}^{\infty} \left(\frac{q^n e^{2\pi iz}}{(1-q^n e^{2\pi iz})^2} + \frac{q^{-n} e^{2\pi iz}}{(1-q^{-n} e^{2\pi iz})^2} + \frac{2nq^n}{1-q^n} \right) \right),$$

$$\wp'(z;\tau) = (2\pi i)^3 \left(\frac{e^{2\pi iz}(1+e^{2\pi iz})}{(1-e^{2\pi iz})^3} \sum_{n=1}^{\infty} \left(\frac{q^n e^{2\pi iz}(1+q^n e^{2\pi iz})}{(1-q^n e^{2\pi iz})^3} + \frac{q^{-n} e^{2\pi iz}(1+q^{-n} e^{2\pi iz})}{(1-q^{-n} e^{2\pi iz})^3} \right) \right).$$

2.6 Elliptic Function and Jacobi Theta Functions

Here we review the definition of elliptic functions.

Definition. Let Λ be a complex lattice with period ω_1, ω_2. An elliptic function f with respect to λ is a meromorphic function that satisfies

$$f(z+\omega_1) = f(z+\omega_2) = f(z),$$

for all $z \in \mathbb{C}$.

Next we review the properties of elliptic function.

Theorem 2.6.1. (Proposition 2.1.2,[2]) Let f be a nonzero elliptic function with respect to a lattice Λ with period ω_1, ω_2. Let $D = \{s\omega_1 + t\omega_2 : 0 \le s, t < 1\}$.

(a) With multiplicity, f has the same number of poles as the number of zeros in D.

(b) If f is not constant function, then f has at least two poles and at least two zeros, with multiplicity.

Note that (b) implies that a holomorphic elliptic function is necessarily a constant function. A classic example of elliptic functions is the Weierstrass $\wp$-function.

doi:10.6342/NTU202501859

Next we define the Jacobi theta function $\theta_1(z;\tau)$ by

$$\theta_1(z;\tau) = -ie^{\pi iz}q^{1/8}\prod_{m=1}^{\infty}(1-q^m)(1-q^m e^{2\pi iz})(1-q^{m-1}e^{-2\pi iz}), \quad q = e^{2\pi i\tau}.$$

The Jacobi theta function is a holomorphic function with zeros only on $\mathbb{Z}+\mathbb{Z}\tau$. Also, it satisfies the equations

$$\theta_1(z+1;\tau) = -\theta_1(z;\tau),$$

$$\theta_1(z+\tau;\tau) = -e^{2\pi iz}q^{-1/2}\theta_1(z;\tau),$$

$$\theta_1(z+\tau+1;\tau) = e^{2\pi iz}q^{-1/2}\theta_1(z;\tau).$$

Finally, we conclude this section with a theorem about the relation between the Weierstrass $\wp$-function and the Jacobi theta function θ_1.

Theorem 2.6.2. Let $z, w \in \mathbb{C}$ and τ be a complex number with nonzero imaginary part. Then we have

$$\wp(z;\tau) - \wp(w;\tau) = C(\tau)\cdot\frac{\theta_1(z-w;\tau)\cdot\theta_1(z+w;\tau)}{\theta_1(z;\tau)^2\cdot\theta_1(w;\tau)^2},$$

where $C(\tau)$ is a function of τ.

Proof. We only give a brief sketch of the proof. Let

$$F(z;\tau) = \wp(z;\tau) - \wp(w;\tau),\ G(z;\tau) = \frac{\theta_1(z-w;\tau)\cdot\theta_1(z+w;\tau)}{\theta_1(z;\tau)^2\cdot\theta_1^2(w;\tau)}.$$

Fix w and view F and G as functions of z and τ. By the equations of θ_1 above, it is clear that both F and G are elliptic functions with respect to the lattice $\mathbb{Z}+\mathbb{Z}\tau$.

doi:10.6342/NTU202501859

Next, note that the poles of F are $m+n\tau,\ m,n\in\mathbb{Z}$ and the zeros of G are $\pm w+m+n\tau,\ m,n\in\mathbb{Z}$. Using the fact that the zeros of θ_1 are $m+n\tau,\ m,n\in\mathbb{Z}$, the same is true for G. Therefore, F/G is a holomorphic elliptic function with respect to $\mathbb{Z}+\mathbb{Z}\tau$, and thus is a function of τ. Write $C(\tau)=F(z;\tau)/G(z;\tau)$ and we have

$$\wp(z;\tau)-\wp(w;\tau)=C(\tau)\cdot\frac{\theta_1(z-w;\tau)\cdot\theta_1(z+w;\tau)}{\theta_1(z;\tau)^2\cdot\theta_1(w;\tau)^2}.$$

□

Remark. By comparing the coefficients of the Laurent series of both sides, it can be shown that $C(\tau)=-4\pi^2\eta(\tau)^6$, where $\eta(\tau)$ is the Dedekind eta function defined in section 2.7.

2.7 Generalized Dedekind Eta Function

Recall that the Dedekind η-function is defined by

$$\eta(\tau)=q^{1/24}\prod_{m=1}^{\infty}(1-q^m),\quad q=e^{2\pi i\tau}.$$

The generalized Dedekind η-functions $E_{g,h}^{(N)}$ and $E_g^{(N)}$ are defined by

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

for real numbers g and h which are not simultaneously multiples of N and

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

doi:10.6342/NTU202501859

for real number g which is not a multiple of N, where $B(x) = \{x\}^2 - \{x\} + 1/6$, $\{x\} = x - [x]$ and $[x]$ is the largest integer less than x. These functions are useful for constructing modular forms and modular functions.

First we cite a theorem about the transformation of $\eta(\tau)$

Theorem 2.7.1. ([7]) Let $\eta(\tau)$ be the function defined above and let h be a positive integer. Then

$$\eta\left(-\frac{1}{h\tau}\right) = \sqrt{\frac{h\tau}{i}}\eta(h\tau).$$

Theorem 2.7.2. ([7]) Let $E_{g,h}^{(N)}$ and $E_g^{(N)}$ be the functions defined above. Then

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

Also, we have

$$E_{g+N,h}(\tau) = E_{-g,-h}(\tau) = -e^{2\pi ih/N}E_{g,h}(\tau), \quad E_{g,h+N} = E_{g,h}.$$

Furthermore, let

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

If $c = 0$,

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

Otherwise,

$$E_{g,h}(\gamma\tau) = \epsilon e^{\pi i\delta}E_{ag+ch,bg+dh}(\tau)$$

where ϵ and δ are quantities determined by a, b, c, d, g, h.

doi:10.6342/NTU202501859

2.8 Generators for the field of modular functions with respect to $\Gamma_1(N)$

For $N \in \{4, 5, 6, 7, 8, 9, 10, 12\}$, the field of modular functions on $\Gamma_1(N)$ is generated by a single modular function $t(\tau)$ listed below:

N	$t(\tau)$	N	$t(\tau)$
4	$\frac{1}{16}\frac{\eta(\tau)^{16}\eta(4\tau)^8}{\eta(2\tau)^{24}}$	8	$i\frac{E_{0,1}(\tau)^2}{E_{0,3}(\tau)^2}$
5	$-\frac{E_{0,1}(\tau)^5}{E_{0,2}(\tau)^5}$	9	$e^{4\pi i/9}\frac{E_{0,1}(\tau)^2}{E_{0,2}(\tau)E_{0,4}(\tau)}$
6	$\frac{1}{9}\frac{\eta(\tau)^8\eta(6\tau)^4}{\eta(3\tau)^8\eta(2\tau)^4}$	10	$e^{4\pi i/10}\frac{E_{0,1}(\tau)E_{0,2}(\tau)}{E_{0,3}(\tau)E_{0,4}(\tau)}$
7	$e^{4\pi i/7}\frac{E_{0,1}(\tau)^3}{E_{0,2}(\tau)^2E_{0,3}(\tau)}$	12	$e^{4\pi i/12}\frac{E_{0,1}(\tau)}{E_{0,5}(\tau)}$

Table 2.1

doi:10.6342/NTU202501859

For $N \in \{11, 13, 14, 15, 16, 17, 18, 19, 20\}$, the field of modular functions on $\Gamma_1(N)$ is generated by two modular functions defined below. For simplicity, we write $E_{g,h}^k$ to represent $(E_{g,h}^{(N)})^k$.

N	X	Y
11	$e^{8\pi i/11}\frac{E_{0,3}E_{0,4}E_{0,5}}{E_{0,1}^2E_{0,2}}$	$e^{12\pi i/11}\frac{E_{0,4}^3E_{0,5}}{E_{0,1}^3E_{0,2}}-1$
13	$e^{12\pi i/13}\frac{E_{0,4}^2E_{0,5}E_{0,6}}{E_{0,1}^2E_{0,2}E_{0,3}}$	$e^{17\pi i/13}\frac{E_{0,4}E_{0,6}^3}{E_{0,1}^3E_{0,2}}$
14	$e^{8\pi i/14}\frac{E_{0,3}E_{0,4}^2E_{0,7}}{E_{0,1}E_{0,2}^2E_{0,5}}-1$	$e^{12\pi i/14}\frac{E_{0,4}E_{0,5}^2E_{0,6}}{E_{0,1}E_{0,2}^2E_{0,3}}-1$
15	$e^{8\pi i/15}\frac{E_{0,4}E_{0,7}}{E_{0,1}E_{0,2}}-1$	$e^{14\pi i/15}\frac{E_{0,4}E_{0,5}E_{0,6}^2}{E_{0,1}E_{0,2}E_{0,3}^2}-1$
16	$e^{3\pi i/4}\frac{E_{0,5}E_{0,6}E_{0,7}}{E_{0,1}E_{0,2}E_{0,3}}-1$	$e^{9\pi i/8}\frac{E_{0,4}E_{0,7}^2E_{0,8}}{E_{0,1}E_{0,2}^2E_{0,3}}+1$
17	$e^{20\pi i/17}\frac{E_{0,6}^2E_{0,7}E_{0,8}}{E_{0,1}^2E_{0,2}E_{0,3}}$	$e^{28\pi i/17}\frac{E_{0,6}^2E_{0,7}E_{0,8}^2}{E_{0,1}^3E_{0,2}^2}$
18	$e^{2\pi i/3}\frac{E_{0,4}E_{0,5}E_{0,9}}{E_{0,1}E_{0,2}E_{0,3}}$	$e^{8\pi i/9}\frac{E_{0,5}E_{0,6}E_{0,7}E_{0,8}}{E_{0,1}E_{0,2}E_{0,3}E_{0,4}}-1$
19	$e^{25\pi i/19}\frac{E_{0,6}E_{0,8}E_{0,9}^2}{E_{0,1}^2E_{0,2}E_{0,3}}+1$	$e^{44\pi i/19}\frac{E_{0,4}E_{0,6}^2E_{0,7}^2E_{0,8}^2E_{0,9}^2}{E_{0,1}^3E_{0,2}^3E_{0,3}^2E_{0,5}}$
20	$e^{4\pi i/5}\frac{E_{0,6}E_{0,8}E_{0,9}}{E_{0,1}E_{0,2}E_{0,4}}$	$e^{11\pi i/10}\frac{E_{0,5}E_{0,8}E_{0,9}E_{0,10}}{E_{0,1}E_{0,2}E_{0,3}E_{0,4}}+1$

Table 2.2

doi:10.6342/NTU202501859

Here we also show a table of equations satisfied by X and Y defined above.

N	equation
11	$Y^2 + Y = X^3 - X^2$
13	$Y^3 - (X-1)Y^2 - XY = X^4 + X^3$
14	$Y^2 + XY + Y = X^3 - X$
15	$Y^2 + XY + Y = X^3 + X^2$
16	$Y^3 + (X-1)Y^2 - X^2Y = X^4 - X^3$
17	$Y^5 - (4X-1)Y^4 + (6X^2-3X)Y^3$ $-(X^4+4X^3-5X^2+X)Y^2$ $+X^3(4X-1)(X-1)Y$ $= X^6(X-1)$
18	$Y^3 + XY^2 + (2X^2-2X)Y$ $= X^4 - 3X^3 + 2X^2$
19	$Y^6 - (5X-3)Y^5$ $-(3X^3-15X^2+14X-3)Y^4$ $+(X-1)(9X^4-18X^3+7X^2-1)Y^3$ $-X^2(X-1)(9X^4-20X^3+13X^2-X-2)Y$ $= X^7(X-1)^4$
20	$Y^4 + XY^3 + X(2X-3)Y^2 - X(2X^2-1)Y$ $-X(2X^2-1)Y = X^4(X-1)$

Table 2.3

doi:10.6342/NTU202501859

Note that $\begin{pmatrix} 0 & 1 \\ N & 0 \end{pmatrix}$ normalizes the group $\Gamma_1(N)$. Therefore, if f is a modular function on $\Gamma_1(N)$, then so is $f|_0 \begin{pmatrix} 0 & 1 \\ N & 0 \end{pmatrix}$. The generators listed in Table 2.1 and 2.2 hold the following properties:

(a) The set of generators under the slash operator of weight 0 of $\begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix}$ is still a set of generators.

(b) The quotient of η -functions (generalized η -functions, respectively) under the slash operator of weight 0 of $\begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix}$ is again a quotient of η -functions (generalized η -functions, respectively).

(c) For $N \in \{11, 13, 15, 17, 18, 19, 20\}$, the poles of the generators are at ∞.

Remark. For $4 \leq N \leq 20$ with $N \neq 4, 6$, we choose $E_{0,g}$ instead of E_g so that the cusp corresponding to 0 is $\mathbb{Q}$-rational in the model of $X_1(N)$ given by $\tau \mapsto (X(\tau), Y(\tau))$.

For $N \in \{4, 5, 6, 7, 8, 9, 10, 12\}$, the result can be found in [7].

For $N \in \{11, 13, 14, 15, 16, 17, 18, 19, 20\}$, the result can be found in [8].

doi:10.6342/NTU202501859

Chapter 3

Main Result

Let $N \geq 4$. Recall that in theorem 2.2.2, the function f and g on $\mathbb{H}$ are defined as

$$f(\tau) = \frac{(\wp(1/N;\tau) - \wp(2/N;\tau))^3}{\wp'(1/N;\tau)^2},$$
$$g(\tau) = \frac{\wp'(2/N;\tau)}{\wp'(1/N;\tau)}.$$

which are modular functions on $\Gamma_1(N)$. Our aim is to write f and g in terms of t (or X, Y) for $4 \leq N \leq 20$.

3.1 The order at cusps of f and g

To calculate the order at cusps of f and g, we first write f and g as products of generalized Dedekind eta functions. For simplicity, we write $E_{g,h}$ and E_g instead of $E_{g,h}^{(N)}$ and $E_g^{(N)}$. Let a, b be two real numbers not a multiple of N and let τ be a complex number with nonzero imaginary part. Set $q = e^{2\pi i\tau}$. By direct computation,

doi:10.6342/NTU202501859

we have

$$\theta_1(-\frac{a\tau+b}{N};\tau) = -ie^{-\pi ib/N}q^{a^2/2N^2}\eta(\tau)E_{a,b}(\tau),$$

where θ_1 is the Jacobi theta function defined in Section 2.5, η is the Dedekind eta function, and $E_{a,b}$ is the generalized Dedekind eta function. Thus, by Theorem 2.6.2 and the fact that $E_{-a,-b}(\tau) = -e^{-2\pi ib/N}E_{a,b}(\tau)$, we have

$$\begin{aligned}\wp(1/N;\tau) - \wp(2/N;\tau) &= C\eta(\tau)^4\frac{E_{0,1}(\tau)E_{0,3}(\tau)}{E_{0,1}(\tau)^2E_{0,2}(\tau)^2}\\ &= C\eta(\tau)^4\frac{E_{0,3}(\tau)}{E_{0,1}(\tau)E_{0,2}(\tau)^2},\end{aligned}$$

for some constant C. By equation (2.2) in chapter 2 and Theorem 2.6.2,

$$\begin{aligned}&\wp'(a/N;\tau)^2\\ &= 4(\wp(a/N;\tau) - \wp(1/2;\tau))(\wp(a/N;\tau) - \wp(\tau/2;\tau))(\wp(a/N;\tau) - \wp((\tau+1)/2;\tau))\\ &= C'\eta(\tau)^{12}\frac{E_{0,-a+N/2}(\tau)E_{0,a+N/2}(\tau)}{E_{0,a}(\tau)^2E_{0,N/2}(\tau)^2}\frac{E_{N/2,a}(\tau)E_{N/2,-a}(\tau)}{E_{0,a}(\tau)^2E_{N/2,0}(\tau)^2}\frac{E_{N/2,-a+N/2}(\tau)E_{N/2,a+N/2}(\tau)}{E_{0,a}(\tau)^2E_{N/2,N/2}(\tau)^2}\\ &= C''\eta(\tau)^{12}\frac{E_{0,a+N/2}(\tau)^2E_{N/2,a}(\tau)^2E_{N/2,a+N/2}(\tau)^2}{E_{0,a}(\tau)^6E_{0,N/2}(\tau)^2E_{N/2,0}(\tau)^2E_{N/2,N/2}(\tau)^2},\end{aligned}$$

for some constant C' and C''. Note that

$$\begin{aligned}E_{0,N/2}(\tau) &= 2q^{1/12}\prod_{m=1}^{\infty}(1+q^m)^2,\\ E_{N/2,N/2}(\tau) &= q^{-1/24}\prod_{m=1}^{\infty}(1+q^{m-1/2})^2,\\ E_{N/2,0}(\tau) &= q^{-1/24}\prod_{m=1}^{\infty}(1-q^{m-1/2})^2.\end{aligned}$$

doi:10.6342/NTU202501859

Therefore,

$$E_{N/2,N/2}(\tau)E_{N/2,0}(\tau) = q^{-1/12}\prod_{m=1}^{\infty}(1-q^{2m-1})^2$$
$$= q^{-1/12}\prod_{m=1}^{\infty}\frac{(1-q^m)^2}{(1-q^{2m})^2}.$$

Also,

$$E_{0,N/2}(\tau) = 2q^{1/12}\prod_{m=1}^{\infty}\frac{(1-q^{2m})^2}{(1-q^m)^2}.$$

Therefore, $E_{0,N/2}(\tau)E_{N/2,N/2}(\tau)E_{N/2,0}(\tau) = 2$.

Hence,

$$\wp'(a/N;\tau)^2 = C'''\eta(\tau)^{12}\frac{E_{0,a+N/2}(\tau)^2E_{N/2,a}(\tau)^2E_{N/2,a+N/2}(\tau)^2}{E_{0,a}(\tau)^6},$$

where $C''' = C''/2$. Note that

$$E_{0,a+N/2}(\tau) = (1+e^{2\pi ia/N})q^{1/12}\prod_{m=1}^{\infty}(1+e^{2\pi ia/N}q^m)(1+e^{-2\pi ia/N}q^m),$$
$$E_{N/2,a+N/2}(\tau) = q^{-1/24}\prod_{m=1}^{\infty}(1+e^{2\pi ia/N}q^{m-1/2})(1+e^{-2\pi ia/N}q^{m-1/2}),$$
$$E_{N/2,a}(\tau) = q^{-1/24}\prod_{m=1}^{\infty}(1-e^{2\pi ia/N}q^{m-1/2})(1-e^{2\pi ia/N}q^{m-1/2}).$$

Therefore,

$$E_{N/2,a+N/2}(\tau)E_{N/2,a}(\tau) = q^{-1/12}\prod_{m=1}^{\infty}(1-e^{4\pi ia/N}q^{2m-1})(1-e^{-4\pi ia/N}q^{2m-1}),$$

and

$$E_{0,a+N/2}(\tau) = (1+e^{2\pi ia/N})q^{1/12}\prod_{m=1}^{\infty}\frac{(1-e^{4\pi ia/N}q^{2m})(1-e^{-4\pi ia/N}q^{2m})}{(1-e^{2\pi ia/N}q^m)(1-e^{-2\pi ia/N}q^m)}.$$

doi:10.6342/NTU202501859

Hence, if $2a$ is not a multiple of N,

$$\begin{aligned}
&E_{0,a+N/2}(\tau)E_{N/2,a+N/2}(\tau)E_{N/2,a}(\tau)\\
&= (1+e^{2\pi ia/N})\prod_{m=1}^{\infty}\frac{(1-e^{4\pi ia/N}q^m)(1-e^{-4\pi ia/N}q^m)}{(1-e^{2\pi ia/N}q^m)(1-e^{-2\pi ia/N}q^m)}\\
&= (1+e^{2\pi ia/N})\frac{E_{0,2a}(\tau)}{E_{0,a}(\tau)},
\end{aligned}$$

and we have

$$\wp'(a/N;\tau)^2 = C^*\eta(\tau)^{12}\frac{E_{0,2a}(\tau)^2}{E_{0,a}(\tau)^8},$$

and

$$\wp'(a/N;\tau)^2 = D\eta(\tau)^{12}\frac{E_{0,2a}(\tau)}{E_{0,a}(\tau)^4},$$

where $C^* = (1+e^{2\pi ia/N})C'''$ and $D = \sqrt{C^*}$. Combining all the results, we have

$$\begin{aligned}
f(\tau) &= \frac{(\wp(1/N;\tau)-\wp(2/N;\tau))^3}{\wp'(1/N;\tau)^2}\\
&= D'\frac{E_{0,3}(\tau)^3E_{0,1}(\tau)^5}{E_{0,2}(\tau)^8},
\end{aligned}$$

and

$$\begin{aligned}
g(\tau) &= \frac{\wp'(2/N;\tau)}{\wp'(1/N;\tau)}\\
&= D''\frac{E_{0,4}(\tau)E_{0,1}(\tau)^4}{E_{0,2}(\tau)^5},
\end{aligned}$$

for some quantities D', D'' determined by N.

With this expression, we may now calculate the order at cusps of f and g. Let a/c be a cusp of $\Gamma_1(N)$ written in the lowest terms. Then there is $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ such that $\gamma\infty = a/c$. Let g, h be two real numbers that are not simultaneously the

doi:10.6342/NTU202501859

multiples of N. By Theorem 2.7.2, $E_{g,h}(\gamma\tau) = \epsilon e^{2\pi i\delta} E_{ag+ch,bg+dh}$, where ϵ and ϵ are quantities determined by a, b, c, d, g, h. Again by Theorem 2.7.2, the lowest exponent of the q-expansions of $E_{ag+ch,bg+dh}$ is $\frac{1}{2}B(ag+ch)$, where $B(x) = \{x\}^2 - \{x\} + 1/6$, $\{x\} = x - [x]$, and $[x]$ is the greatest integer lower than x. By Theorem 2.3.3, the width of a/c is $N/\gcd(c, N)$ if $N \geq 5$. Therefore, denote the order of f and g at the cusp a/c by $\mathrm{ord}_{a/c} f$ and $\mathrm{ord}_{a/c} g$ and for $N \geq 5$, we have

$$\mathrm{ord}_{a/c} f = \frac{N}{2\gcd(c,N)}[3B(\frac{3c}{N}) + 5B(\frac{c}{N}) - 8B(\frac{2c}{N})],$$
$$\mathrm{ord}_{a/c} g = \frac{N}{2\gcd(c,N)}[B(\frac{4c}{N}) + 4B(\frac{c}{N}) - 5B(\frac{2c}{N})].$$

Finally, we conclude this section with a table of the order of f and g at $\Gamma_1(N)$-inequivalent cusps for $4 \leq N \leq 20$.

N	cusps	$\mathrm{ord}_{a/c} f$	$\mathrm{ord}_{a/c} g$
4	0	1	∞
	1/2	-1	∞
	∞	0	∞
5	0	1	1
	2/5	0	0
	1/2	-1	-1
	∞	0	0
6	0	1	1
	1/3	-2	-1
	1/2	1	0
	∞	0	0
7	0	1	1
	2/7	0	0
	1/3	-3	-2
	3/7	0	0
	1/2	2	1
	∞	0	0
8	0	1	1
	1/4	-2	-1
	1/3	0	-1
	3/8	0	0
	1/2	1	1

Table 3.1

doi:10.6342/NTU202501859

N	cusps	$\mathrm{ord}_{a/c} f$	$\mathrm{ord}_{a/c} g$
8	∞	0	0
9	0	1	1
	2/9	0	0
	1/4	-5	-3
	1/3	1	0
	4/9	0	0
	1/2	2	2
	2/3	1	0
	∞	0	0
10	0	1	1
	1/5	-2	-1
	1/4	-1	-1
	3/10	0	0
	1/3	3	1
	2/5	-2	-1
	1/2	1	1
	∞	0	0
11	0	1	1
	2/11	0	0
	1/5	-7	-4
	1/4	1	-1
	3/11	0	0
	1/3	3	2
	4/11	0	0
	5/11	0	0
	1/2	2	2
	∞	0	0
12	0	1	1
	1/6	-2	-1
	1/5	-4	-3
	1/4	1	0
	1/3	1	1
	5/12	0	0
	2/3	1	1
	3/4	1	0
	1/2	2	2
	∞	0	0
13	0	1	1
	2/13	0	0
	1/6	-9	-5
	1/5	-1	-2
	3/13	0	0
	1/4	4	1
	4/13	0	0
	1/3	3	3
	5/13	0	0

N	cusps	$\mathrm{ord}_{a/c} f$	$\mathrm{ord}_{a/c} g$
13	6/13	0	0
	1/2	2	2
	∞	0	0
14	0	1	1
	1/7	-2	-1
	1/6	-3	-2
	1/5	2	-1
	3/14	0	0
	1/4	2	1
	2/7	-2	-1
	1/3	3	3
	5/14	0	0
	3/7	-2	-1
	1/2	1	1
	∞	0	0
15	0	1	1
	2/15	0	0
	1/7	-11	-6
	1/6	-1	-1
	1/5	1	0
	1/4	4	3
	4/15	0	0
	1/3	1	1
	2/5	1	0
	7/15	0	0
	1/2	2	2
	3/5	1	0
	2/3	1	1
	4/5	1	0
	5/6	-1	-1
	∞	0	0
16	0	1	1
	1/8	-2	-1
	1/7	-8	-5
	1/6	0	-1
	3/16	0	0
	1/5	5	1
	1/4	1	1
	5/16	0	0
	1/3	3	3
	3/8	-2	-1
	7/16	0	0
	1/2	1	1
	3/4	1	1
	∞	0	0
17	0	1	1

Table 3.2

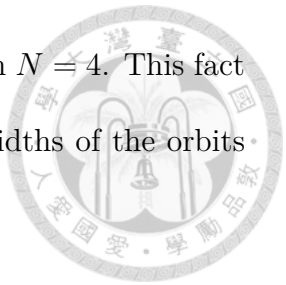
doi:10.6342/NTU202501859

N	cusps a/c	$\mathrm{ord}_{a/c}\, f$	$\mathrm{ord}_{a/c}\, g$
17	2/17	0	0
	1/8	−13	−7
	1/7	−5	−4
	1/6	3	−1
	3/17	0	0
	1/5	5	2
	4/17	0	0
	1/4	4	4
	5/17	0	0
	1/3	3	3
	6/17	0	0
	7/17	0	0
	8/17	0	0
	1/2	2	2
	∞	0	0
18	0	1	1
	1/9	−2	−1
	1/8	−5	−3
	1/7	−2	−3
	1/6	1	0
	1/5	5	3
	2/9	−2	−1
	1/4	2	2
	5/18	0	0
	1/3	1	1
	7/18	0	0
	4/9	−2	−1
	1/2	1	1
	2/3	1	1
	5/6	1	0
	∞	0	0
19	0	1	1
	2/19	0	0
	1/9	−15	−8
	1/7	−7	−5
	1/7	1	−2
	3/19	0	0
	1/6	6	1
	1/5	5	4
	4/19	0	0
	1/4	4	4
	5/19	0	0
	6/19	0	0
	1/3	3	3

N	cusps a/c	$\mathrm{ord}_{a/c}\, f$	$\mathrm{ord}_{a/c}\, g$
19	7/19	0	0
	8/19	0	0
	9/19	0	0
	1/2	2	2
	∞	0	0
20	0	1	1
	1/10	−2	−1
	1/9	−12	−7
	1/8	−1	−1
	1/7	4	−1
	3/20	0	0
	1/6	3	1
	1/5	1	1
	1/4	1	1
	3/10	−2	−1
	1/3	3	3
	7/20	0	0
	3/8	−1	−1
	2/5	1	1
	9/20	0	0
	1/2	1	1
	3/5	1	1
	3/4	1	1
	4/5	1	1
	∞	0	0

Table 3.3

doi:10.6342/NTU202501859



Remark. For $N = 4$, $g \equiv 0$ when $N = 4$, the order of g is ∞ when $N = 4$. This fact can be proved using Corollary 2.4.1.2. By Theorem 2.3.3, the widths of the orbits [0], [1/2] and [∞] are 4,1 and 1. Therefore,

$$\begin{aligned} ord_0 f &= \frac{4}{2}[3B(\frac{3}{4}) + 5B(\frac{1}{4}) - 8B(\frac{2}{4})] = 1, \\ ord_{1/2} f &= \frac{1}{2}[3B(\frac{3\cdot 2}{4}) + 5B(\frac{2}{4}) - 8B(\frac{2\cdot 2}{4})] = -1, \\ ord_\infty f &= 0. \end{aligned}$$

3.2 A representation of f and g in terms of generators

The problem divides into two cases.

1. The first case is for $N \in \{4, 5, 6, 7, 8, 9, 10, 12\}$. In this case, the field of modular functions can be generated by one modular function t.

2. The second case is for $N \in \{11, 13, 14, 15, 16, 17, 18, 19, 20\}$. In this case, the field of modular functions can be generated by one modular function X, Y.

We describe our method by giving an example for each case.

Example 1. ($N = 7$) Set

$$\begin{aligned} F(\tau) &= \left(f|_0 \begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix} \right)(\tau) = f\left(-\frac{1}{N\tau}\right) = \frac{(\wp(\tau; N\tau) - \wp(2\tau; N\tau))^3}{\wp'(\tau; N\tau)}, \\ G(\tau) &= \left(g|_0 \begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix} \right)(\tau) = g\left(-\frac{1}{N\tau}\right) = \frac{\wp'(2\tau; N\tau)}{\wp'(\tau; N\tau)}. \end{aligned}$$

The final equality is due to Theorem 2.5.1. Write $T(\tau) = t(-\frac{1}{N\tau})$. By Theorem

doi:10.6342/NTU202501859

2.7.2, we have

$$T(\tau) = \frac{E_1(\tau)^3}{E_2(\tau)^2 E_3(\tau)}.$$

Note that $T(\tau)$ is still a generator of $\Gamma_1(N)$ and we have

$$F(\tau) = \frac{P(T(\tau))}{Q(T(\tau))},\ G(\tau) = \frac{R(T(\tau))}{S(T(\tau))},$$

for some polynomial P, Q, R, S in one variable with complex coefficients. We can further rewrite it as

$$Q(T(\tau))(\wp(\tau; N\tau) - \wp(2\tau; N\tau))^3 - P(T(\tau))\wp'(\tau; N\tau)^2 = 0, \tag{3.1}$$

and

$$S(T(\tau))\wp'(2\tau; N\tau) - R(T(\tau))\wp'(\tau; N\tau) = 0. \tag{3.2}$$

For the first equation above, assume that

$$P(x) = \sum_{n=0}^{m} a_n x^n,\ Q(x) = \sum_{n=0}^{m} b_n x^n,$$

for some $a_0, \cdots, a_n, b_0, \cdots, b_n \in \mathbb{C}$. Note that the equation has a solution $a_0, \ldots, a_n, b_0, \ldots, b_n$ not all zero when n is large enough. In this case, we set $m = 3$. By calculating the q-expansion of the left-hand side (For q-expansion of $\wp$-function, see Theorem 2.5.2; For q-expansion for $E_g^{(N)}$, see Section 2.7.),

doi:10.6342/NTU202501859

$$a_0q^2+(-b_0+8a_0+a_1)q^3+(-3b_0-b_1+34a_0+5a_1+a_2)q^4$$
$$+(-12b_0-b_2+104a_0+15a_1+2a_2+a_3)q^5$$
$$+(-25b_0-8b_1+3b_2-b_3+259a_0+36a_1+5a_2-a_3)q^6$$
$$+(-60b_0+2b_1-13b_2+6b_3+558a_0+76a_1+10a_2+4a_3)q^7$$
$$+(-105b_0-34b_1+35b_2-27b_3+1084a_0+146a_1+20a_2-a_3)q^8$$
$$+(-204b_0+8b_1-87b_2+92b_3+1952a_0+266a_1+36a_2+10a_3)q^9+\cdots=0.$$

Therefore, by solving the system of linear equations

$$\begin{cases} a_0 & =0 \\ -b_0+8a_0+a_1 & =0 \\ -3b_0-b_1+34a_0+5a_1+a_2 & =0 \\ -12b_0-b_2+104a_0+15a_1+2a_2+a_3 & =0 \\ -25b_0-8b_1+3b_2-b_3+259a_0+36a_1+5a_2-a_3 & =0 \\ -60b_0+2b_1-13b_2+6b_3+558a_0+76a_1+10a_2+4a_3 & =0 \\ -105b_0-34b_1+35b_2-27b_3+1084a_0+146a_1+20a_2-a_3 & =0 \\ -204b_0+8b_1-87b_2+92b_3+1952a_0+266a_1+36a_2+10a_3 & =0 \end{cases}$$

we have

$$a_0=0,\ a_1=b_0,\ a_2=-2b_0,\ a_3=b_0,\ b_0=b_0,\ b_1=0,\ b_2=0,\ b_3=0.$$

Note that the left-hand side of equations (5.1) and (5.2) are modular forms of weight

doi:10.6342/NTU202501859

6 and 3 respectively. By applying this solution to the equation and checking the coefficients of q^k are zeros for $0 \leq k \leq 13$, by Corollary 2.3.1.2, $F = T - 2T^2 + T^3 = T(1-T)^2$. By similar way, we have $G = T - T^2 = T(T-1)$. Finally, note that

$$f(\tau) = F(-\frac{1}{N\tau}),\ g(\tau) = G(-\frac{1}{N\tau}),\ T(-\frac{1}{N\tau}) = t(\tau).$$

Therefore, $f = t(1-t)^2$ and $g = t(1-t)$.

Example 2. ($N = 11$) Define F and G the same way as in Example 1, and define $x(\tau)$ and $y(\tau)$ by

$$x(\tau) = X(-\frac{1}{N\tau}) = \frac{E_3(\tau)E_4(\tau)E_5(\tau)}{E_1(\tau)^2E_2(\tau)},$$
$$y(\tau) = Y(-\frac{1}{N\tau}) = \frac{E_4^3(\tau)E_5(\tau)}{E_1(\tau)^3E_2(\tau)} - 1,$$

by Theorem 2.7.2. Then, x and y generate the field of modular functions on $\Gamma_1(N)$ and satisfy the equation

$$y^2 + y = x^3 - x^2, \tag{3.3}$$

in Table 2.3. Again, F and G can be written as

$$F(\tau) = \frac{P(x(\tau), y(\tau))}{Q(x(\tau), y(\tau))},\ G(\tau) = \frac{R(x(\tau), y(\tau))}{S(x(\tau), y(\tau))},$$

for some polynomials P, Q, R, S in two variables with complex coefficients. These can further be rewritten as

$$Q(x(\tau), y(\tau))(\wp(\tau; N\tau) - \wp(2\tau; N\tau))^3 - P(x(\tau), y(\tau))\wp'(\tau; N\tau) = 0, \tag{3.4}$$

doi:10.6342/NTU202501859

and

$$S(x(\tau), y(\tau))\wp'(2\tau; N\tau) - R(x(\tau), y(\tau))\wp'(\tau; N\tau) = 0. \tag{3.5}$$

By equation (5.3), we may assume that the degree of y is smaller than 2 in P, Q, R, S. In this case, we may assume that

$$R(x, y) = a_0 + a_1x + a_2y + a_3x^2 + a_4xy + a_5x^3,$$

$$S(x, y) = b_0 + b_1x + b_2y + b_3x^2 + b_4xy + b_5x^3.$$

Note that the terms in R and S are sorted by the smallest degree k of q^k in the q-expansion of $x(\tau)^m y(\tau)^n$, $m, n \in \mathbb{N} \cup \{0\}$. Then by similar method in Example 1, we have

$$a_0 = 0, a_1 = b_5, a_2 = 0, a_3 = -b_5, a_4 = b_5, a_5 = 0,$$

$$b_0 = 0, b_1 = 0, b_2 = 0, b_3 = b_5, b_4 = 2b_5, b_5 = b_5.$$

Since $x^3 + 2xy - y \equiv (x + y)^2 (\text{mod } y^2 + y - x^3 + x^2)$ (Note that this is just for simplification), we have

$$G = -\frac{x(x - y - 1)}{(x + y)^2},$$

From Table 3.2 and 3.3, observe that for $N \in \{11, 13, 14, 15, 16, 17, 18, 19, 20\}$, f and g don't have poles at ∞ and whenever f and g have poles at a cusp a/c, $\text{ord}_{a/c} f \geq 2\,\text{ord}_{a/c} g$. Since X and Y has only poles at ∞, $S(X(\tau), Y(\tau))$ has zeros of order more than $-\text{ord}_{a/c} g$ at a/c. Therefore, $S(X(\tau), Y(\tau))^2 \cdot F$ is a modular function with no poles at cusps except ∞. Hence, we may assume that $Q(x, y) = S(x, y)^2$. By similar method, we have

$$F = \frac{x^3 y(x - 1)}{(x + y)^4}.$$

doi:10.6342/NTU202501859

By $\tau \mapsto -\frac{1}{N\tau}$, we have

$$f = \frac{X^3Y(X-1)}{(X+Y)^4},$$

$$g = -\frac{X(X-Y-1)}{(X+Y)^2}.$$

3.3 Table of Results

Finally, we conclude this chapter with tables of f and g writing in terms of t (or X and Y respectively). For $N \in \{4, 5, 6, 7, 8, 9, 10, 12\}$,

N	f	g
4	t	0
5	t	t
6	$t - t^2$	t
7	$t(1-t)^2$	$t - t^2$
8	$\frac{t(1-t)}{(t+1)^2}$	$\frac{t(1-t)}{t+1}$
9	$t(1-t)^2(1-t+t^2)$	$t(1-t)^2$
10	$\frac{t(1-t)}{(1+t)(1+t-t^2)^2}$	$\frac{t(1-t)}{(1+t)(1+t-t^2)}$
12	$\frac{t(1-t)(1-t+t^2)(1+t^2)}{(1+t)^2}$	$\frac{t(1-t)(1-t+t^2)}{1+t}$

Table 3.4

For $N \in \{11, 13, 14, 15, 16, 17, 18, 19, 20\}$, for simplicity, we break f and g into three polynomial $P, Q, R \in \mathbb{Z}[x, y]$ such that

$$f = \frac{P(X,Y)}{R(X,Y)^2},\ g = \frac{Q(X,Y)}{R(X,Y)}.$$

doi:10.6342/NTU202501859

N	$P(X,Y)$	$Q(X,Y)$
11	$X^3Y(X-1)$	$-X(X-Y-1)$
13	$-X(X-1)$ $\cdot(X^3-2X^2+Y^2+X+Y)$	$-X(X-Y-1)$
14	$X^3(X^3+X^2Y-X-Y)$	$X(X^2-Y-1)$
15	$(X^2+X+1)(X+1)^2X^2$ $\cdot(X^2+XY+X+Y+1)$	$X(X+1)(X^2+X-Y)$
16	$(X-1)^2$ $\cdot\big[X^4-X^3Y+(2Y-1)X^2$ $-XY^2-Y^2+Y\big]$	$X^3-X^2+XY-2Y^2+Y$
17	$X(X-1)$ $\cdot\big[X^9-X^8+(-4Y+1)X^7$ $+(-Y^2+5Y-1)X^6+(6Y^2-5Y)X^5$ $+(-5Y^2+5Y)X^4+(Y^4+5Y^2-Y)X^3$ $+(-3Y^4-5Y^3-5Y^2)X^2$ $+(4Y^4+3Y^3+Y^2)X-Y^4\big]$	$-2X^5+(-Y+3)X^4$ $+(4Y-1)X^3+(-3Y-4Y)X^2$ $+(2Y^3+2Y^2+Y)X-Y^3$
18	$X(X-2)(X-1)^3$ $\cdot(X+Y)(X^2-X-Y)$	X $\cdot\big[X^3-3X^2+(-Y+2)X$ $-Y^2+Y\big]$
19	$(X-1)^4X^2$ $\cdot\big[X^{10}+(-Y-2)X^9-X^8+$ $(5Y^2+Y+5)X^7$ $+2(-4Y^2+3Y+2)X^6$ $+(-11Y^3+5Y^2-12Y+1)X^5$ $+(19Y^3-9Y^2+6Y)X^4$ $+(12y^4-7Y^3+11Y^2+Y)X^3$ $+(-Y^5-18Y^4+3Y^3-5Y^2-Y)X^2$ $+(-2Y^5-Y^4-Y^2)X$ $+5Y^5+3Y^4-Y^3+Y^2\big]$	$(X-1)Y$ $\cdot\big[X^5-X^4-3X^3Y$ $+(Y^2+2Y)X^2$ $+(2Y^2+2Y)X-Y(Y+1)^2\big]$
20	$(X-1)X^2$ $\cdot\big[2X^6+2(Y-1)X^5+(2Y^2+Y+1)X^4$ $+(Y-1)(Y^2+1)X^3+2(Y^3-Y^2+Y)X^2$ $-2Y(Y-1)^2X-Y^2(Y-1)\big]$	$(Y-1)(X^3+XY^2-Y^2+Y)$

Table 3.5

doi:10.6342/NTU202501859

N	$R(X,Y)$
11	$(X+Y)^2$
13	$(X+Y)^2$
14	$3X^3+X^2Y+(Y-1)X-Y$
15	$3X^4+X^3Y+6X^3$ $+3X^2Y+6X^2$ $+2XY+3X+Y+1$
16	$(2X+Y-1)(X^2-X-Y+1)$
17	$(-Y-1+2X)$ $\cdot(X^4-X^2Y-2XY^2+Y^3+Y^2)$
18	$3X^4+(Y-9)X^3$ $+(-5Y+8)X^2$ $+(Y^2+7Y-2)X-2Y$
19	$4X^8-17X^7+(-10Y+29)X^6$ $+(-Y^2+34Y-25)X^5$ $+(15Y^2-43Y+11)X^4$ $+(-2Y^3-42Y^2+23Y+2)X^3$ $+(11Y^3+45Y^2-2Y)X^2$ $+(-2Y^4-11Y^3-20Y^2-3Y)X+Y(Y+1)^3$
20	$X^5-X^4+(5Y-1)X^3$ $+(4Y^2-8Y+2)X^2$ $+(3Y^3-3Y^2+4Y-1)X-Y^2$

Table 3.6

doi:10.6342/NTU202501859

doi:10.6342/NTU202501859

References

[1] H. Baaziz. Equations for the modular curve $X_1(N)$ and models of elliptic curves with torsion points. MATHEMATICS OF COMPUTATION, 79(272): 2371–2386, 2010.

[2] H. Cohen and F. Strömberg. Modular Form: A Classical Approach, volume 179 of Graduate Studies in Mathematics. American Mathematical Society, Providence, RI, 2017.

[3] P. Deligne and M. Rapoport. Les schémas de modules de courbes elliptiques. In P. Deligne and W. Kuijk, editors, Modular Functions of One Variable II, pages 143–316, Berlin, Heidelberg, 1973. Springer Berlin Heidelberg. ISBN 978-3-540-37855-6.

[4] J. S. Fred Diamond. A First Course in Modular Forms. Springer New York, NY, 2010.

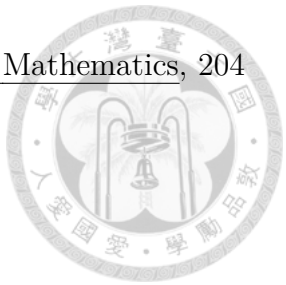
[5] T. Miyake. Modular Forms. Springer Berlin, Heidelberg, 2005.

[6] J. H. Silverman. The Arithmetic of Elliptic Curves. Springer New York, NY, 2nd edition, 2009.

[7] Y. Yang. Transformation formulas for generalized dedekind eta functions. Bulletin of the London Mathematical Society, 36(5):671–682, 2004.

doi:10.6342/NTU202501859

[8] Y. Yang. Defining equations of modular curves. Advances in Mathematics, 204 (2):481–508, 2006. ISSN 0001-8708.



doi:10.6342/NTU202501859