國立交通大學

應用數學系

博 士 論 文

Cuspidal Q-rational Torsion Subgroups of Jacobians of Modular Curves

Cuspidal Q-rational Torsion Subgroups of Jacobians of Modular Curves

研 究 生：陳耀漢

指導教授：楊一帆　教授

中 華 民 國 九十九年 九 月

Cuspidal Q-rational Torsion Subgroups of Jacobians of Modular Curves

Cuspidal Q-rational Torsion Subgroups of Jacobians of Modular Curves

研 究 生：陳耀漢　　Student: YaoHan Chen
指導教授：楊一帆　　Advisor: Yifan Yang

國 立 交 通 大 學
應用數學系
博 士 論 文

A Thesis
Submitted to Department of Applied Mathematics
College of Science
National Chiao Tung University
in partial Fulfillment of the Requirements
for the Degree of
Doctor of Philosophy
in
Applied Mathematics

September 2010

Hsinchu, Taiwan, Republic of China

中華民國九十九年九月

Cuspidal Q-rational Torsion Subgroups of Jacobians of Modular Curves

研究生：陳耀漢　　**指導教授：楊一帆教授**

國 立 交 通 大 學

應 用 數 學 系

摘要

對於p是一個大於3的質數並且r是一個正整數，讓Γ是一個介於$\Gamma_1(p^r)$和$\Gamma_0(p^r)$之間的congruence subgroup。在這篇論文中，我們給予 the group of modular units on X(Γ) that have divisors defined over Q 一個明確的basis。然後應用此結果去決定 the order of the cuspidal Q-rational torsion subgroup of J(Γ) generated by the divisor classes of cuspidal divisors of degree 0 defined over Q 當 Γ 是 $\Gamma_0(p^r)$或 $\Gamma_1(p^r)$ 。

Cuspidal Q-rational Torsion Subgroups of Jacobians of Modular Curves

Student：YaoHan Chen **Advisor：Prof. Yifan Yang**

Department of Applied Mathematics

National Chiao Tung University

Abstract

For $p > 3$ an odd prime and $r > 0$, let Γ be a congruence subgroup between $\Gamma_1(p^r)$ and $\Gamma_0(p^r)$. In this dissertation, we give an explicit basis for the group of modular units on $X(\Gamma)$ that have divisors defined over $\mathbb{Q}$. As an application, we determine the order of the cuspidal $\mathbb{Q}$-rational torsion subgroup of $J(\Gamma)$ generated by the divisor classes of cuspidal divisors of degree 0 defined over $\mathbb{Q}$ when $\Gamma = \Gamma_0(p^r)$, $\Gamma_1(p^r)$.

誌謝

在交大的日子已佔了目前人生歲月的三分之一，其中充滿了許許多多的喜怒哀樂。感謝許多人長久以來的支持，讓我能順利完成學業。首先，感謝我的指導教授楊一帆老師在我的學業上的指導與建議。他的包容與愛護讓我能在迷途中，有了指引。從他身上，我看到了一個數學家的熱誠與堅持。研究所求學期間，與他討論數學相關議題，已成為我的興趣之一。他也鼓勵與支持我參加國內外的研討會及訪問。讓我能推廣見聞及培養我的國際觀，藉以提升我數學的深度。

感謝其他口試委員李文卿教授、于靖教授、余正道教授、夏良忠教授、翁志文教授的寶貴建議。其中特別感謝李文卿老師在 Penn State 訪問期間的招待與指導。感謝于靖老師在我的問題上提供更深度的建議與指導。感謝余正道老師在 Queen's University 期間的招待與建議。

感謝我的前指導教授林松山老師，在他門下學習了四年，雖然最後因興趣問題而離開。但是他的教導，一直讓我深深記得。做研究應該有的態度、培養國際觀等等一直都是他時常教導我們的重要課題。

感謝陳秋媛教授從我大一到現在不斷的關心與教導。無論遇到什麼困難，她都會盡全力幫忙，讓我一直非常感激。她對待學生就像照顧自己的小孩，盡心盡力。

在交大這麼多年，修的課程及認識的老師自然也不少。在此非常感謝各位的教導。其中特別感謝黃大原教授常常與我討論代數相關問題。感謝王夏聲教授時常與我討論實變等分析數學。感謝吳培元教授的矩陣分析讓我對線代有更深的了解。

在博士班的生活中，感謝各位學長姐、同學、學弟妹的教導與包容。其中特別感謝前師門榮超學長、吟衡學姐、志鴻學長、同研究室的明杰、隔壁研究室的文貴、恭儉、同師門的芳婷，在與他們的相處與討論中，時常充滿歡樂。

最後，感謝我的父母，因為有他們的幫忙與教養，才能有如今的我。無論

遇到甚麼事，他們始終支持我。感謝我的大哥，時常關心我的生活。感謝我的女朋友一直以來的支持與包容，讓我無後顧之憂地勇於面對挑戰。

陳耀漢 99/09/09　　於交大

Contents


E S A
1896

CHAPTER 1

Introduction

Let Γ be a congruence subgroup between $\Gamma_1(N)$ and $\Gamma_0(N)$ for some positive integer N. Denote by $X(\Gamma)$ the modular curve over $\mathbb{Q}$ and let $J(\Gamma)$ be the Jacobian variety of $X(\Gamma)$. In number theory, it is very important to understand $X(\Gamma)$ and $J(\Gamma)$. For example, by the modularity theorem, any elliptic curve over $\mathbb{Q}$ can be obtained from $X_0(N)$ for some positive integer N. Besides, the existence of rational N-isogenies and the existence of rational torsion points of order N on elliptic curves essentially depend on the existence of non-cuspidal rational points on $X(\Gamma_0(N))$ and $X(\Gamma_1(N))$, respectively. In this thesis, we are interested in the arithmetic aspects of $X(\Gamma)$ and $J(\Gamma)$. We will study modular units of $X(\Gamma)$ that have divisors defined over $\mathbb{Q}$ and the cuspidal $\mathbb{Q}$-rational torsion subgroup of $J(\Gamma)$ for the case the level N is a prime power.

Let $\mathfrak{C}(\Gamma)$ denote the cuspidal $\mathbb{Q}$-rational torsion subgroup of $J(\Gamma)$ generated by the divisor classes of cuspidal divisors of degree 0 defined over $\mathbb{Q}$. It is of finite order by the result of Manin and Drinfeld [**13**]. In general, it is believed that the cuspidal $\mathbb{Q}$-rational torsion subgroup should be the whole $\mathbb{Q}$-rational torsion subgroup of $J(\Gamma)$. (For $\Gamma = \Gamma_1(p)$, the conjecture was formally stated in [**2**, Conjecture 6.2.2]). Even if it is not the whole group, it still provides us some information about a lower bound of $\mathbb{Q}$-rational torsion subgroup of Jacobian.

The study of cuspidal torsion subgroup of $J(\Gamma)$ is essentially the same as the study of modular units on Γ because the divisor of a modular unit corresponds to the zero of the Jacobian $J(\Gamma)$. In the case $\Gamma = \Gamma_0(N)$, a good source of modular units comes from the Dedekind eta functions. M. Newman [**16, 17**] determined sufficient conditions for a product $\prod_{d|N} \eta(d\tau)^{r_d}$ of Dedekind eta functions to be modular on $\Gamma_0(N)$. In [**22**], Takagi showed that for square-free integers N, these functions generate the group of modular units on $\Gamma_0(N)$. When $N = p$ is a prime, Ogg [**18**] showed that $\mathfrak{C}(\Gamma_0(p))$ is cyclic of order $\frac{p-1}{(p-1,12)}$. Moreover, Ogg [**19**] conjectured and Mazur [**14**] proved that the full $\mathbb{Q}$-rational torsion subgroup of $J(\Gamma_0(p))$ is $\mathfrak{C}(\Gamma_0(p))$ generated by $[(0) - (\infty)]$. For $N = p^r$ with $p \geq 3$ a prime, Ling [**12**] computed $\mathfrak{C}(\Gamma_0(p^r))$ and apply it to determine the component group of the Néron model of $J(\Gamma_0(p^r))$ over $\mathbb{Z}_p$. When $N = pq$, where p, q are two distinct primes, Chua and Ling [**1**] studied in $\mathfrak{C}(\Gamma_0(pq))$ and use their results to refine some results of Berkovič on the nontriviality of the Mordell-Weil group of some Eisenstein factors of $J(\Gamma_0(pq))$.

We remark that many mathematicians, for example, Klimek [**4**], Kubert and Lang [**9**], Yu [**26**], Yang [**24, 25**], and Yu [**25**] have studied cuspidal $\mathbb{Q}$-rational torsion subgroups of $J(\Gamma_1(N))$. However, all of their works only considered a special subgroup $\mathfrak{C}^\infty(\Gamma_1(N))$ of $\mathfrak{C}(\Gamma_1(N))$ for different levels N, where $\mathfrak{C}^\infty(\Gamma_1(N))$ is generated by the divisor classes of the differences of the cusps of $X(\Gamma_1(N))$ lying over ∞ of $X(\Gamma_0(N))$. (In fact, Klimek [**4**], Kubert and Lang [**9**], Yu [**26**] considered the the subgroup generated by the divisor classes of the differences of the cusps of $X(\Gamma_1(N))$ lying over 0 of $X(\Gamma_0(N))$. However, it is plain that the Atkin-Lehner involution $\begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix}$ gives rise to an isomorphism between the two divisor class groups.) In [**26**], Yu showed that for arbitrary level N, all modular units on

$X(\Gamma_1(N))$ that have divisors supported on cusps of $X(\Gamma_1(N))$ lying over ∞ of $X(\Gamma_0(N))$ are generated by a subclass of Siegel functions and then he computed the order of $\mathfrak{C}^{\infty}(\Gamma_1(N))$. In [**24**], Yang used Yu's order formula to construct a basis of the modular units on $X(\Gamma_1(N))$ that have divisors supported on cusps of $X(\Gamma_1(N))$ lying over ∞ of $X(\Gamma_0(N))$. In general, $\mathfrak{C}^{\infty}(\Gamma)$ is not equal to $\mathfrak{C}(\Gamma)$. Thus, now it is more important to consider $\mathfrak{C}(\Gamma)$. However, for the whole $\mathfrak{C}(\Gamma)$, it is unknown whether modular units on $X(\Gamma)$ that have divisors defined over $\mathbb{Q}$ are still generated by this subclass of Siegel functions. Moreover, there is no information about the order of $\mathfrak{C}(\Gamma)$. Hence, it is very difficult to study in the case of arbitrary level N.

In this thesis, we use the results of Kubert and Lang [**8**] or [**11**], which says the group of modular units on $\Gamma(N)$ is generated by (products of) the Siegel functions (except for 2-cotorsions in the case when N is not a prime power), to show that modular units on $X(\Gamma)$ that have divisors defined over $\mathbb{Q}$ are indeed generated by a special class of Siegel functions when the level is a prime power. (For general level, we guess that the 2-cotorsion would disappear in our situation. However, it is not easy to verify it. Thus, we work on $\mathfrak{C}(\Gamma)$ for the case the level is a prime power herein and leave general cases in later studies.) Then we construct a basis for the group of modular units on $X(\Gamma)$ that have divisors defined over $\mathbb{Q}$. (The result is too complicated to be stated here. We refer the reader to Theorem 4.1 and Theorem 4.2 for details.) As an application, we determine the order $h(\Gamma)$ of $\mathfrak{C}(\Gamma)$ when $\Gamma = \Gamma_1(p^r), \Gamma_0(p^r)$.

Here given a Dirichlet character χ modulo N, we let $B_{k,\chi}$ denote the generalized Bernoulli numbers defined by the power series

$$\sum_{a=1}^{N} \chi(a) \frac{te^{at}}{e^{Nt}-1} = \sum_{k=0}^{\infty} \frac{B_{k,\chi}}{k!} t^k.$$

In particular, if we let $\{x\}$ be the fractional part of a real number x, then we have

$$B_{2,\chi} = N \sum_{a=1}^{N} \chi(a) B_2(a/N),$$

where

$$B_2(x) = \{x\}^2 - \{x\} + \frac{1}{6}.$$

THEOREM 1.1. *Let $p > 3$ be a prime and $r > 0$. Then we have*

$$h(\Gamma_1(p^r)) = \left(\frac{(p-1)(p+1)}{24}\right)^{r-1} \cdot \left(p^{\left(\frac{p^r-p}{p-1}\right)-2r+3}\right) \cdot \prod_{i=1}^{r} \prod_{\chi \neq \chi_0 \bmod p^i,\ \textit{even}} \frac{1}{4} B_{2,\chi \bmod p^i}.$$

where the innermost product is taken over all even nonprincipal Dirichlet characters modulo p^i for $i = 1, \ldots, r$.

We note that the order of $\mathfrak{C}^\infty(\Gamma_1(p^r))$ is

$$p^{p^{r-1}-2r+2} \cdot \prod_{\chi \neq \chi_0,\ \textit{even}} \frac{1}{4} B_{2,\chi},$$

where the product is taken over all even nonprincipal Dirichlet characters modulo p^r. This is given by Kubert and Lang [**9**]. Then we can find that $\mathfrak{C}^\infty(\Gamma_1(p^r)) \neq \mathfrak{C}(\Gamma_1(p^r))$ for $r > 1$.

THEOREM 1.2. *Let $p > 3$ be a prime and $r > 0$. Then we have*

$$h(\Gamma_0(p^r)) = \frac{p-1}{\gcd(p-1, 12)} \cdot \left(\frac{(p+1)(p-1)}{24}\right)^{r-1} \cdot p^{(r-1)^2}.$$

Note that Ling [**12**] computed the structure of $\mathfrak{C}(\Gamma_0(p^r))$ for a prime $p \geq 3$ and $r > 0$. (We don't describe it here because of the complicated statement.)

REMARK. For $p = 2, 3$, we can go through similar proof to get similar results. Moreover, for $\Gamma \neq \Gamma_0(p^r), \Gamma_1(p^r)$, we still can compute the order of $\mathfrak{C}(\Gamma)$ by similar methods. However, their statements are so complicated that we omit them herein.

The rest of this thesis is organized as follows. In Chapter 2, we will review some backgrounds about modular curves and modular units. Then in Chapter 3 we recall some notion and properties about cuspidal $\mathbb{Q}$-rational torsion subgroups of Jacobians of modular curves and Siegel functions. Finally, in Chapter 4, we will prove our main results.


E S A
1896

CHAPTER 2

Backgrounds

In this section, we will recall some basic knowledge about modular curves.

1. Modular groups

Let $SL_2(\mathbb{Z})$ be the group of 2×2 matrices which have integral entries and determinant 1, and then we set

$$PSL_2(\mathbb{Z}) = SL_2(\mathbb{Z})/\{\pm I\}$$

DEFINITION 2.1. Let Γ be a subgroup of $PSL_2(\mathbb{Z})$ of finite index. If Γ contains the subgroup

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

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

Especially, we are interested in the following two congruence subgroups

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

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

Finally, we note that

$$\Gamma_0(N)/\Gamma_1(N) \cong (\mathbb{Z}/N\mathbb{Z})^\times/\pm 1.$$

2. Modular curves

Let X be a one-dimensional connected complex analytic manifold. A *local coordinate* (U, z) is an open subset U of X, together with a homeomorphism $z : U \mapsto \mathbb{C}$ onto an open subset of $\mathbb{C}$. The local coordinates are also called local charts or local parameters.

DEFINITION 2.2. A *Riemann surface* is a one-dimensional connected complex analytic manifold X with a set of local coordinates $\{(U_\alpha, z_\alpha)\}_{\alpha\in A}$, where A is an index set, such that

(1) $X = \cup_\alpha U_\alpha$,

(2) the transition function

$$z_\alpha \circ z_\beta^{-1} : z_\beta(U_\alpha \cap U_\beta) \mapsto z_\alpha(U_\alpha \cap U_\beta)$$

are holomorphic whenever $U_\alpha \cap U_\beta \neq \emptyset$.

For example, the unit sphere $S = \{(x, y, z) \in \mathbb{R}^3 : x^2 + y^2 + z^2 = 1\}$ is a Riemann surface. Moreover, it is a one-point compactification of $\mathbb{C}$.

Denote $GL_2^+(\mathbb{R})$ the group of 2×2 real matrices of positive determinant. Let $\mathbb{H} = \{x + iy : \mathrm{Im}(y) > 0\}$ be the *upper half plane*. We know $GL_2^+(\mathbb{R})$ acts on $\mathbb{H}$ by the following way

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \times \tau \mapsto \frac{a\tau + b}{c\tau + d}.$$

If Γ is a subgroup of $PSL_2(\mathbb{Z})$ of finite index, by giving a complex structure, we get a Riemann surface $Y(\Gamma) := \Gamma \setminus \mathbb{H}$ and it can be compactified

by adjoining cusps to it. The compactified modular curve $\Gamma \setminus \mathbb{H} \cup \{\text{cusps}\}$ will be denoted by $X(\Gamma)$. (For details, please see [**20**].)

Let $p \in X$, where X is a Riemann surface and let f be a complex-valued function defined on a neighborhood W of p.

DEFINITION 2.3. We say f is *holomorphic (meromorphic)* at p if there exists a chart $z : U \mapsto V$ with $p \in U$, such that $f \circ z^{-1}$ is holomorphic (meromorphic) at $z(p)$. We say f is *holomorphic (meromorphic)* in W if it is holomorphic (meromorphic) at every point of W.

Later on, we can find modular functions are meromorphic function on modular curves.

DEFINITION 2.4. A *differential* 1*-form* ω (or simply 1*-form*) is an assignment of functions f_α to each chart (U_α, z_α) such that $f_\alpha(z_\alpha)dz_\alpha$ is invariant under coordinate changes and agrees on overlaps of charts. (Note that this function f is defined only locally on U_α, not globally on the whole X.) To be explicit, write $w_{\alpha\beta} = z_\alpha \circ z_\beta^{-1} : z_\beta(U_\alpha \cap U_\beta) \mapsto z_\alpha(U_\alpha \cap U_\beta)$. Then a differential 1-form satisfies $f_\beta(z_\beta)dz_\beta = f_\alpha(\omega_{\alpha\beta}(z_\beta))\omega'_{\alpha\beta}(z_\beta)dz_\beta$, for each pair of overlapping U_α and U_β. Furthermore, a 1-form ω is *holomorphic (meromorphic)* provided that locally $\omega = df$ with f holomorphic (meromorphic).

In essence, modular forms of weight 2 are differential 1-forms on certain Riemann surfaces (modular curves).

By similar ways, on Riemann surfaces, we can also define integration, the order of a meromorphic function at a point, and so on. (For details, please see [**15**].)

3. Modular forms

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

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

The factor $c\tau + d$ is called the *automorphy factor*.

DEFINITION 2.5. Let Γ be a subgroup of $PSL_2(\mathbb{Z})$ of finite index, and k be an even integer. A meromorphic function $f : \mathbb{H} \mapsto \mathbb{C}$ is a *meromorphic modular form* of weight k with respect to Γ if

(1) $f(\tau)|[\gamma]_k = f(\tau)$ for all $\tau \in \mathbb{H}$ and $\gamma \in \Gamma$,
(2) f is meromorphic at every cusp.

For instance, Eisenstein series

$$E_k(\tau) = \sum_{c,\ d \in \mathbb{Z},\ (c,d) \neq (0,0)} \frac{1}{(c\tau + d)^k}$$

are modular forms of weight k with respect to $PSL_2(\mathbb{Z})$.

We note that there is an isomorphism between the two vector spaces

$$\{\text{meromorphic modular forms of weight } 2k \text{ on } \Gamma\}$$

and

$$\{\text{meromorphic } k\text{-fold differential forms on } X(\Gamma)\}.$$

DEFINITION 2.6. A meromorphic modular form of weight 0 is called a *modular function*.

DEFINITION 2.7. A *modular unit* $f(\tau)$ on Γ is a modular function on Γ whose poles and zeros are all at cusps.

3.1. Dedekind eta functions.

DEFINITION 2.8. Let $\tau \in \mathbb{H}$, and write $q = e^{2\pi i\tau}$. The *Dedekind eta function* $\eta(\tau)$ is defined by

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

The Dedekind eta function provides a convenient way of constructing modular forms and modular functions. For example, $\eta(\tau)^{24}$ is a cusp form of weight 12 on $PSL_2(\mathbb{Z})$. In particular, the Dedekind eta function can be utilized to construct modular units on $\Gamma_0(N)$. For instance, $(\eta(11\tau)/\eta(\tau))^{12}$ is a modular unit on $\Gamma_0(11)$. Furthermore, it generates the group of modular units on $\Gamma_0(11)$. (For details, please see [**16, 17**].)

3.2. Siegel functions.

DEFINITION 2.9. For $a = (a_1, a_2) \in \mathbb{Q}^2, a \notin \mathbb{Z}^2$, the *Siegel function* g_a is defined by

$$g_a(\tau) = \mathfrak{f}_a(\tau)\eta(\tau)^2,$$

where $\mathfrak{f}_a(\tau)$ is the Klein form associated to a:

$$\mathfrak{f}_a(\tau) = e^{-\frac{1}{2}(a_1\eta_1+a_2\eta_2)z}\sigma\left(z,[\tau,1]\right).$$

Here η_1, η_2 are the quasi periods of Weierstrass zeta function associated with the period lattice $[\tau, 1]$, $z = a_1\tau + a_2$, σ is the corresponding Weierstrass sigma function

$$\sigma\left(z,[\tau,1]\right) = z\prod_{\omega\in[\tau,1]-(0,0)}\left(1-\frac{z}{\omega}\right)e^{z/\omega+(z/\omega)^2/2}.$$

Setting $q_\tau = e^{2\pi i\tau}$ and $q_z = e^{2\pi iz}$, we know the Siegel functions have the following infinite product representation

$$g_a(\tau) = -q_\tau^{(1/2)B_2(a_1)} e^{2\pi a_2(a_1-1)/2}(1-q_z)\prod_{n=1}^{\infty}(1-q_\tau^n q_z)(1-q_\tau^n/q_z),$$

where $B(x) = x^2 - x + 1/6$ is the second Bernoulli polynomial. Siegel functions give us a convenient way to construct modular units on $\Gamma(N)$ and $\Gamma_1(N)$. For example, $g_a^{12\cdot 5^3}$ with $a \in (1/5^3)\mathbb{Z}^2$, $a \notin \mathbb{Z}^2$ are modular units on $\Gamma(5^3)$. (For details, please see [**5, 6, 7, 8, 10**].)

4. Algebraic curves

DEFINITION 2.10. An *projective algebraic curve* is an algebraic projective variety of dimension one.

We recall a fundamental result in the theory of Riemann surfaces.

THEOREM 2.1 (cf. [**15**]). *Every compact Riemann surface X is a non-singular projective algebraic curve C. The curve C is unique determined, up to isomorphism.*

In particular, this theorem asserts that every compact Riemann surface is isomorphic to a curve defined by the zero set of a set of homogeneous polynomials over $\mathbb{C}$ in a projective space $\mathbb{P}^n(\mathbb{C})$.

Furthermore, it is well-known that

THEOREM 2.2 (cf.[**20, 21**]). *If Γ is a congruence subgroup of $PSL_2(\mathbb{Z})$ of level N, then modular curves $X(\Gamma)$ are defined over $\mathbb{Q}(\mu_N)$, where μ_N is the group of Nth roots of unity. In particular, it can be defined over $\mathbb{Q}$ when Γ is between $\Gamma_0(N)$ and $\Gamma_1(N)$.*

Also, cusps of $X(\Gamma)$ are defined over $\mathbb{Q}(\mu_N)$.

5. Jacobian varieties

Let X be a compact Riemann surface.

DEFINITION 2.11. The Jacobian of X is the quotient space

$$J(X) = \Omega^1(X)^*/\Lambda$$

of functionals on the space $\Omega^1(X)$ of all holomorphic differentials on X modulo the lattice Λ of elements of $\Omega^1(X)^*$ of the form

$$\int_X : \Omega^1(X) \mapsto \mathbb{C}$$

defined by

$$\omega \mapsto \int_\gamma \omega,$$

where γ is a closed path in X.

The *group of divisors* $\mathrm{Div}(X)$ on X is the free abelian group generated by points on X. That is, the element of $\mathrm{Div}(X)$ is a finite sum $\sum n_i P_i, n_i \in \mathbb{Z}$. Denote $\mathrm{PDiv}(X)$ by the subgroup of $\mathrm{Div}(X)$ consisting of $div(f) := \sum ord_P(f) \cdot P$ for some meromorphic function f on X. We call it the *group of principal divisors*. The *degree* of a divisor $\sum n_i P_i$ is $\sum n_i$. Denote $\mathrm{Div}_0(X)$ by the subgroup of $\mathrm{Div}(X)$ consisting of divisor of degree 0.

By Abel-Jacobi Theorem, we know

THEOREM 2.3. $J(X) \cong \mathrm{Div}_0(X)/\mathrm{PDiv}(X)$.

In this article, we are interested in the cuspidal $\mathbb{Q}$-rational torsion subgroup of $J(X)$. We believe it should be the whole $\mathbb{Q}$-rational torsion subgroup of $J(X)$. (For $\Gamma = \Gamma_1(p)$, the conjecture was formally stated in [**2**,

Conjecture 6.2.2]). Even if it is not the whole group, we still get a lower bound of $\mathbb{Q}$-rational torsion subgroup of Jacobian by studying the cuspidal $\mathbb{Q}$-rational torsion subgroup.

CHAPTER 3

Preliminaries

In this section, we will briefly review basics of modular curves that are relevant to our problem. We then describe properties of Siegel functions, which will be the building blocks for modular units on modular curves.

1. Cuspidal $\mathbb{Q}$-rational torsion subgroups of $J(\Gamma)$

Let Γ be a congruence subgroup between $\Gamma_1(N)$ and $\Gamma_0(N)$ for some positive integer N. Denote by $X(\Gamma)$ the modular curve over $\mathbb{Q}$ and let $J(\Gamma)$ be the Jacobian variety of $X(\Gamma)$. We know the cusps of $X(\Gamma)$ are rational over $\mathbb{Q}(\zeta_N)$, where ζ_N is a primitive Nth root of unity. The following lemma describes the action of the Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_{p^r})/\mathbb{Q})$ on the cusps of $X(\Gamma)$.

LEMMA 1. *Let p be an odd prime and $r > 0$. Let $k := [\Gamma_0(p^r) : \Gamma] = p^u v$ with $p \nmid v$. For a positive integer ℓ, we set $\phi_\ell = \phi(p^\ell)/2$ and $k_\ell = (k, \phi_\ell)$. Let a, b be generators of $(\mathbb{Z}/p^r\mathbb{Z})^\times$ with $(a, b) = 1$. Then the cusps on $X(\Gamma)$ can be represented by*

$$\begin{cases} \frac{a^s}{p^r} & \text{for } 0 \le s < k_r, \\ \frac{1}{b^t} & \text{for } 0 \le t < k_r, \\ \frac{a^s}{p^i b^t} & \text{for } 0 < i < \min\{r-u-1, r/2\},\ 0 \le s < k_i, \\ & \quad \text{and } 0 \le t < (2\phi_i k)/k_i, \\ \frac{a^s}{p^i b^t} & \text{for } \min\{r-u-1, r/2\} \le i < r,\ 0 \le s < k_i, \text{ and } 0 \le t < 2\phi_{r-i}. \end{cases}$$

Moreover, for $0 \le j < 2\phi_r$, $\sigma_{b^j} \in \mathrm{Gal}(\mathbb{Q}(\zeta_{p^r})/\mathbb{Q})$ *defined by* $\sigma_{b^j} : \zeta_{p^r} \mapsto \zeta_{p^r}^{b^j}$, *we have*

$$\begin{cases} \sigma_{b^j}\left(\frac{a^s}{p^r}\right) = \frac{a^s}{p^r}, \\ \sigma_{b^j}\left(\frac{1}{b^t}\right) = \frac{1}{b^{\overline{t-j}}}, & \text{where } 0 \le \overline{t-j} \le k_r - 1 \text{ such that } \overline{t-j} \equiv \widetilde{t-j} \mod k_r \\ & \quad \text{for } 0 \le \widetilde{t-j} \le \phi_r - 1 \text{ and } \widetilde{t-j} \equiv \pm(t-j) \mod 2\phi_r, \\ \sigma_{b^j}\left(\frac{a^s}{p^i b^t}\right) = \frac{a^s}{p^i b^{\overline{t-j}}}, & \text{where } 0 < i < \min\{r-u-1, r/2\}, \\ & \quad \text{and } 0 \le \overline{t-j} \le (2\phi_i k)/k_i - 1 \\ & \quad \text{such that } \overline{t-j} \equiv t-j \mod (2\phi_i k)/k_i, \\ \sigma_{b^j}\left(\frac{a^s}{p^i b^t}\right) = \frac{a^s}{p^i b^{\overline{t-j}}}, & \text{where } \min\{r-u-1, r/2\} < i < r, \\ & \quad \text{and } 0 \le \overline{t-j} \le 2\phi_{r-i} - 1 \\ & \quad \text{such that } \overline{t-j} \equiv t-j \mod 2\phi_{r-i}. \end{cases}$$

PROOF. From [3] or [18], all inequivalent cusps of $\Gamma_1(p^r)$ are given by the following numbers:

$$\frac{x}{p^r},$$

where $1 \le x < p^r/2$ and $(x,p) = 1$, and

$$\frac{x}{p^i y},$$

where $0 \le i < r$, $x \in \{1, \dots, p^i\} \bmod p^i$, $1 \le y < p^{r-i}/2$, $(x,p) = 1$, $(y,p) = 1$, and $(x,y) = 1$. Because $\Gamma_0(p^r)/\Gamma_1(p^r) \simeq (\mathbb{Z}/p^r\mathbb{Z})^\times/\pm 1$, we can write

$$\Gamma = \langle \Gamma_1(p^r), \gamma \rangle$$

for some $\gamma \equiv \begin{pmatrix} a^k & * \\ p^r & b^k \end{pmatrix} \mod p^r$. Thus, the inequivalent cusps of $X(\Gamma)$ can be represented by numbers in the lemma.

For the second part of this lemma, it directly follows from [**21**, Theorem 1.3.1]. □

Let K be a subfield of $\mathbb{Q}(\zeta_N)$. A cusp P is said to be *defined over* K, if $P^\sigma = P$ for all $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_N)/K)$. More generally, a cuspidal divisor $D = \sum n_i P_i$ is *defined over* K, if $D^\sigma := \sum n_i P_i^\sigma$ satisfies $D^\sigma = D$ for all $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_N)/K)$. Here we are interested in the case $K = \mathbb{Q}$. From the above lemma, we immediately obtain the following information about the $\mathbb{Q}$-rational cuspidal divisor group of $X(\Gamma)$.

COROLLARY 2. *Let all the notations be given as in Lemma 1. Then the $\mathbb{Q}$-rational cuspidal divisor group of $X(\Gamma)$ is a free abelian group of rank $(\sum_{i=1}^{r} k_i) + 1$ generated by the divisors*

$$\begin{cases} \left(\frac{a^s}{p^r}\right) & \text{for } 0 \le s < k_r, \\ \sum_{t=0}^{k_r-1} \left(\frac{1}{b^t}\right), & \\ \sum_{t=0}^{(2\phi_i k)/k_i - 1} \left(\frac{a^s}{p^i b^t}\right) & \text{for } 0 < i < \min\{r-u-1, r/2\} \text{ and } 0 \le s < k_i, \\ \sum_{t=0}^{2\phi_{r-i}-1} \left(\frac{a^s}{p^i b^t}\right) & \text{for } \min\{r-u-1, r/2\} \le i < r \text{ and } 0 \le s < k_i. \end{cases}$$

PROOF. Let D be a $\mathbb{Q}$-rational cuspidal divisor of $X(\Gamma)$. Because D is a cuspidal divisor, we have

$$\begin{aligned} D = &\sum_{s=0}^{k_r-1} c_{r,s} \left(\frac{a^s}{p^r}\right) + \sum_{t=0}^{k_r-1} c_{1,t} \left(\frac{1}{b^t}\right) \\ &+ \sum_{i=1}^{\min\{r-u-1, r/2\}-1} \sum_{s=0}^{k_i-1} \sum_{t=0}^{(2\phi_i k)/k_i - 1} c_{i,s,t} \left(\frac{a^s}{p^i b^t}\right) \\ &+ \sum_{i=\min\{r-u-1, r/2\}}^{r-1} \sum_{s=0}^{k_i-1} \sum_{t=0}^{2\phi_{r-i}-1} c_{i,s,t} \left(\frac{a^s}{p^i b^t}\right) \end{aligned}$$

for some integers $c_{r,s}$, $c_{1,t}$, and $c_{i,t}$. Let $\sigma_{b^j} \in \mathrm{Gal}(\mathbb{Q}(\zeta_{p^r})/\mathbb{Q})$, where $0 \leq j < 2\phi_r$. By above lemma,

$$D^{\sigma_{b^j}} = \sum_{s=0}^{k_r-1} c_{r,s}\left(\frac{a^s}{p^r}\right) + \sum_{t=0}^{k_r-1} c_{1,t}\left(\frac{1}{b^{\overline{t-j}}}\right) + \sum_{i=1}^{\min\{r-u-1,r/2\}-1} \sum_{s=0}^{k_i-1} \sum_{t=0}^{(2\phi_i k)/k_i-1} c_{i,s,t}\left(\frac{a^s}{p^i b^{\overline{t-j}}}\right) + \sum_{i=\min\{r-u-1,r/2\}}^{r-1} \sum_{s=0}^{k_i-1} \sum_{t=0}^{2\phi_{r-i}-1} c_{i,s,t}\left(\frac{a^s}{p^i b^{\overline{t-j}}}\right),$$

where $\overline{t-j}$ are defined in the above lemma. Because D is defined over $\mathbb{Q}$, i.e., $D^{\sigma_{b^j}} = D$ for all $\sigma_{b^j} \in \mathrm{Gal}(\mathbb{Q}(\zeta_{p^r})/\mathbb{Q})$, we know $c_{1,t}$ are the same, and for fixed $i = 1, \ldots, r-1$, fixed $s = 0, \ldots, k_i - 1$, $c_{i,s,t}$ are the same for all t. Thus, D is generated by the divisors in the lemma. Then, clearly, the $\mathbb{Q}$-rational cuspidal divisor group of $X(\Gamma)$ is a free abelian group of rank $(\sum_{s=1}^{r} k_s) + 1$.

□

Now if $D = \sum n_i P_i$ is a $\mathbb{Q}$-rational cuspidal divisor of degree 0, then the divisor class $[D]$ is a $\mathbb{Q}$-rational point on $J(\Gamma)$. Moreover, by the result of Manin and Drinfeld [**13**], this is a torsion point on $J(\Gamma)$. We call the subgroup $\mathfrak{C}(\Gamma)$ of $J(\Gamma)$ generated by all such divisor classes the *cuspidal* $\mathbb{Q}$*-rational torsion subgroup* of $J(\Gamma)$. In order to investigate the order and the structure of this torsion subgroup, we will study the group of modular units on $X(\Gamma)$ that have divisors defined over $\mathbb{Q}$. In the next subsection, we will recall the Siegel functions, which will be used to construct an explicit basis for the group of modular units.

2. Properties of Siegel functions

In this subsection we will introduce and discuss properties of Siegel functions we will use. (See [**6**] and [**8**] for details.) For $a = (a_1, a_2) \in \mathbb{Q}^2, a \notin \mathbb{Z}^2$, the Siegel functions $g_a(\tau)$ are usually defined in terms of the Klein forms and the squares of Dedekind eta functions. Setting $z = a_1\tau + a_2$, $q_\tau = e^{2\pi i\tau}$, and $q_z = e^{2\pi iz}$, we have

$$g_a(\tau) = -q_\tau^{(1/2)B_2(a_1)} e^{2\pi a_2(a_1-1)/2}(1-q_z)\prod_{n=1}^{\infty}(1-q_\tau^n q_z)(1-q_\tau^n/q_z),$$

where $B(x) = x^2 - x + 1/6$ is the second Bernoulli polynomial. From the transformation law of Klein forms, we observe that if we change a by an integral vector in $\mathbb{Z}^2$, then g_a changes by a root of unity. Furthermore, g_a and g_{-a} also differ only by a root of unity.

For a given integer N, we also define a class functions

$$E_a^{(N)}(\tau) = -g_{(a/N,0)}(N\tau) = q^{NB(a/N)/2}\prod_{n=1}^{\infty}(1-q^{(n-1)N+a})(1-q^{nN-a}),$$

for integers a not congruent to 0 modulo N, where $q = e^{2\pi i\tau}$. Since we only consider congruence groups of a fixed level in this note, we shall omit the superscript from the notation $E_a^{(N)}$.

Note that it is easy to see that $E_{g+N} = E_{-g} = -E_g$. Hence, there are only $\lceil (N-1)/2 \rceil$ essentially distinct E_g, indexed over the set $(\mathbb{Z}/N\mathbb{Z})/\pm 1 - \{0\}$, for given N. Thus, a product $\prod_g E_g^{e_g}$ is taken over $g \in (\mathbb{Z}/N\mathbb{Z})/\pm 1 - \{0\}$.

Now we give some properties of E_g relevant to our consideration. The first is the transformation law for E_g.

PROPOSITION 3 ([**23**, Corollary 2]). *The functions E_g satisfy*

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

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

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

and, for $c > 0$,

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

where

$$\epsilon(\gamma) = \epsilon(a, bN, c, d)$$

and

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

From Proposition 3, we give sufficient and necessary conditions for a product $\prod_g E_g^{e_g}$ to be modular on $\Gamma_1(N)$.

PROPOSITION 4 ([**11**, Chapter 3, Theorem 5.2], [**23**, Corollary 3]). *Suppose* $\gcd(N, 6) = 1$. *Consider a function* $f(\tau) = \prod_g E_g(\tau)^{e_g}$, *where* g *and* e_g *are integers with* g *not divisible by* N. *Then one has*

$$\sum_g e_g \equiv 0 \mod 12, \qquad \sum_g g e_g \equiv 0 \mod 2 \tag{1}$$

and

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

if and only if f is a modular function on $\Gamma_1(N)$. Furthermore, for the cases where N is a positive odd integer, conditions (1) and (2) can be reduced to

$$\sum_g e_g \equiv 0 \mod 12$$

and

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

respectively.

The following proposition gives the order of E_g at cusps of $X(\Gamma_1(N))$.

PROPOSITION 5 ([**23**, Lemma 2]). *The order of the function E_g at a cusps a/c of $X_1(N)$ with $(a,c) = 1$ is $(c,N)B_2(ag/(c,N))/2$, where $B_2(x) = \{x\}^2 - \{x\} + 1/6$ and $\{x\}$ denotes the fractional part of a real number x.*

Finally, we need the following lemma in the computation of the cuspidal class number.

LEMMA 6. *Let $p > 3$ be a prime. For a positive integer ℓ, we set $\phi_\ell = \phi(p^\ell)/2$. Then for $k > \ell > 0$ and $j \geq 0$, we have*

$$p^{k-\ell} \sum_{i=0}^{p^{k-\ell}-1} B_2\left(\frac{a^{j+i\phi_\ell}}{p^k}\right) = B_2\left(\frac{a^j}{p^\ell}\right).$$

In particular, for $\ell > 1$, we have

$$p \sum_{i=0}^{\phi_\ell - 1} B_2\left(\frac{a^i}{p^\ell}\right) = \sum_{i=0}^{\phi_{\ell-1}-1} B_2\left(\frac{a^i}{p^{\ell-1}}\right)$$

and

$$\frac{p}{2} \sum_{i=0}^{\phi_1 - 1} B_2\left(\frac{a^i}{p}\right) = \frac{1-p}{24}.$$

PROOF. The proof of the statement is a straightforward computation. □

CHAPTER 4

Main results

1. Notations

Throughout this section, we let $p > 3$ be a prime, $r > 0$, and Γ be an intermediate group between $\Gamma_0(p^r)$ and $\Gamma_1(p^r)$. Let $k := [\Gamma_0(p^r) : \Gamma]$. For a positive integer ℓ, we set $\phi_\ell = \phi(p^\ell)/2$ and $k_\ell = (k, \phi_\ell)$. Let a be an even generator of $(\mathbb{Z}/p^r\mathbb{Z})^\times$. Note that we have

$$\phi_r = [\Gamma_0(p^r) : \Gamma_1(p^r)]$$

and

$$\Gamma = \langle \Gamma_1(p^r), \gamma \rangle$$

for some

$$\gamma = \begin{pmatrix} a^k & * \\ p^r & * \end{pmatrix}.$$

We shall adopt the following notations for $X(\Gamma)$.

$\mathscr{D}(\Gamma) =$ the group of cuspidal divisors of degree 0 on $X(\Gamma)$ having divisors defined over $\mathbb{Q}$,

$\mathscr{F}(\Gamma) =$ the group of modular units on Γ that have divisors defined over $\mathbb{Q}$,

$\mathfrak{C}(\Gamma) = \mathscr{D}(\Gamma)/\mathrm{div}\mathscr{F}(\Gamma)$, the cuspidal $\mathbb{Q}$-rational torsion subgroup of $J(\Gamma)$,

$h(\Gamma) = |\mathfrak{C}(\Gamma)|$, the order of $\mathfrak{C}(\Gamma)$.

2. Case $\Gamma = \Gamma_1(p^r)$

In this subsection, we will give a basis for $\mathscr{F}(\Gamma_1(p^r))$. First, we show $\mathscr{F}(\Gamma_1(p^r))$ is generated by the special class of Siegel functions E_g.

LEMMA 7. *Let $p > 3$ be an odd prime and $r > 0$. Then every element of $\mathscr{F}(\Gamma_1(p^r))$ is a product of E_a modulo $\mathbb{C}^\times$, where $0 \neq a \in (\mathbb{Z}/p^r\mathbb{Z})/\pm 1$.*

PROOF. Let S be the group of modular functions on $\Gamma_1(p^r)$ which are products of E_a for $0 \neq a \in (\mathbb{Z}/p^r\mathbb{Z})/\pm 1$. From Lemma 1 and Proposition 5, it is easy to see $S \subseteq \mathscr{F}(\Gamma_1(p^r))$. By the work of Manin and Drinfeld [**13**] and Corollary 2, we know the rank of $\mathscr{F}(\Gamma_1(p^r))$ is $(p^r-1)/2$. Moreover, the rank of S is $(p^r-1)/2$, too. Thus, it remains to show S has no co-torsion in $\mathscr{F}(\Gamma_1(p^r))$. Let S' be the group of modular functions on $\Gamma_1(p^r)$ which are products of $g_{(0,a/p^r)}$ for $0 \neq a \in (\mathbb{Z}/p^r\mathbb{Z})/\pm 1$. By the Atkin-Lehner involution $\begin{pmatrix} 0 & 1 \\ -N & 0 \end{pmatrix}$, it is equivalent to show S' has no co-torsion in $\mathscr{F}(\Gamma_1(p^r))$.

Let $\ell \in \mathbb{Z}$ and let $f \in \mathscr{F}(\Gamma_1(p^r))$ such that

$$f^\ell = \prod g_{(0,a/p^r)}^{e_a} \in S'$$

for some integers e_a. Because $f \in \mathscr{F}(\Gamma_1(p^r))$, by the result of Kubert and Lang [**11**, Theorem 1.3] about modular units on $\Gamma(p^r)$, we know

$$f = \prod g_{(a_1/p^r,a_2/p^r)}^{e_{(a_1/p^r,a_2/p^r)}}$$

for some integers (a_1, a_2) not congruent to $(0,0)$ mod p^r, and some integers $e_{(a_1/p^r,a_2/p^r)}$. This tell us

$$\prod g_{(a_1/p^r,a_2/p^r)}^{\ell e_{(a_1/p^r,a_2/p^r)}} = f^\ell = \prod g_{(0,a/p^r)}^{e_a}.$$

Hence, we get $\ell \mid e_a$ and then $f \in S'$. □

Now, we want to construct some modular units in $\mathscr{F}(\Gamma_1(p^r))$.

LEMMA 8. *Let $p > 3$ be an odd prime and $r > 0$. For a positive integer ℓ, we set $\phi_\ell = \phi(p^\ell)/2$. Suppose a is a generator of $(\mathbb{Z}/p^r\mathbb{Z})^\times$. Let b be the multiplicative inverse of (a^2-1) mod p^r. Then*

$$\begin{cases} E_{a^j p^{r-i}} E_{a^0}^{b(a^{2j}p^{2(r-i)}-1)-1} E_{a^1}^{-b(a^{2j}p^{2(r-i)}-1)} & \text{for } i = 1,\dots,r-1 \\ & \text{and } j = 0,\dots,\phi_i - 1, \\ E_{a^j} E_{a^0}^{b(a^{2j}-1)-1} E_{a^1}^{-b(a^{2j}-1)} & \text{for } j = 2,\dots,\phi_r - 1, \\ E_{a^0}^{12(b+1)} E_{a^1}^{-12b}, & \\ E_{a^0}^{-p^r} E_{a^1}^{p^r} & \end{cases}$$

are in $\mathscr{F}(\Gamma_1(p^r))$.

PROOF. Clearly, these functions have zeros and poles only at cusps. By Proposition 5, they have divisors defined over $\mathbb{Q}$. Next, we will use Proposition 4 to show these functions are modular on $\Gamma_1(p^r)$. In each cases, it is clear that Condition (1) is satisfied. All we have to do is to show Condition (2) holds in each case. For $i = 1,\dots,r-1$ and $j = 0,\dots,\phi_i - 1$,

$$\begin{aligned} &(a^j p^{r-i})^2 + (a^0)^2(b(a^{2j}p^{2(r-i)} - 1) - 1) + (a^1)^2(-b(a^{2j}p^{2(r-i)} - 1)) \\ &\equiv a^{2j}p^{2(r-i)} - 1 + (1-a^2)b(a^{2j}p^{2(r-i)} - 1) \equiv 0 \mod p^r \end{aligned}$$

because b is the multiplicative inverse of (a^2-1) mod p^r.

Similarly, for $j = 2,\dots,\phi_r - 1$,

$$(a^j)^2 + (a^0)^2(b(a^{2j} - 1) - 1) + (a^1)^2(-b(a^{2j} - 1)) \equiv 0 \mod p^r.$$

In the third case,

$$(a^0)^2(12(b+1)) + (a^1)^2(-12b) \equiv 12b(1-a^2) + 12 \equiv 0 \mod p^r.$$

In the final case, it is trivial. □

Finally, we want to show the functions in above lemma form a basis for $\mathscr{F}(\Gamma_1(p^r))$.

THEOREM 4.1. *Let $p > 3$ be an odd prime and $r > 0$. For a positive integer ℓ, we set $\phi_\ell = \phi(p^\ell)/2$. Suppose a is a generator of $(\mathbb{Z}/p^r\mathbb{Z})^\times$. Let b be the multiplicative inverse of (a^2-1) mod p^r. Then*

$$\begin{cases} E_{a^j p^{r-i}} E_{a^0}^{b(a^{2j}p^{2(r-i)}-1)-1} E_{a^1}^{-b(a^{2j}p^{2(r-i)}-1)} & \text{for } i = 1, \dots, r-1 \\ & \text{and } j = 0, \dots, \phi_i - 1, \\ E_{a^j} E_{a^0}^{b(a^{2j}-1)-1} E_{a^1}^{-b(a^{2j}-1)} & \text{for } j = 2, \dots, \phi_r - 1, \\ E_{a^0}^{12(b+1)} E_{a^1}^{-12b}, \\ E_{a^0}^{-p^r} E_{a^1}^{p^r} \end{cases}$$

form a basis for $\mathscr{F}(\Gamma_1(p^r))$ modulo $\mathbb{C}^\times$.

PROOF. Let $f \in \mathscr{F}(\Gamma_1(p^r))$. We want to show f is generated by these functions. By Lemma 7 and Proposition 4,

$$f = \prod_{i=1}^{r} \prod_{j=0}^{\phi_i - 1} E_{a^j p^{r-i}}^{e_{i,j}},$$

where

$$12 \mid \sum_{i=1}^{r} \sum_{j=0}^{\phi_i-1} e_{i,j} \quad \text{and} \quad \sum_{i=1}^{r} \sum_{j=0}^{\phi_i-1} e_{i,j}(a^j p^{r-i})^2 \equiv 0 \mod p^r.$$

Because $\sum_{i=1}^{r}\sum_{j=0}^{\phi_i-1} e_{i,j} = 12x$ for some integer x, we have

$$(a^2-1)e_{r,1} \equiv -\sum_{i=1}^{r-1}\sum_{j=0}^{\phi_i-1} e_{i,j}(a^{2j}p^{2(r-i)}-1) - \sum_{j=2}^{\phi_r-1} e_{i,j}(a^{2j}-1) - 12x \mod p^r.$$

This implies

$$e_{r,1} \equiv -\sum_{i=1}^{r-1}\sum_{j=0}^{\phi_i-1} e_{i,j}b(a^{2j}p^{2(r-i)}-1) - \sum_{j=2}^{\phi_r-1} e_{i,j}b(a^{2j}-1) - 12bx \mod p^r$$

and then

$$e_{r,1} = -\sum_{i=1}^{r-1}\sum_{j=0}^{\phi_i-1} e_{i,j}b(a^{2j}p^{2(r-i)}-1) - \sum_{j=2}^{\phi_r-1} e_{i,j}b(a^{2j}-1) - 12bx + p^r y$$

for some integer y. Thus,

$$e_{r,0} = \sum_{i=1}^{r-1}\sum_{j=0}^{\phi_i-1} e_{i,j}(b(a^{2j}p^{2(r-i)}-1)-1) + \sum_{j=2}^{\phi_r-1} e_{i,j}(b(a^{2j}-1)-1) + 12(b+1)x - p^r y.$$

Sum up above discussions, we get

$$f = \prod_{i=1}^{r-1}\prod_{j=0}^{\phi_i-1}\left(E_{a^j p^{r-i}}E_{a^0}^{b(a^{2j}p^{2(r-i)}-1)-1}E_{a^1}^{-b(a^{2j}p^{2(r-i)}-1)}\right)^{e_{i,j}} \cdot \prod_{j=2}^{\phi_r-1}\left(E_{a^j}E_{a^0}^{b(a^{2j}-1)-1}E_{a^1}^{-b(a^{2j}-1)}\right)^{e_{r,j}} \cdot \left(E_{a^0}^{12(b+1)}E_{a^1}^{-12b}\right)^x \cdot \left(E_{a^0}^{-p^r}E_{a^1}^{p^r}\right)^y.$$

This completes our proof. □

3. Case $\Gamma \neq \Gamma_1(p^r)$

In this subsection, we want to construct a basis for $\mathscr{F}(\Gamma)$. Especially, we get a basis for $\mathscr{F}(\Gamma_0(p^r))$.

First, we give two lemmas which will be used often in later proof.

LEMMA 9. *Let $p > 3$ be an odd prime and $r > 0$. For a positive integer ℓ, we set $\phi_\ell = \phi(p^\ell)/2$. Let a be an even generator of $(\mathbb{Z}/p^r\mathbb{Z})^\times$. Let $c \in \mathbb{Z}^+ \cup \{0\}$. For $i = 1, \dots, r$, if $j > 0$, then*

$$E_{a^{j+c\phi_i}p^{r-i}} = (-1)^c E_{a^j p^{r-i}}.$$

If $j = 0$, then

$$E_{a^{\phi_i}p^{r-i}} = E_{a^0 p^{r-i}}.$$

PROOF. Given $i = 1, \dots, r$ and $j \geq 0$. Let $a^{\phi_i} = -1 + xp^i$ for some odd integer x. We know

$$a^{j+c\phi_i}p^{r-i} = a^j(-1+xp^i)^c p^{r-i} = (-1)^c a^j p^{r-i} + a^j x' p^r$$

for some integer x'. Thus, by the transformation formula of Proposition 3, if $j > 0$, then

$$E_{a^{j+c\phi_i}p^{r-i}} = (-1)^{c+a^j x'} E_{a^j p^{r-i}} = (-1)^c E_{a^j p^{r-i}}$$

because $2 \mid a$. Similarly, if $j = 0$ and $c = 1$, then

$$E_{a^{\phi_i}p^{r-i}} = (-1)^{1+x} E_{a^0 p^{r-i}} = E_{a^0 p^{r-i}}$$

because x is odd. □

LEMMA 10. *Let $p > 3$ be an odd prime and $r > 0$. Let $k := [\Gamma_0(p^r) : \Gamma]$. For a positive integer ℓ, we set $\phi_\ell = \phi(p^\ell)/2$ and $k_\ell = (k, \phi_\ell)$. Let a be an even generator of $(\mathbb{Z}/p^r\mathbb{Z})^\times$. Suppose $\Gamma \neq \Gamma_1(p^r)$. For $i = 1, \dots, r$ and $j = 0, \dots, k_i - 1$,*

$$\prod_{s=0}^{\phi_i/k_i - 1} E_{a^{j+sk_i}p^{r-i}}$$

satisfies the following conditions:

(1) *it has zeros and poles only at cusps.*

(2) *it has the divisor defined over* $\mathbb{Q}$.

In addition, if $\phi_i/k_i > 1$, *then,*

(3) *it satisfies Condition (2) of Proposition 4.*

(4)

$$\prod_{s=0}^{\phi_i/k_i-1} E_{a^{j+sk_i}p^{r-i}}(\gamma\tau) = -\epsilon(\gamma)^{\phi_i/k_i} \cdot \prod_{s=0}^{\phi_i/k_i-1} E_{a^{j+sk_i}p^{r-i}}(\tau),$$

where $\epsilon(\gamma)$ *is defined in Proposition 3. (Note that* $\epsilon(\gamma)$ *is a* 12*th root of unity and only depends on* γ*.)*

PROOF. Given $i = 1, \ldots, r$ and $j = 1, \ldots, k_i$, clearly, we know $f_{i,j} := \prod_{s=0}^{\phi_i/k_i-1} E_{a^{j+sk_i}p^{r-i}}$ has zeros and poles only at cusps. By Proposition 5, $f_{i,j}$ has the divisor defined over $\mathbb{Q}$. If $a^{2k_i} \equiv 1 \mod p^r$, then $2\phi_r \mid 2k_i \mid 2k$ and thus $k = \phi_r$, which is impossible from our assumption. Hence, we get $a^{2k_i} \not\equiv 1 \mod p^r$. Then

$$\sum_{s=0}^{\phi_i/k_i-1} a^{2(j+sk_i)}p^{2(r-i)} \equiv a^{2j}(a^{2\phi_i}-1)(a^{2k_i}-1)^{-1}p^{2(r-i)} \equiv 0 \mod p^r$$

because $\phi_i/k_i > 1$ and $a^{2\phi_i} \equiv 1 \mod p^i$. Thus Condition (2) of Proposition 4 is satisfied. Next, we show $f_{i,j}(\gamma\tau) = -\epsilon(\gamma)^{\phi_i/k_i} \cdot f_{i,j}(\tau)$. Because $2 \mid a$, we see that

$$\sum_{s=0}^{\phi_i/k_i-1} a^{j+sk_i}p^{r-i} \equiv 0 \mod 2$$

and

$$\sum_{s=0}^{\phi_i/k_i-1} a^{2(j+sk_i)}p^{2(r-i)} \equiv 0 \mod 2p^r.$$

Then by the transformation law in Proposition 3 and $k = ck_i$ for some odd integer c, we know

$$f_{i,j}(\gamma\tau) = \prod_{s=0}^{\phi_i/k_i-1} E_{a^{j+sk_ip^{r-i}}}(\gamma\tau) = \epsilon(\gamma)^{\phi_i/k_i} \cdot \prod_{s=0}^{\phi_i/k_i-1} E_{a^{j+sk_i+k}p^{r-i}}(\tau)$$
$$= \epsilon(\gamma)^{\phi_i/k_i} \cdot \prod_{s=0}^{\phi_i/k_i-1} E_{a^{j+(s+c)k_ip^{r-i}}}(\tau).$$

Let $c = c'(\phi_i/k_i) + s_0$ for some integer s_0 with $0 \le s_0 \le \phi_i/k_i - 1$. Then

$$f_{i,j}(\gamma\tau) = \epsilon(\gamma)^{\phi_i/k_i} \cdot \prod_{s=0}^{\phi_i/k_i-1} E_{a^{j+(s+s_0)k_i+c'\phi_ip^{r-i}}}(\tau)$$
$$= \epsilon(\gamma)^{\phi_i/k_i} \cdot \prod_{s=0}^{\phi_i/k_i-1-s_0} E_{a^{j+(s+s_0)k_i+c'\phi_ip^{r-i}}}(\tau)$$
$$\cdot \prod_{s=\phi_i/k_i-s_0}^{\phi_i/k_i-1} E_{a^{j+(s+s_0)k_i+c'\phi_ip^{r-i}}}(\tau)$$
$$= \epsilon(\gamma)^{\phi_i/k_i} \cdot \prod_{s=s_0}^{\phi_i/k_i-1} E_{a^{j+sk_i+c'\phi_ip^{r-i}}}(\tau) \cdot \prod_{s=0}^{s_0-1} E_{a^{j+sk_i+\phi_i+c'\phi_ip^{r-i}}}(\tau).$$

For $s_0 \le s \le \phi_i/k_i - 1$, by Lemma 9,

$$E_{a^{j+sk_i+c'\phi_ip^{r-i}}} = (-1)^{c'} E_{a^{j+sk_ip^{r-i}}}.$$

Similarly, for $0 \le s \le s_0 - 1$, by Lemma 9,

$$E_{a^{j+sk_i+\phi_i+c'\phi_ip^{r-i}}} = (-1)^{c'+1} E_{a^{j+sk_ip^{r-i}}}.$$

Thus,

$$\begin{aligned} f_{i,j}(\gamma\tau) &= \epsilon(\gamma)^{\phi_i/k_i} \cdot (-1)^{c'(\phi_i/k_i)+s_0} \prod_{s=0}^{\phi_i/k_i-1} E_{a^{j+sk_i}p^{r-i}}(\tau) \\ &= \epsilon(\gamma)^{\phi_i/k_i} \cdot (-1)^{c'(\phi_i/k_i)+s_0} f_{i,j}(\tau) \\ &= \epsilon(\gamma)^{\phi_i/k_i} \cdot (-1)^{c} f_{i,j}(\tau). \end{aligned}$$

Because c is odd, we get $f_{i,j}(\gamma\tau) = -\epsilon(\gamma)^{\phi_i/k_i} \cdot f_{i,j}(\tau)$.

For $i = 1, \ldots, r$, let $f_{i,0} := \prod_{s=0}^{\phi_i/k_i-1} E_{a^{sk_i}p^{r-i}}$. By similar discussions, we know $f_{i,0}$ satisfies the preceding three conditions. From Lemma 9, we get

$$f_{i,0} = \prod_{s=0}^{\phi_i/k_i-1} E_{a^{sk_i}p^{r-i}} = \prod_{s=1}^{\phi_i/k_i} E_{a^{sk_i}p^{r-i}} = f_{i,k_i}.$$

Thus, $f_{i,0}$ also satisfies the fourth condition. □

Next, we show the following functions are in $\mathscr{F}(\Gamma)$.

LEMMA 11. *Let $p > 3$ be an odd prime and $r > 0$. Let $k := [\Gamma_0(p^r) : \Gamma] = p^u v$, where $p \nmid v$. For a positive integer ℓ, we set $\phi_\ell = \phi(p^\ell)/2$ and $k_\ell = (k, \phi_\ell)$. Let a be an even generator of $(\mathbb{Z}/p^r\mathbb{Z})^\times$. Suppose $\Gamma \neq \Gamma_1(p^r)$. Then*

(1) *If $v \neq (p-1)/2$, let b be the multiplicative inverse of $\phi_r/(k_r \cdot \gcd((p-1)/2v, 12))$ modulo $12/\gcd((p-1)/2v, 12)$, then*

$$\begin{cases} \prod_{s=0}^{\phi_i/k_i-1} E_{a^{j+sk_i}p^{r-i}} \cdot \left(\prod_{s=0}^{\phi_r/k_r-1} E_{a^{sk_r}} \right)^{b\left(\frac{\phi_r/k_r-\phi_i/k_i}{\gcd((p-1)/2v,12)}\right)-1} & \text{for } i = 1, \ldots, r-1 \\ & \text{and } j = 0, \ldots, k_i - 1, \\ \dfrac{\prod_{s=0}^{\phi_r/k_r-1} E_{a^{j+sk_r}}}{\prod_{s=0}^{\phi_r/k_r-1} E_{a^{sk_r}}} & \text{for } j = 1, \ldots, k_r - 1, \\ \left(\prod_{s=0}^{\phi_r/k_r-1} E_{a^{sk_r}} \right)^{\frac{12}{\gcd((p-1)/2v,6)}} & \end{cases}$$

are in $\mathscr{F}(\Gamma)$.

(2) *If* $v = (p-1)/2$ *and* $u < (r-2)/2$, *let* b *be the multiplicative inverse of* ϕ_r/k_r *modulo* 12, *then*

$$\begin{cases} \dfrac{\prod_{s=0}^{\phi_r/k_r-1} E_{a^{j+sk_r}}}{\prod_{s=0}^{\phi_r/k_r-1} E_{a^{sk_r}}} & \text{for } j = 1, \dots, k_r - 1, \\ \dfrac{\prod_{s=0}^{\phi_i/k_i-1} E_{a^{j+sk_i p^{r-i}}}}{\left(\prod_{s=0}^{\phi_r/k_r-1} E_{a^{sk_r}}\right)^{b(\phi_i/k_i)}} & \text{for } i = 1, \dots, r-1 \text{ and } j = 0, \dots, k_i - 1, \\ \left(\prod_{s=0}^{\phi_r/k_r-1} E_{a^{sk_r}}\right)^{12} & \end{cases}$$

are in $\mathscr{F}(\Gamma)$.

(3) *If* $v = (p-1)/2$ *and* $u \geq (r-2)/2$, *let* b *be the multiplicative inverse of* ϕ_r/k_r *modulo* 12, *then*

$$\begin{cases} \dfrac{\prod_{s=0}^{\phi_r/k_r-1} E_{a^{j+sk_r}}}{\prod_{s=0}^{\phi_r/k_r-1} E_{a^{sk_r}}} & \text{for } j = 1, \dots, k_r - 1, \\ \dfrac{\prod_{s=0}^{\phi_i/k_i-1} E_{a^{j+sk_i p^{r-i}}}}{\left(\prod_{s=0}^{\phi_r/k_r-1} E_{a^{sk_r}}\right)^{b(\phi_i/k_i)}} & \text{for } i = u+2, \dots, r-1 \\ & \text{and } j = 0, \dots, k_i - 1, \\ \dfrac{\prod_{s=0}^{\phi_{u+1}/k_{u+1}-1} E_{a^{j+sk_{u+1}p^{r-(u+1)}}}}{\left(\prod_{s=0}^{\phi_r/k_r-1} E_{a^{sk_r}}\right)^{b(1-a^{2j})} \cdot \left(\prod_{s=0}^{\phi_{u+1}/k_{u+1}-1} E_{a^{sk_{u+1}p^{r-(u+1)}}}\right)^{a^{2j}}} & \text{for } j = 1, \dots, k_{u+1} - 1, \\ \dfrac{\prod_{s=0}^{\phi_i/k_i-1} E_{a^{j+sk_i p^{r-i}}}}{\left(\prod_{s=0}^{\phi_r/k_r-1} E_{a^{sk_r}}\right)^{b(1-a^{2j}p^{2(u+1-i)})} \cdot \left(\prod_{s=0}^{\phi_{u+1}/k_{u+1}-1} E_{a^{sk_{u+1}p^{r-(u+1)}}}\right)^{a^{2j}p^{2(u+1-i)}}} & \text{for } i = 1, \dots, u \\ & \text{and } j = 0, \dots, k_i - 1, \\ \dfrac{\left(\prod_{s=0}^{\phi_{u+1}/k_{u+1}-1} E_{a^{sk_{u+1}p^{r-(u+1)}}}\right)^{p^{2(u+1)-r}}}{\left(\prod_{s=0}^{\phi_r/k_r-1} E_{a^{sk_r}}\right)^{bp^{2(u+1)-r}}}, & \\ \left(\prod_{s=0}^{\phi_r/k_r-1} E_{a^{sk_r}}\right)^{12} & \end{cases}$$

are in $\mathscr{F}(\Gamma)$.

PROOF. For $i = 1, \ldots, r$ and $j = 0, \ldots, k_i$, let

$$f_{i,j} := \prod_{s=0}^{\phi_i/k_i - 1} E_{a^{j+sk_i}p^{r-i}}.$$

We will show this lemma in the three cases, respectively.

(1) Suppose $v \neq (p-1)/2$.

(1.a) For $i = 1, \ldots, r$ and $j = 0, \ldots, k_i - 1$, consider

$$f_{i,j} f_{r,0}^{b\left(\frac{\phi_r/k_r - \phi_i/k_i}{\gcd((p-1)/2v,12)}\right)-1}.$$

We know

$$\begin{aligned}
&\phi_i/k_i + (\phi_r/k_r)\left(b\left(\frac{\phi_r/k_r - \phi_i/k_i}{\gcd((p-1)/2v,12)}\right) - 1\right) \\
&= (\phi_i/k_i)\left(1 - b \cdot \frac{\phi_r/k_r}{\gcd((p-1)/2v,12)}\right) \\
&\quad - (\phi_r/k_r)\left(1 - b \cdot \frac{\phi_r/k_r}{\gcd((p-1)/2v,12)}\right) \\
&\equiv 0 \mod 12
\end{aligned}$$

because $1 - b\frac{\phi_r/k_r}{\gcd((p-1)/2v,12)} \equiv 0 \mod 12/\gcd((p-1)/2v, 12)$ and $(p-1)/2v \mid \phi_i/k_i, \phi_r/k_r$. Thus, Condition (1) of Proposition 4 is satisfied. Also, we know

$$\begin{aligned}
&1 + \left(b\left(\frac{\phi_r/k_r - \phi_i/k_i}{\gcd((p-1)/2v,12)}\right) - 1\right) \\
&= b\left(\frac{\phi_r/k_r - \phi_i/k_i}{\gcd((p-1)/2v,12)}\right) \equiv 0 \mod 2
\end{aligned}$$

because $2(p-1)/2v \mid \phi_r/k_r - \phi_i/k_i$. Combining Proposition 4 with Lemma 10, we get $f_{i,j} f_{r,0}^{b\left(\frac{\phi_r/k_r - \phi_i/k_i}{\gcd((p-1)/2v,12)}\right)-1}$ are in $\mathscr{F}(\Gamma)$.

(1.b) For $j = 1, \ldots, k_r - 1$, consider

$$\frac{f_{r,j}}{f_{r,0}}.$$

Similarly and clearly, by Lemma 10 and Proposition 4, $f_{r,j}/f_{r,0}$ are in $\mathscr{F}(\Gamma)$.

(1.c) Consider

$$f_{r,0}^{\frac{12}{\gcd((p-1)/2v,6)}}.$$

It is clear that

$$(\phi_r/k_r)\left(\frac{12}{\gcd((p-1)/2v,6)}\right) \equiv 0 \mod 12.$$

Moreover, we have

$$\frac{12}{\gcd((p-1)/2v,6)} \equiv 0 \mod 2.$$

Similarly, combining Proposition 4 with Lemma 10, we get $f_{r,0}^{\frac{12}{\gcd((p-1)/2v,6)}}$ are in $\mathscr{F}(\Gamma)$.

(2) Suppose $v = (p-1)/2$ and $u < (r-2)/2$. Before proving this case, we note that for $i = 1, \ldots, r$,

$$\begin{cases} k_i = k \quad \text{and} \quad \phi_i/k_i = p^{i-u-1} & \text{if } i > u+1, \\ k_i = \phi_i = p^{i-u-1}k & \text{if } i \leq u+1. \end{cases}$$

Also, we note that b is odd.

Now, we can start our proof. By Lemma 9, we know

$$E_{a^{\phi_i}p^{r-i}} = E_{a^0p^{r-i}}.$$

Thus, it is equivalent to show

$$\begin{cases} \frac{f_{r,j}}{f_{r,k_r}} & \text{for } j = 1, \ldots, k_r - 1, \\ \frac{f_{i,j}}{f_{r,k_r}^{b(\phi_i/k_i)}} & \text{for } i = 1, \ldots, r-1 \text{ and } j = 1, \ldots, k_i, \\ f_{r,k_r}^{12} & \end{cases}$$

are in $\mathscr{F}(\Gamma)$.

(2.a) For $j = 1, \ldots, k_r - 1$, consider

$$\frac{f_{r,j}}{f_{r,k_r}}.$$

Because $\phi_r/k_r > 1$, clearly, by Lemma 10 and Proposition 4, $f_{r,j}/f_{r,k_r}$ are in $\mathscr{F}(\Gamma)$.

(2.b) For $i = 1, \ldots, r-1$ and $j = 1, \ldots, k_i$, consider

$$\frac{f_{i,j}}{f_{r,k_r}^{b(\phi_i/k_i)}}.$$

We know

$$\phi_i/k_i - (\phi_r/k_r)b(\phi_i/k_i) \equiv 0 \mod 12$$

because b is the multiplicative inverse of ϕ_r/k_r modulo 12. Thus, Condition (1) of Proposition 4 is satisfied. Also, because b and ϕ_i/k_i are odd, we know

$$1 - b(\phi_i/k_i) \equiv 0 \mod 2.$$

For $i > u + 1$, we know $\phi_i/k_i > 1$, and by combining Proposition 4 with Lemma 10, we get $f_{i,j}/f_{r,k_r}^{b(\phi_i/k_i)}$ are in $\mathscr{F}(\Gamma)$.

For $i \leq u+1$, because $1-b(\phi_i/k_i) \equiv 0 \mod 2$, by combining Proposition 4 with Lemma 10, it suffices to show

$$f_{i,j}(\gamma\tau) = -\epsilon(\gamma)^{\phi_i/k_i} \cdot f_{i,j}(\tau) = -\epsilon(\gamma) \cdot f_{i,j}(\tau)$$

and it satisfies Condition (2) of Proposition 4. Clearly,

$$\sum_{s=0}^{\phi_i/k_i-1} a^{2j+2sk_i} p^{2r-2i} = a^{2j} p^{2r-2i} \equiv 0 \mod 2p^r$$

because $u < (r-2)/2$ and $2 \mid a$. In particular, Condition (2) of Proposition 4 is satisfied. Also,

$$\sum_{s=0}^{\phi_i/k_i-1} a^{j+sk_i} p^{r-i} = a^j p^{r-i} \equiv 0 \mod 2,$$

so, by the transformation formula of Proposition 3, we know

$$f_{i,j}(\gamma\tau) = E_{a^j p^{r-i}}(\gamma\tau) = \epsilon(\gamma) \cdot E_{a^{j+k} p^{r-i}}(\tau) = \epsilon(\gamma) \cdot E_{a^{j+p^{u-i+1}\phi_i} p^{r-i}}(\tau).$$

Then by Lemma 9,

$$f_{i,j}(\gamma\tau) = \epsilon(\gamma)\cdot(-1)^{p^{u-i+1}} E_{a^j p^{r-i}}(\tau) = -\epsilon(\gamma)\cdot E_{a^j p^{r-i}}(\tau) = -\epsilon(\gamma)\cdot f_{i,j}(\tau).$$

Therefore, we get $f_{i,j}/f_{r,k_r}^{b(\phi_i/k_i)}$ are also in $\mathscr{F}(\Gamma)$.

(2.c) Consider

$$f_{r,k}^{12}.$$

By Lemma 10 and Proposition 4, clearly, $f_{r,k}^{12}$ is in $\mathscr{F}(\Gamma)$.

(3) Suppose $v = (p-1)/2$ and $u \geq (r-2)/2$. Before proving this case, we note that for $i = 1, \ldots, r$,

$$\begin{cases} k_i = k \quad \text{and} \quad \phi_i/k_i = p^{i-u-1} & \text{if } i > u+1, \\ k_i = \phi_i = p^{i-u-1}k & \text{if } i \leq u+1. \end{cases}$$

Also, we note that b is odd.

Now, we can start our proof. By Lemma 9, we know

$$E_{a^{\phi_i}p^{r-i}} = E_{a^0p^{r-i}}.$$

Thus, it is equivalent to show

$$\begin{cases} \frac{f_{r,j}}{f_{r,k_r}} & \text{for } j = 1, \ldots, k_r - 1, \\ \frac{f_{i,j}}{f_{r,k_r}^{b(\phi_i/k_i)}} & \text{for } i = u+2, \ldots, r-1 \text{ and } j = 1, \ldots, k_i, \\ \frac{f_{u+1,j}}{f_{r,k_r}^{b(1-a^{2j})} f_{u+1,k_{u+1}}^{a^{2j}}} & \text{for } j = 1, \ldots, k_{u+1} - 1, \\ \frac{f_{i,j}}{f_{r,k_r}^{b(1-a^{2j}p^{2(u+1-i)})} f_{u+1,k_{u+1}}^{a^{2j}p^{2(u+1-i)}}} & \text{for } i = 1, \ldots, u \text{ and } j = 1, \ldots, k_i, \\ \frac{f_{u+1,k_{u+1}}^{p^{2(u+1)-r}}}{f_{r,k_r}^{bp^{2(u+1)-r}}}, & \\ f_{r,k_r}^{12} & \end{cases}$$

are in $\mathscr{F}(\Gamma)$.

(3.a) For $j = 1, \ldots, k_r - 1$, consider

$$\frac{f_{r,j}}{f_{r,k_r}}.$$

Because $\phi_r/k_r > 1$, clearly, by Lemma 10 and Proposition 4, $f_{r,j}/f_{r,k_r}$ are in $\mathscr{F}(\Gamma)$.

(3.b) For $i = u+2, \ldots, r-1$ and $j = 1, \ldots, k_i$, consider

$$\frac{f_{i,j}}{f_{r,k_r}^{b(\phi_i/k_i)}}.$$

We know

$$\phi_i/k_i - (\phi_r/k_r)b(\phi_i/k_i) \equiv 0 \mod 12$$

because $(\phi_r/k_r)b \equiv 1 \mod 12$. Condition (1) of Proposition 4 is satisfied. Also, we know

$$1 - b(\phi_i/k_i) \equiv 0 \mod 2$$

because b is odd. In addition, from $\phi_i/k_i > 1$, we get $f_{i,j}/f_{r,k_r}^{b(\phi_i/k_i)}$ are in $\mathscr{F}(\Gamma)$ by combining Lemma 10 with Proposition 4.

(3.c) For $j = 1, \ldots, k_{u+1} - 1$, consider

$$\frac{f_{u+1,j}}{f_{r,k_r}^{b(1-a^{2j})} f_{u+1,k_{u+1}}^{a^{2j}}}.$$

We see

$$\begin{aligned}\phi_{u+1}/k_{u+1} &- (\phi_r/k_r)b(1-a^{2j}) - (\phi_{u+1}/k_{u+1})a^{2j} \\ &\equiv 1 - (1-a^{2j}) - a^{2j} \equiv 0 \mod 12\end{aligned}$$

because $\phi_{u+1}/k_{u+1} = 1$ and $(\phi_r/k_r)b \equiv 1 \mod 12$. The functions satisfy Condition (1) of Proposition 4. In addition,

$$1 - b(1-a^{2j}) = 1 - b + ba^{2j} \equiv 0 \mod 2$$

because $2 \mid a$ and b is odd. Thus, by combining Proposition 4 with Lemma 10, it suffices to show

$$\begin{aligned}\frac{f_{u+1,j}}{f_{u+1,k_{u+1}}^{a^{2j}}}(\gamma\tau) &= -\epsilon(\gamma)^{\phi_{u+1}/k_{u+1} - (\phi_{u+1}/k_{u+1})a^{2j}} \cdot \frac{f_{u+1,j}}{f_{u+1,k_{u+1}}^{a^{2j}}}(\tau) \\ &= -\epsilon(\gamma)^{1-a^{2j}} \cdot \frac{f_{u+1,j}}{f_{u+1,k_{u+1}}^{a^{2j}}}(\tau)\end{aligned}$$

and it satisfies Condition (2) of Proposition 4.

$$\sum_{s=0}^{\phi_{u+1}/k_{u+1}-1} a^{2j+2sk_{u+1}}p^{2r-2(u+1)} - a^{2j}\sum_{s=0}^{\phi_{u+1}/k_{u+1}-1} a^{2k_{u+1}+2sk_{u+1}}p^{2r-2(u+1)}$$

$$= a^{2j}p^{2r-2(u+1)} - a^{2j}a^{2k_{u+1}}p^{2r-2(u+1)}$$

$$= a^{2j}(1-a^{2k_{u+1}})p^{2r-2(u+1)}$$

$$= a^{2j}(1-a^{2\phi_{u+1}})p^{2r-2(u+1)} \equiv 0 \mod 2p^r$$

because $2 \mid a$ and $1 - a^{2\phi_{u+1}} \equiv 0 \mod p^{u+1}$. In particular, Condition (2) of Proposition 4 is satisfied. Also, we see

$$\sum_{s=0}^{\phi_{u+1}/k_{u+1}-1} a^{j+sk_{u+1}}p^{r-(u+1)} - a^{2j}\sum_{s=0}^{\phi_{u+1}/k_{u+1}-1} a^{k_{u+1}+sk_{u+1}}p^{r-(u+1)}$$

$$= a^{j}p^{r-(u+1)} - a^{2j}a^{k_{u+1}}p^{r-(u+1)} \equiv 0 \mod 2.$$

Thus, by the transformation formula of Proposition 3 and Lemma 9, we see

$$\begin{aligned}
\left(\frac{f_{u+1,j}}{f_{u+1,k_{u+1}}^{a^{2j}}}\right)(\gamma\tau) &= \frac{E_{a^j p^{r-(u+1)}}}{\left(E_{a^{k_{u+1}} p^{r-(u+1)}}\right)^{a^{2j}}}(\gamma\tau) \\
&= \epsilon(\gamma)^{1-a^{2j}} \cdot \frac{E_{a^{j+k} p^{r-(u+1)}}}{\left(E_{a^{k_{u+1}+k} p^{r-(u+1)}}\right)^{a^{2j}}}(\tau) \\
&= \epsilon(\gamma)^{1-a^{2j}} \cdot \frac{E_{a^{j+\phi_{u+1}} p^{r-(u+1)}}}{\left(E_{a^{k_{u+1}+\phi_{u+1}} p^{r-(u+1)}}\right)^{a^{2j}}}(\tau) \\
&= \epsilon(\gamma)^{1-a^{2j}} \cdot (-1)^{1-a^{2j}} \frac{E_{a^j p^{r-(u+1)}}}{\left(E_{a^{k_{u+1}} p^{r-(u+1)}}\right)^{a^{2j}}}(\tau) \\
&= -\epsilon(\gamma)^{1-a^{2j}} \cdot \left(\frac{f_{u+1,j}}{f_{u+1,k_{u+1}}^{a^{2j}}}\right)(\tau).
\end{aligned}$$

Hence, we get $f_{u+1,j} / \left(f_{r,k_r}^{b(1-a^{2j})} f_{u+1,k_{u+1}}^{a^{2j}}\right)$ are in $\mathscr{F}(\Gamma)$.

(3.d) For $i = 1, \ldots, u$ and $j = 1, \ldots, k_i$, consider

$$\frac{f_{i,j}}{f_{r,k_r}^{b(1-a^{2j}p^{2(u+1-i)})} f_{u+1,k_{u+1}}^{a^{2j}p^{2(u+1-i)}}}.$$

We know

$$\begin{aligned}
&\phi_i/k_i - (\phi_r/k_r)b\left(1 - a^{2j}p^{2(u+1-i)}\right) \\
&\qquad - (\phi_{u+1}/k_{u+1})a^{2j}p^{2(u+1-i)} \\
&= 1 - 1 + a^{2j}p^{2(u+1-i)} - a^{2j}p^{2(u+1-i)} \\
&\equiv 0 \mod 12
\end{aligned}$$

because $\phi_i/k_i = 1$ and $(\phi_r/k_r)b \equiv 1 \mod 12$. The functions satisfy Condition (1) of Proposition 4.

Clearly,

$$1 - b\left(1 - a^{2j}p^{2(u+1-i)}\right) = 1 - b + ba^{2j}p^{2(u+1-i)}$$
$$\equiv 0 \mod 2$$

because $2 \mid a$ and b is odd. Then by combining Proposition 4 with Lemma 10, it suffices to show

$$\frac{f_{i,j}}{f_{u+1,k_{u+1}}^{a^{2j}p^{2(u+1-i)}}}(\gamma\tau) = -\epsilon(\gamma)^{\phi_i/k_i-(\phi_{u+1}/k_{u+1})a^{2j}p^{2(u+1-i)}} \cdot \frac{f_{i,j}}{f_{u+1,k_{u+1}}^{a^{2j}p^{2(u+1-i)}}}(\tau)$$
$$= -\epsilon(\gamma)^{1-a^{2j}p^{2(u+1-i)}} \cdot \frac{f_{i,j}}{f_{u+1,k_{u+1}}^{a^{2j}p^{2(u+1-i)}}}(\tau)$$

and it satisfies Condition (2) of Proposition 4.

$$\sum_{s=0}^{\phi_i/k_i-1} a^{2j+2sk_i}p^{2r-2i}$$
$$- a^{2j}p^{2(u+1-i)} \sum_{s=0}^{\phi_{u+1}/k_{u+1}-1} a^{2k_{u+1}+2sk_{u+1}}p^{2r-2(u+1)}$$
$$= a^{2j}p^{2r-2i} - a^{2j}p^{2(u+1-i)}a^{2k_{u+1}}p^{2r-2(u+1)}$$
$$= a^{2j}p^{2r-2i} - a^{2j+2k_{u+1}}p^{2r-2i}$$
$$= a^{2j}p^{2r-2i}(1 - a^{2k_{u+1}}) \equiv 0 \mod 2p^r$$

because $2 \mid a$ and $1 - a^{2k_{u+1}} = 1 - a^{2\phi_{u+1}} \equiv 0 \mod p^{u+1}$. In particular, Condition (2) of Proposition 4 is satisfied. Also,

we see

$$\sum_{s=0}^{\phi_i/k_i-1} a^{j+sk_i}p^{r-i} - a^{2j}p^{2(u+1-i)} \sum_{s=0}^{\phi_{u+1}/k_{u+1}-1} a^{k_{u+1}+sk_{u+1}}p^{r-(u+1)}$$
$$= a^j p^{r-i} - a^{2j}p^{2(u+1-i)}a^{k_{u+1}}p^{r-(u+1)} \equiv 0 \mod 2$$

Thus, by the transformation formula of Proposition 3 and Lemma 9, we see

$$\begin{aligned}
\frac{f_{i,j}}{f_{u+1,k_{u+1}}^{a^{2j}p^{2(u+1-i)}}}(\gamma\tau) &= \frac{E_{a^jp^{r-i}}}{\left(E_{a^{k_{u+1}}p^{r-(u+1)}}\right)^{a^{2j}p^{2(u+1-i)}}}(\gamma\tau) \\
&= \epsilon(\gamma)^{1-a^{2j}p^{2(u+1-i)}} \cdot \frac{E_{a^{j+k}p^{r-i}}}{\left(E_{a^{k_{u+1}+k}p^{r-(u+1)}}\right)^{a^{2j}p^{2(u+1-i)}}}(\tau) \\
&= \epsilon(\gamma)^{1-a^{2j}p^{2(u+1-i)}} \cdot \frac{E_{a^{j+p^{u+1-i}\phi_i}p^{r-i}}}{\left(E_{a^{k_{u+1}+\phi_{u+1}}p^{r-(u+1)}}\right)^{a^{2j}p^{2(u+1-i)}}}(\tau) \\
&= \epsilon(\gamma)^{1-a^{2j}p^{2(u+1-i)}} \cdot (-1)^{p^{u+1-i}-a^{2j}p^{2(u+1-i)}} \\
&\quad \cdot \frac{E_{a^jp^{r-i}}}{\left(E_{a^{k_{u+1}}p^{r-(u+1)}}\right)^{a^{2j}p^{2(u+1-i)}}}(\tau) \\
&= -\epsilon(\gamma)^{1-a^{2j}p^{2(u+1-i)}} \cdot \frac{f_{i,j}}{f_{u+1,k_{u+1}}^{a^{2j}p^{2(u+1-i)}}}(\tau).
\end{aligned}$$

Thus, we get $f_{i,j}/\left(f_{r,k_r}^{b(1-a^{2j}p^{2(u+1-i)})}f_{u+1,k_{u+1}}^{a^{2j}p^{2(u+1-i)}}\right)$ are in $\mathscr{F}(\Gamma)$.

(3.e) Consider

$$\frac{f_{u+1,k_{u+1}}^{p^{2(u+1)-r}}}{f_{r,k_r}^{bp^{2(u+1)-r}}}.$$

We know

$$(\phi_{u+1}/k_{u+1})(p^{2(u+1)-r}) - (\phi_r/k_r)(bp^{2(u+1)-r})$$
$$\equiv 0 \mod 12$$

because $\phi_{u+1}/k_{u+1} = 1$ and $(\phi_r/k_r)b \equiv 1 \mod 12$. Condition (1) of Proposition 4 is satisfied.

In addition,

$$1 - bp^{2(u+1)-r} \equiv 0 \mod 2.$$

because b is odd. Then by combining Proposition 4 with Lemma 10, it suffices to show

$$f^{p^{2(u+1)-r}}_{u+1,k_{u+1}}(\gamma\tau) = -\epsilon(\gamma)^{(\phi_{u+1}/k_{u+1})(p^{2(u+1)-r})} \cdot f^{p^{2(u+1)-r}}_{u+1,k_{u+1}}(\tau)$$
$$= -\epsilon(\gamma)^{p^{2(u+1)-r}} \cdot f^{p^{2(u+1)-r}}_{u+1,k_{u+1}}(\tau)$$

and it satisfies Condition (2) of Proposition 4.

$$p^{2(u+1)-r} \sum_{s=0}^{\phi_{u+1}/k_{u+1}} a^{2k_{u+1}+2sk_{u+1}} p^{2r-2(u+1)}$$
$$= p^{2(u+1)-r} a^{2k_{u+1}} p^{2r-2(u+1)}$$
$$= a^{2k_{u+1}} p^r \equiv 0 \mod 2p^r$$

because $2 \mid a$. In particular, Condition (2) of Proposition 4 is satisfied. Also, we see

$$p^{2(u+1)-r}\sum_{s=0}^{\phi_{u+1}/k_{u+1}} a^{k_{u+1}+sk_{u+1}}p^{r-(u+1)}$$
$$= p^{2(u+1)-r}a^{k_{u+1}}p^{r-(u+1)} \equiv 0 \mod 2$$

Thus, by the transformation formula of Proposition 3 and Lemma 9, we see

$$\begin{aligned} f_{u+1,k_{u+1}}^{p^{2(u+1)-r}}(\gamma\tau) &= E_{a^{k_{u+1}}p^{r-(u+1)}}^{p^{2(u+1)-r}}(\gamma\tau) = \epsilon(\gamma)^{p^{2(u+1)-r}} \cdot E_{a^{k_{u+1}+k}p^{r-(u+1)}}^{p^{2(u+1)-r}}(\tau) \\ &= \epsilon(\gamma)^{p^{2(u+1)-r}} \cdot E_{a^{k_{u+1}+\phi_{u+1}}p^{r-(u+1)}}^{p^{2(u+1)-r}}(\tau) \\ &= \epsilon(\gamma)^{p^{2(u+1)-r}} \cdot (-1)^{p^{2(u+1)-r}} E_{a^{k_{u+1}}p^{r-(u+1)}}^{p^{2(u+1)-r}}(\tau) \\ &= -\epsilon(\gamma)^{p^{2(u+1)-r}} \cdot f_{u+1,k_{u+1}}^{p^{2(u+1)-r}}(\tau). \end{aligned}$$

Therefore, we get $f_{u+1,k_{u+1}}^{p^{2(u+1)-r}} / f_{r,k_r}^{bp^{2(u+1)-r}}$ is in $\mathscr{F}(\Gamma)$.

(3.f) Consider

$$f_{r,k_r}^{12}.$$

Clearly, by Lemma 10 and Proposition 4, f_{r,k_r}^{12} is in $\mathscr{F}(\Gamma)$.

□

Now, we can show the functions in above lemma form a basis for $\mathscr{F}(\Gamma)$.

THEOREM 4.2. *Let $p > 3$ be an odd prime and $r > 0$. Let $k := [\Gamma_0(p^r) : \Gamma] = p^u v$, where $p \nmid v$. For a positive integer ℓ, we set $\phi_\ell = \phi(p^\ell)/2$ and $k_\ell = (k, \phi_\ell)$. Let a be an even generator of $(\mathbb{Z}/p^r\mathbb{Z})^\times$. Suppose $\Gamma \neq \Gamma_1(p^r)$. Then*

(1) *If* $v \neq (p-1)/2$, *let* b *be the multiplicative inverse of* $\phi_r/(k_r \cdot \gcd((p-1)/2v, 12))$ *modulo* $12/\gcd((p-1)/2v, 12)$, *then*

$$\begin{cases} \prod_{s=0}^{\phi_i/k_i-1} E_{a^{j+sk_i p^{r-i}}} \cdot \left(\prod_{s=0}^{\phi_r/k_r-1} E_{a^{sk_r}} \right)^{b\left(\frac{\phi_r/k_r - \phi_i/k_i}{\gcd((p-1)/2v,12)}\right)-1} & \text{for } i = 1, \ldots, r-1 \\ & \text{and } j = 0, \ldots, k_i - 1, \\ \dfrac{\prod_{s=0}^{\phi_r/k_r-1} E_{a^{j+sk_r}}}{\prod_{s=0}^{\phi_r/k_r-1} E_{a^{sk_r}}} & \text{for } j = 1, \ldots, k_r - 1, \\ \left(\prod_{s=0}^{\phi_r/k_r-1} E_{a^{sk_r}} \right)^{\frac{12}{\gcd((p-1)/2v,6)}} \end{cases}$$

form a basis for $\mathscr{F}(\Gamma)$ *modulo* $\mathbb{C}^\times$.

(2) *If* $v = (p-1)/2$ *and* $u < (r-2)/2$, *let* b *be the multiplicative inverse of* ϕ_r/k_r *modulo* 12, *then*

$$\begin{cases} \dfrac{\prod_{s=0}^{\phi_r/k_r-1} E_{a^{j+sk_r}}}{\prod_{s=0}^{\phi_r/k_r-1} E_{a^{sk_r}}} & \text{for } j = 1, \ldots, k_r - 1, \\ \dfrac{\prod_{s=0}^{\phi_i/k_i-1} E_{a^{j+sk_i p^{r-i}}}}{\left(\prod_{s=0}^{\phi_r/k_r-1} E_{a^{sk_r}} \right)^{b(\phi_i/k_i)}} & \text{for } i = 1, \ldots, r-1 \text{ and } j = 0, \ldots, k_i - 1, \\ \left(\prod_{s=0}^{\phi_r/k_r-1} E_{a^{sk_r}} \right)^{12} \end{cases}$$

form a basis for $\mathscr{F}(\Gamma)$ *modulo* $\mathbb{C}^\times$.

(3) *If* $v = (p-1)/2$ *and* $u \geq (r-2)/2$, *let* b *be the multiplicative inverse of* ϕ_r/k_r *modulo* 12, *then*

$$\begin{cases} \dfrac{\prod_{s=0}^{\phi_r/k_r-1} E_{a^{j+sk_r}}}{\prod_{s=0}^{\phi_r/k_r-1} E_{a^{sk_r}}} & \text{for } j = 1, \dots, k_r - 1, \\ \dfrac{\prod_{s=0}^{\phi_i/k_i-1} E_{a^{j+sk_i p^{r-i}}}}{\left(\prod_{s=0}^{\phi_r/k_r-1} E_{a^{sk_r}}\right)^{b(\phi_i/k_i)}} & \text{for } i = u+2, \dots, r-1 \\ & \text{and } j = 0, \dots, k_i - 1, \\ \dfrac{\prod_{s=0}^{\phi_{u+1}/k_{u+1}-1} E_{a^{j+sk_{u+1}p^{r-(u+1)}}}}{\left(\prod_{s=0}^{\phi_r/k_r-1} E_{a^{sk_r}}\right)^{b(1-a^{2j})} \cdot \left(\prod_{s=0}^{\phi_{u+1}/k_{u+1}-1} E_{a^{sk_{u+1}p^{r-(u+1)}}}\right)^{a^{2j}}} & \text{for } j = 1, \dots, k_{u+1} - 1, \\ \dfrac{\prod_{s=0}^{\phi_i/k_i-1} E_{a^{j+sk_i p^{r-i}}}}{\left(\prod_{s=0}^{\phi_r/k_r-1} E_{a^{sk_r}}\right)^{b(1-a^{2j}p^{2(u+1-i)})} \cdot \left(\prod_{s=0}^{\phi_{u+1}/k_{u+1}-1} E_{a^{sk_{u+1}p^{r-(u+1)}}}\right)^{a^{2j}p^{2(u+1-i)}}} & \text{for } i = 1, \dots, u \\ & \text{and } j = 0, \dots, k_i - 1, \\ \dfrac{\left(\prod_{s=0}^{\phi_{u+1}/k_{u+1}-1} E_{a^{sk_{u+1}p^{r-(u+1)}}}\right)^{p^{2(u+1)-r}}}{\left(\prod_{s=0}^{\phi_r/k_r-1} E_{a^{sk_r}}\right)^{bp^{2(u+1)-r}}}, & \\ \left(\prod_{s=0}^{\phi_r/k_r-1} E_{a^{sk_r}}\right)^{12} & \end{cases}$$

form a basis for $\mathscr{F}(\Gamma)$ *modulo* $\mathbb{C}^\times$.

PROOF. For $i = 1, \dots, r$ and $j = 0, \dots, k_i$, let

$$f_{i,j} := \prod_{s=0}^{\phi_i/k_i-1} E_{a^{j+sk_i p^{r-i}}}.$$

We will show this theorem in the three cases, respectively.

(1) Suppose $v \neq (p-1)/2$. Let $f \in \mathscr{F}(\Gamma)$. Then $f \in \mathscr{F}(\Gamma_1(p^r))$. By Lemma 7, $f(\gamma\tau) = f(\tau)$, and Proposition 4, we have

$$f = \prod_{i=1}^{r} \prod_{j=0}^{k_i-1} f_{i,j}^{e_{i,j}}$$

for some integers $e_{i,j}$ satisfying

$$\sum_{i=1}^{r}\sum_{j=0}^{k_i-1}(\phi_i/k_i)e_{i,j} \equiv 0 \mod 12.$$

By Lemma 10, we know

$$f_{i,j}(\gamma\tau) = -\epsilon(\gamma)^{\phi_i/k_i} \cdot f_{i,j}(\tau).$$

Thus, we get

$$f(\gamma\tau) = (-1)^{\sum_{i=1}^{r}\sum_{j=0}^{k_i-1} e_{i,j}} f(\tau).$$

Because $f(\gamma\tau) = f(\tau)$, we know

$$2 \mid \sum_{i=1}^{r}\sum_{j=0}^{k_i-1} e_{i,j}.$$

This tell us

$$\sum_{i=1}^{r}\sum_{j=0}^{k_i-1} e_{i,j} = 2x$$

for some integer x. Combining above two equations of $e_{i,j}$, we get

$$\sum_{i=1}^{r-1}\sum_{j=0}^{k_i-1}(\phi_r/k_r - \phi_i/k_i)e_{i,j} \equiv (2x)(\phi_r/k_r) \mod 12.$$

Then

$$\sum_{i=1}^{r-1}\sum_{j=0}^{k_i-1}\frac{\phi_r/k_r - \phi_i/k_i}{\gcd((p-1)/2v, 12)}e_{i,j} \equiv (2x)\frac{\phi_r/k_r}{\gcd((p-1)/2v, 12)}$$

$$\mod \frac{12}{\gcd((p-1)/2v, 12)}.$$

and thus

$$\sum_{i=1}^{r-1}\sum_{j=0}^{k_i-1} b\left(\frac{\phi_r/k_r-\phi_i/k_i}{\gcd((p-1)/2v,12)}\right)e_{i,j}\equiv(2x)\equiv\sum_{i=1}^{r}\sum_{j=0}^{k_i-1}e_{i,j}$$

$$(*)\qquad \bmod \frac{12}{\gcd((p-1)/2v,12)},$$

where b is the multiplicative inverse of $\phi_r/(k_r\cdot\gcd((p-1)/2v,12))$ modulo $12/\gcd((p-1)/2v,12)$.

If $2\nmid 12/\gcd((p-1)/2v,12)$, then $\gcd((p-1)/2v,12)=4$ or 12, and thus $\gcd((p-1)/2v,6)=2$ or 6, respectively. In addition, because $2(p-1)/(2v)\mid \phi_r/k_r-\phi_i/k_i$ and $2\mid\sum_{i=1}^{r}\sum_{j=0}^{k_i-1}e_{i,j}$, from above equation (*) of $e_{i,j}$, there exists an even integer y' such that

$$\begin{aligned}
e_{r,0} &= -\sum_{j=1}^{k_r-1}e_{r,j}+\sum_{i=1}^{r-1}\sum_{j=0}^{k_i-1}\left(b\left(\frac{\phi_r/k_r-\phi_i/k_i}{\gcd((p-1)/2v,12)}\right)-1\right)e_{i,j}\\
&\qquad +y'\frac{12}{\gcd((p-1)/2v,12)}\\
&= -\sum_{j=1}^{k_r-1}e_{r,j}+\sum_{i=1}^{r-1}\sum_{j=0}^{k_i-1}\left(b\left(\frac{\phi_r/k_r-\phi_i/k_i}{\gcd((p-1)/2v,12)}\right)-1\right)e_{i,j}\\
&\qquad +(y'/2)\frac{24}{\gcd((p-1)/2v,12)}\\
&= -\sum_{j=1}^{k_r-1}e_{r,j}+\sum_{i=1}^{r-1}\sum_{j=0}^{k_i-1}\left(b\left(\frac{\phi_r/k_r-\phi_i/k_i}{\gcd((p-1)/2v,12)}\right)-1\right)e_{i,j}\\
&\qquad +(y'/2)\frac{12}{\gcd((p-1)/2v,6)}.
\end{aligned}$$

Otherwise, $2 \mid 12/\gcd((p-1)/2v, 12)$, then $12/\gcd((p-1)/2v, 12) = 12/\gcd((p-1)/2v, 6)$. Thus, from (*), there exists y''

$$\begin{aligned} e_{r,0} &= -\sum_{j=1}^{k_r-1} e_{r,j} + \sum_{i=1}^{r-1}\sum_{j=0}^{k_i-1}\left(b\left(\frac{\phi_r/k_r - \phi_i/k_i}{\gcd((p-1)/2v, 12)}\right) - 1\right) e_{i,j} \\ &\qquad + y''\frac{12}{\gcd((p-1)/2v, 12)} \\ &= -\sum_{j=1}^{k_r-1} e_{r,j} + \sum_{i=1}^{r-1}\sum_{j=0}^{k_i-1}\left(b\left(\frac{\phi_r/k_r - \phi_i/k_i}{\gcd((p-1)/2v, 12)}\right) - 1\right) e_{i,j} \\ &\qquad + y''\frac{12}{\gcd((p-1)/2v, 6)}. \end{aligned}$$

Set $y = y'/2$ if $2 \nmid 12/\gcd((p-1)/2v, 12)$ and $y = y''$ if $2 \mid 12/\gcd((p-1)/2v, 12)$. Therefore,

$$\begin{aligned} f = \prod_{j=1}^{k_r-1}\left(\frac{f_{r,j}}{f_{r,0}}\right)^{e_{r,j}} \cdot \prod_{i=1}^{r-1}\prod_{j=1}^{k_i-1}\left(f_{i,j}\cdot f_{r,0}^{b\left(\frac{\phi_r/k_r-\phi_i/k_i}{\gcd((p-1)/2v,12)}\right)-1}\right)^{e_{i,j}} \\ \cdot \left(f_{r,0}^{\frac{12}{\gcd((p-1)/2v,6)}}\right)^{y}. \end{aligned}$$

This complete our proof in this case.

(2) Suppose $v = (p-1)/2$ and $u < (r-2)/2$. Let $f \in \mathscr{F}(\Gamma)$. Then $f \in \mathscr{F}(\Gamma_1(p^r))$. By Lemma 7, $f(\gamma\tau) = f(\tau)$, and Proposition 4, we know

$$f = \prod_{i=1}^{r}\prod_{j=0}^{k_i-1} f_{i,j}^{e_{i,j}}$$

for some integers $e_{i,j}$ satisfying

$$\sum_{i=1}^{r}\sum_{j=0}^{k_i-1}(\phi_i/k_i)e_{i,j} \equiv 0 \mod 12.$$

Because $v = (p-1)/2$, we have $\gcd(\phi_r/k_r, 12) = 1$. Then

$$e_{r,0} = -\sum_{j=1}^{k_r-1} e_{r,j} - \sum_{i=1}^{r-1}\sum_{j=0}^{k_i-1} b(\phi_i/k_i)e_{i,j} + 12x$$

for some integer x, where b is the multiplicative inverse of ϕ_r/k_r modulo 12. Therefore, we get

$$f = \prod_{j=1}^{k_r-1}(f_{r,j}/f_{r,0})^{e_{i,j}} \cdot \prod_{i=1}^{r-1}\prod_{j=0}^{k_i-1}\left(f_{i,j}/f_{r,0}^{b(\phi_i/k_i)}\right)^{e_{i,j}} \cdot \left(f_{r,0}^{12}\right)^x.$$

This complete our proof in this case.

(3) Suppose $v = (p-1)/2$ and $u \geq (r-2)/2$. Let $f \in \mathscr{F}(\Gamma)$. Then $f \in \mathscr{F}(\Gamma_1(p^r))$. By Lemma 7, $f(\gamma\tau) = f(\tau)$, and Proposition 4, we get

$$f = \prod_{i=1}^{r}\prod_{j=0}^{k_i-1} f_{i,j}^{e_{i,j}}$$

for some integers $e_{i,j}$ satisfying

$$\sum_{i=1}^{r}\sum_{j=0}^{k_i-1}(\phi_i/k_i)e_{i,j} \equiv 0 \mod 12$$

and

$$\sum_{i=1}^{r}\sum_{j=0}^{k_i-1}\sum_{s=0}^{\phi_i/k_i-1} e_{i,j}a^{2j+2sk_i}p^{2(r-i)} \equiv 0 \mod p^r.$$

Because $v = (p-1)/2$, we have $\gcd(\phi_r/k_r, 12) = 1$. Then from the first equation of $e_{i,j}$, we can get

$$e_{r,0} = -\sum_{j=1}^{k_r-1} e_{r,j} - \sum_{i=1}^{r-1}\sum_{j=0}^{k_i-1} b(\phi_i/k_i)e_{i,j} + 12x$$

for some integer x, where b is the multiplicative inverse of ϕ_r/k_r modulo 12.

Moreover, because $\phi_i/k_i = p^{i-u-1} > 1$ for $i > u+1$ and $\phi_i/k_i = 1$ for $i \leq u+1$, the second equation of $e_{i,j}$ can be reduced to

$$\sum_{i=1}^{u+1}\sum_{j=0}^{k_i-1} e_{i,j}a^{2j}p^{2(u+1-i)} \equiv 0 \mod p^{2(u+1)-r}.$$

Then we get

$$e_{u+1,0} = -\sum_{j=1}^{k_{u+1}-1} e_{u+1,j}a^{2j} - \sum_{i=1}^{u}\sum_{j=0}^{k_i-1} e_{i,j}a^{2j}p^{2(u+1-i)} + p^{2(u+1)-r}y$$

for some integer y.

Combining above two new equations, we have

$$\begin{aligned} e_{r,0} = &-\sum_{j=1}^{k_r-1} e_{r,j} - \sum_{i=u+2}^{r-1}\sum_{j=0}^{k_i-1} b(\phi_i/k_i)e_{i,j} \\ &- \sum_{j=1}^{k_{u+1}-1} b(1-a^{2j})e_{u+1,j} \\ &- \sum_{i=1}^{u}\sum_{j=0}^{k_i-1} b(1-a^{2j}p^{2(u+1-i)})e_{i,j} \\ &+ 12x - bp^{2(u+1)-r}y. \end{aligned}$$

Hence, we have

$$\begin{aligned} f = &\prod_{j=1}^{k_r-1}\left(\frac{f_{r,j}}{f_{r,0}}\right)^{e_{r,j}} \cdot \prod_{i=u+2}^{r-1}\prod_{j=0}^{k_i-1}\left(\frac{f_{i,j}}{f_{r,0}^{b(\phi_i/k_i)}}\right)^{e_{i,j}} \\ &\cdot \prod_{j=1}^{k_{u+1}-1}\left(\frac{f_{u+1,j}}{f_{r,0}^{b(1-a^{2j})}f_{u+1,0}^{a^{2j}}}\right)^{e_{u+1,j}} \\ &\cdot \prod_{i=1}^{u}\prod_{j=0}^{k_i-1}\left(\frac{f_{i,j}}{f_{r,0}^{b(1-a^{2j}p^{2(u+1-i)})}f_{u+1,0}^{a^{2j}p^{2(u+1-i)}}}\right)^{e_{i,j}} \\ &\cdot \left(\frac{f_{u+1,0}^{p^{2(u+1)-r}}}{f_{r,0}^{bp^{2(u+1)-r}}}\right)^{y} \cdot \left(f_{r,0}^{12}\right)^{x}. \end{aligned}$$

We finish the proof of this theorem.

□

REMARK. When $k = 1$, that is, $\Gamma = \Gamma_0(p^r)$, let b be the multiplicative inverse of $\phi_r/\gcd((p-1)/2, 12)$ modulo $12/\gcd((p-1)/2, 12)$, and then

$$\prod_{s=0}^{\phi_i - 1} E_{a^s p^{r-i}} \cdot \left(\prod_{s=0}^{\phi_r - 1} E_{a^s} \right)^{b\left(\frac{\phi_r - \phi_i}{\gcd((p-1)/2,12)}\right)-1}$$
$$= \left(\frac{\eta(p^{r-i}\tau)}{\eta(p^{r-i+1}\tau)} \right) \left(\frac{\eta(\tau)}{\eta(p\tau)} \right)^{b\left(\frac{\phi_r - \phi_i}{\gcd((p-1)/2,12)}\right)-1}$$

for $i = 1, \ldots, r-1$, and

$$\left(\prod_{s=0}^{\phi_r - 1} E_{a^s} \right)^{\frac{12}{\gcd((p-1)/2,6)}} = \left(\frac{\eta(\tau)}{\eta(p\tau)} \right)^{\frac{12}{\gcd((p-1)/2,6)}}$$

form a basis for $\mathscr{F}(\Gamma_0(p^r))$.

4. Application

In this section, as a corollary of above theorems, we will compute the order $h(\Gamma)$ of cuspidal $\mathbb{Q}$-rational torsion subgroup of $J(\Gamma)$ when $\Gamma = \Gamma_1(p^r), \Gamma_0(p^r)$.

Before computing the order, we need the following elementary lemma from linear algebra.

LEMMA 12. *Let $p > 3$ be an odd prime and $r > 0$. Let $k := [\Gamma_0(p^r) : \Gamma] = p^u v$, where $p \nmid v$. For a positive integer ℓ, we set $\phi_\ell = \phi(p^\ell)/2$ and $k_\ell := \gcd(k, \phi_\ell)$. For $j = 0, \ldots, r-1$, set $d_j = \sum_{s=0}^{j} k_{r-s}$. Let $n := d_{r-1} + 1$. Let $\Lambda \subset \mathbb{R}^n$ be the lattice of dimension $n-1$ generated by the vectors*

$$\epsilon_i = (1, 0, \ldots, -1, 0, \ldots)$$

with the -1 *appearing at* $i+1$ *entry for* $i = 1, \ldots, k_r - 1$,

$$\epsilon_i = (2\phi_j, 0, \ldots, -1, 0, \ldots)$$

with the -1 *appearing at* $i+1$ *entry for* $j = 1, \ldots, r - \min\{r/2, r-u-1\}$ *and* $d_{j-1} \leq i \leq d_j - 1$,

$$\epsilon_i = (2\phi_{r-j}k/k_{r-j}, 0, \ldots, -1, 0, \ldots)$$

with the -1 *appearing at* $i+1$ *entry for* $j = r - \min\{r/2, r-u-1\} + 1, \ldots, r-1$ *and* $d_{j-1} \leq i \leq d_j - 1$, *and*

$$\epsilon_{n-1} = (k_r, 0, \ldots, -1).$$

Let Λ' *be a sublattice of* Λ *of the same rank generated by* $v_1, \ldots, v_{n-1}$. *Let* $v_n = (c_1, \ldots, c_n)$ *be any vector such that*

$$c := \sum_{i=1}^{k_r} c_i + \sum_{j=1}^{r-\min\{r/2,r-u-1\}} \sum_{i=1}^{k_{r-j}} 2\phi_j c_{i+d_{j-1}} + \sum_{j=r-\min\{r/2,r-u-1\}}^{r-1} \sum_{i=1}^{k_{r-j}} (2\phi_{r-j}k/k_{r-j}) c_{i+d_{j-1}} + k_r c_n \neq 0,$$

and M *be the* $n \times n$ *matrix whose* i*th row is* v_i. *Then we have*

$$(\Lambda : \Lambda') = |c^{-1} \det M|.$$

PROOF. In general, to determine the index of a sublattice Λ' in a lattice Λ of codimension 1 in $\mathbb{R}^n$, we pick a nonzero vector x in $\mathbb{R}^n$ that is orthogonal to Λ, and form two matrices A and A', where the rows of A are generators of Λ and x, while those of A' are generators of Λ' and x. Then the index of Λ' in Λ is equal to $|\det A'/\det A|$.

Now for the lattice Λ generated by ϵ_i, we can choose the vector $x = (x_1, \ldots, x_n) \in \mathbb{R}^n$ with

$$\begin{cases} x_i = 1, & \text{if } i = 1, \ldots, k_r, \\ x_i = 2\phi_j, & \text{if } j = 1, \ldots, r - \min\{r/2, r-u-1\} \\ & \qquad \text{and } d_{j-1} + 1 \le i \le d_j, \\ x_i = 2\phi_{r-j} k / k_{r-j}, & \text{if } j = r - \min\{r/2, r-u-1\} + 1, \ldots, r-1 \\ & \qquad \text{and } d_{j-1} + 1 \le i \le d_j, \\ x_n = k_r. \end{cases}$$

Then

$$\begin{aligned} \det(A) = & k_r + 4 \sum_{j=1}^{r - \min\{r/2, r-u-1\}} k_{r-j} \phi_j^2 \\ & + 4 \sum_{j=r-\min\{r/2, r-u-1\}+1}^{r-1} k_{r-j} \phi_{r-j}^2 k^2 / k_{r-j}^2 + k_r^2. \end{aligned}$$

On the other word, for the matrix M in the lemma, by adding suitable multiples of the first $n-1$ rows to the last row, we can bring the last row into $(c, 0, \ldots, 0)$. Note that this procedure does not change the determinant. By the same token, we can also transform the matrix A' corresponding to Λ' into a matrix whose first $n-1$ rows are v_i and whose last row is $(\det(A), 0, \ldots, 0)$ without changing the determinant. From this, we see that $c^{-1} \cdot \det M = (\det A)^{-1} \cdot \det A'$, and therefore $(\Lambda : \Lambda') = |c^{-1} \det M|$. $\square$

Now we can compute the order $h(\Gamma_1(p^r))$.

LEMMA 13. *Let $p > 3$ be a prime and $r > 0$. For a positive integer ℓ, we set $\phi_\ell = \phi(p^\ell)/2$. Let $B_2(x) = \{x\}^2 - \{x\} + 1/6$, where $\{x\}$ denotes*

the fractional part of a real number x. Then we have

$$h(\Gamma_1(p^r)) = (\phi_r)^{-1} 12 p^c |\det B|,$$

where $c = r + \sum_{i=1}^{r} i\phi_i$ and B is the $(\sum_{i=1}^{r} \phi_i) \times (\sum_{i=1}^{r} \phi_i)$ symmetric matrix with row vectors

$$\left\{ \overrightarrow{B^{i,j}} \right\}_{i=r,\ldots,1; j=0,\ldots,\phi_i - 1}$$

which have entries

$$\begin{cases} \frac{1}{2} B_2\left(\frac{a^{j+s}}{p^i}\right), & \text{if } s = 0, \ldots, \phi_r - 1, \\ \frac{1}{2} B_2\left(\frac{a^{j+s}}{p^{i-n}}\right), & \text{if } n = 1, \ldots, i-1 \text{ and } s = 0, \ldots, \phi_{r-n} - 1, \\ \frac{1}{12}, & \text{if } n = i, \ldots, r-1 \text{ and } s = 0, \ldots, \phi_{r-n} - 1. \end{cases}$$

PROOF. Let

$$c_0^{(0)} := 1/6.$$

For $i = 1, \ldots, r$ and $j = 0(\mod \phi_i), \ldots, \phi_i - 1(\mod \phi_i)$, set

$$c_j^{(i)} := B_2\left(\frac{a^j}{p^i}\right),$$

where $B_2(x) = \{x\}^2 - \{x\} + 1/6$.

For $i = r, r-1, \ldots, 1$ and $j = 0, \ldots, \phi_i - 1$, by Lemma 1 and Proposition 5, it is easy to see

$$\begin{aligned}\operatorname{div}(E_{a^j p^{r-i}}) = &\sum_{s=0}^{\phi_r - 1} \frac{p^r}{2} c_{j+s}^{i} \left(\frac{a^s}{p^r}\right) \\ &+ \sum_{n=1}^{i-1} \sum_{s=0}^{\phi_{r-n}-1} \sum_{t=0}^{2\phi_n - 1} \frac{p^{r-n}}{2} c_{j+s}^{(i-n)} \left(\frac{a^s}{p^{r-n} b^t}\right) \\ &+ \sum_{n=i}^{r-1} \sum_{s=0}^{\phi_{r-n}-1} \sum_{t=0}^{2\phi_n - 1} \frac{p^{r-n}}{2} c_{0}^{(0)} \left(\frac{a^s}{p^{r-n} b^t}\right) \\ &+ \sum_{t=0}^{\phi_r - 1} \frac{1}{2} c_0^{(0)} \left(\frac{1}{b^t}\right).\end{aligned}$$

Set $d_n := \sum_{t=0}^{n} \phi_{r-t}$ for $n = 0, \ldots, r-1$. Denote $\overrightarrow{\operatorname{div}(E_{a^j p^{r-i}})} \in \mathbb{R}^{d_{r-1}}$ by

$$\begin{cases} \overrightarrow{\operatorname{div}(E_{a^j p^{r-i}})}_{s+1} = \frac{p^r}{2} c_{j+s}^{i}, & \text{if } s = 0, \ldots, \phi_r - 1, \\ \overrightarrow{\operatorname{div}(E_{a^j p^{r-i}})}_{s+d_{n-1}+1} = \frac{p^{r-n}}{2} c_{j+s}^{i-n}, & \text{if } n = 1, \ldots, i-1 \\ & \text{and } s = 0, \ldots, \phi_{r-n} - 1, \\ \overrightarrow{\operatorname{div}(E_{a^j p^{r-i}})}_{s+d_{n-1}+1} = \frac{p^{r-n}}{2} c_0^0, & \text{if } n = i, \ldots, r-1 \\ & \text{and } s = 0, \ldots, \phi_{r-n} - 1. \end{cases}$$

Thus, from Theorem 4.1 and Lemma 12(with the choice of $v_{d_{r-1}+1} = (0, \ldots, 0, 1)$), we know

$$\begin{aligned} h(\Gamma_1(p^r)) &= (\phi_r)^{-1} 12 p^r \left| \det \left[\overrightarrow{\operatorname{div}(E_{a^j p^{r-i}})} \right] \right| \\ &= (\phi_r)^{-1} (12 p^r)(p^{r\phi_r} \cdot p^{(r-1)\phi_{r-1}} \cdot \cdots \cdot p^{\phi_1}) |\det B| \\ &= (\phi_r)^{-1} 12 p^c |\det B|, \end{aligned}$$

where $c = r + \sum_{i=1}^{r} i\phi_i$ and $\left[\overrightarrow{\operatorname{div}(E_{a^j p^{r-i}})}\right]$ means the $(\sum_{i=1}^{r}\phi_i)\times(\sum_{i=1}^{r}\phi_i)$ matrix with row vectors

$$\overrightarrow{\operatorname{div}(E_{a^j p^{r-i}})}$$

and B is the matrix described in the theorem. □

Now, we compute the determinant of B in the above lemma.

LEMMA 14. *All notations as above. Then we have*

$$|\det(B)| = \left(\frac{p-1}{24}\right)\cdot\left(\frac{(p-1)(p+1)}{24}\right)^{r-1}\cdot p^c \cdot \prod_{i=1}^{r}\prod_{\chi\neq\chi_0 \bmod p^i,\, even}\frac{1}{4}B_{2,\chi \bmod p^i},$$

where

$$c := -r + 1 - \sum_{i=1}^{r} i\phi_i + 2\sum_{m=1}^{r-1} m\phi_{r-m},$$

and the innermost product is taken over all even nonprincipal Dirichlet characters modulo p^i for $i = 1, \ldots, r$.

PROOF. Let $\xi = e^{2\pi i/\phi_r}$. For $s, t > 0$, set

$$\overrightarrow{\xi^{s,t}} = \begin{pmatrix} 1 & \xi^s & \cdots & (\xi^s)^{\phi_t - 1}\end{pmatrix}$$

and

$$\overrightarrow{0_t} = \begin{pmatrix} 0 & \cdots & 0\end{pmatrix}$$

with t 0's.

For $s = 1, \ldots, \phi_r - 1$, if $p^{m_s} \mid s$ and $p^{m_s+1} \nmid s$, where $0 \le m_s \le r-1$, define W_s by the subspace of $\mathbb{R}^{(\sum_{i=1}^{r}\phi_i)\times 1}$ generated by

$$\epsilon_s^t = \begin{pmatrix}\overrightarrow{0_{\sum_{i=t+1}^{r}\phi_i}} & \overrightarrow{\xi^{s,t}} & \overrightarrow{0_{\sum_{i=1}^{t-1}\phi_i}}\end{pmatrix}^T,$$

where $t = r, r-1, \ldots, r-m_s$. Also, for $s = 0$, let $m_s = r$. Then define W_0 by the subspace of $\mathbb{R}^{(\sum_{i=1}^{r}\phi_i)\times 1}$ generated by

$$\epsilon_0^t = \left(\overrightarrow{0_{\sum_{i=t+1}^{r}\phi_i}} \quad \overrightarrow{\xi^{0,t}} \quad \overrightarrow{0_{\sum_{i=1}^{t-1}\phi_i}}\right)^T,$$

where $t = r, r-1, \ldots, 1$.

Clearly, $\mathbb{R}^{(\sum_{i=1}^{r}\phi_i)\times 1} = \oplus W_s$. After suitable rows interchanges of B, we claim

$$B(W_s) \subset W_s$$

and compute

$$\det(B|W_s).$$

Then we can get $\det(B)$.

Given $s \in \{1, \ldots, \phi_r - 1\}$ with $0 \le m_s \le r-1$. For $t = r, r-1, \ldots, r-m_s$, by Lemma 6, we know

$$\begin{aligned}
\sum_{j=0}^{\phi_t-1}\frac{1}{2}B_2\left(\frac{a^j}{p^\ell}\right)(\xi^s)^j &= \frac{1}{2}\sum_{j=0}^{\phi_\ell-1}B_2\left(\frac{a^j}{p^\ell}\right)\sum_{i=0}^{p^{t-\ell}-1}(\xi^s)^{j+i\phi_\ell} \\
&= \frac{p^{t-\ell}}{2}\sum_{j=0}^{\phi_\ell-1}B_2\left(\frac{a^j}{p^\ell}\right)(\xi^s)^j \\
&= \frac{p^{t-\ell}}{2}\sum_{j=0}^{\phi_\ell-1}\left(\frac{p^{t-\ell}}{2}\sum_{i=0}^{p^{t-\ell}-1}B_2\left(\frac{a^{j+i\phi_\ell}}{p^t}\right)\right)(\xi^s)^j \\
&= \frac{p^{2(t-\ell)}}{2}\sum_{j=0}^{\phi_\ell-1}\sum_{i=0}^{p^{t-\ell}-1}B_2\left(\frac{a^{j+i\phi_\ell}}{p^t}\right)(\xi^s)^{j+i\phi_\ell} \\
&= \frac{p^{2(t-\ell)}}{2}\sum_{j=0}^{\phi_t-1}B_2\left(\frac{a^j}{p^t}\right)(\xi^s)^j
\end{aligned}$$

when $r - m_s \le \ell \le t$,

$$\sum_{j=0}^{\phi_t-1}\frac{1}{2}B_2\left(\frac{a^j}{p^\ell}\right)(\xi^s)^j = 0$$

when $0 < \ell < r - m_s$, and

$$\sum_{j=0}^{\phi_t - 1} \frac{1}{12} (\xi^s)^j = 0.$$

Hence, by suitable rows interchanges of B, we have

$$B\epsilon_s^t = \left(\sum_{j=0}^{\phi_t - 1} \frac{1}{2} B_2 \left(\frac{a^j}{p^t} \right) (\xi^s)^j \right) \cdot \left(\epsilon_s^r + p^2 \epsilon_s^{r-1} + \cdots + p^{2(t-r+m_s)} \epsilon_s^{2r-t-m_s} \right)$$

for $t = r, r-1, \ldots, r-m_s$. Then we get

$$\det(B|W_s) = p^{m_s(m_s+1)} \cdot \prod_{t=r-m_s}^{r} \sum_{j=0}^{\phi_t - 1} \frac{1}{2} B_2 \left(\frac{a^j}{p^t} \right) (\xi^s)^j.$$

For $s = 0$ with $m_s = r$, similarly, by Lemma 6, we have

$$B\epsilon_0^t = \left(\frac{1}{2} \sum_{j=0}^{\phi_t - 1} B_2 \left(\frac{a^j}{p^t} \right) \right) \cdot \left(\epsilon_0^r + p^2 \epsilon_0^{r-1} + \cdots + p^{2(t-1)} \epsilon_0^{r-t+1} - p^{2t-1} \epsilon_0^{r-t} - \cdots - p^{2t-1} \epsilon_0^1 \right),$$

where $t = r, r-1, \ldots, 1$. Thus, we get

$$\begin{aligned} \det(B|W_0) &= (-1)^{r-1} \prod_{i=1}^{r-1} p^{2i-1}(1+p) \cdot \prod_{i=1}^{r} \sum_{j=0}^{\phi_i - 1} \frac{1}{2} B_2 \left(\frac{a^j}{p^i} \right) \\ &= (-1)^{r-1} p^{(r-1)^2} \cdot (p+1)^{r-1} \cdot \prod_{i=1}^{r} \sum_{j=0}^{\phi_i - 1} \frac{1}{2} B_2 \left(\frac{a^j}{p^i} \right). \end{aligned}$$

Set $\phi_0 := 1$. For fixed $m \in \{0, 1, \ldots, r-1\}$, there are $\phi_{r-m} - \phi_{r-m-1}$ s's in $\{1, \ldots, \phi_r - 1\}$ with $m_s = m$ such that $p^m \mid s$ and $p^{m+1} \nmid s$. Thus,

by combing with above results, we know

$$\begin{aligned}|\det(B)| &= \prod_s |\det(B|W_s)| \\ &= \left| p^{(r-1)^2} \cdot (p+1)^{r-1} \cdot \prod_{m=0}^{r-1} (p^{m(m+1)})^{\phi_{r-m}-\phi_{r-m-1}} \right| \\ &\quad \cdot \left| \prod_{i=1}^{r} \prod_{s=0}^{\phi_i-1} \sum_{j=0}^{\phi_i-1} \frac{1}{2} B_2\left(\frac{a^j}{p^i}\right) (\xi^{p^{r-i}s})^j \right|.\end{aligned}$$

Recall that for a Dirichlet character χ modulo N, where $N \in \mathbb{N}$,

$$B_{2,\chi} = N \sum_{k=1}^{N} \chi(k) B_2\left(\frac{k}{N}\right).$$

Hence, we can reduce the product to

$$\left| p^{(r-1)^2} \cdot (p+1)^{r-1} \cdot \prod_{m=1}^{r-1} (p^{m(m+1)})^{\phi_{r-m}-\phi_{r-m-1}} \right| \cdot \left| \prod_{i=1}^{r} (p^{-i})^{\phi_i} \cdot \prod_{i=1}^{r} \prod_{\chi \bmod p^i, even} \frac{1}{4} B_{2,\chi \bmod p^i} \right|.$$

Note that

$$\begin{aligned}
&\sum_{m=1}^{r-1} m(m+1)(\phi_{r-m}-\phi_{r-m-1}) \\
&\quad=\sum_{m=1}^{r-1} m(m+1)\phi_{r-m}-\sum_{m=1}^{r-1} m(m+1)\phi_{r-m-1} \\
&\quad=\left(2\phi_{r-1}+\sum_{m=2}^{r-1} m(m+1)\phi_{r-m}\right) \\
&\qquad-\left((r-1)r+\sum_{m=1}^{r-2} m(m+1)\phi_{r-m-1}\right) \\
&\quad=\left(2\phi_{r-1}+\sum_{m=2}^{r-1} m(m+1)\phi_{r-m}\right) \\
&\qquad-\left((r-1)r+\sum_{m=2}^{r-1}(m-1)m\phi_{r-m}\right) \\
&\quad=2\phi_{r-1}-(r-1)r+\sum_{m=2}^{r-1} 2m\phi_{r-m} \\
&\quad=-(r-1)r+\sum_{m=1}^{r-1} 2m\phi_{r-m}.
\end{aligned}$$

Then the above product is equal to

$$\begin{aligned}
&\left|p^{(r-1)^2}\cdot(p+1)^{r-1}\cdot p^{-(r-1)r+2\sum_{m=1}^{r-1} m\phi_{r-m}}\right| \\
&\qquad\cdot\left|p^{-\sum_{i=1}^{r} i\phi_i}\cdot\prod_{i=1}^{r}\prod_{\chi \bmod p^i,\,even}\frac{1}{4}B_{2,\chi \bmod p^i}\right| \\
&\quad=\left|(p+1)^{r-1}\cdot p^{-r+1-\sum_{i=1}^{r} i\phi_i+2\sum_{m=1}^{r-1} m\phi_{r-m}}\right| \\
&\qquad\cdot\left|\prod_{i=1}^{r}\prod_{\chi \bmod p^i,\,even}\frac{1}{4}B_{2,\chi \bmod p^i}\right|.
\end{aligned}$$

By Lemma 6, the above product equals

$$\left(\frac{p-1}{24}\right)\cdot\left(\frac{(p-1)(p+1)}{24}\right)^{r-1}\cdot p^{-r+1-\sum_{i=1}^{r} i\phi_i+2\sum_{m=1}^{r-1} m\phi_{r-m}}$$
$$\cdot\prod_{i=1}^{r}\prod_{\chi\neq\chi_0 \bmod p^i,\textit{even}}\frac{1}{4}B_{2,\chi \bmod p^i}.$$

□

By combining above two lemmas, we can prove Theorem 1.1.

PROOF OF THEOREM 1.1. By Lemma 13 and Lemma 14, we get

$$\begin{aligned}
&h(\Gamma_1(p^r))\\
&=(\phi_r)^{-1}12p^{r+\sum_{i=1}^{r} i\phi_i}\cdot\left(\frac{p-1}{24}\right)\cdot\left(\frac{(p-1)(p+1)}{24}\right)^{r-1}\\
&\quad\cdot p^{-r+1-\sum_{i=1}^{r} i\phi_i+2\sum_{m=1}^{r-1} m\phi_{r-m}}\cdot\prod_{i=1}^{r}\prod_{\chi\neq\chi_0 \bmod p^i,\textit{even}}\frac{1}{4}B_{2,\chi \bmod p^i}\\
&=\left(\frac{(p-1)(p+1)}{24}\right)^{r-1}\cdot p^{-r+2+2\sum_{i=1}^{r-1} i\phi_{r-i}}\\
&\quad\cdot\prod_{i=1}^{r}\prod_{\chi\neq\chi_0 \bmod p^i,\textit{even}}\frac{1}{4}B_{2,\chi \bmod p^i}.
\end{aligned}$$

Since

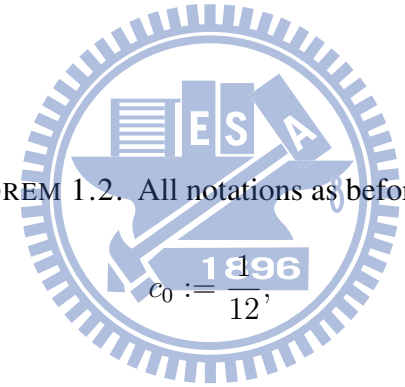
$$\begin{aligned}
2\sum_{i=1}^{r-1} i\phi_{r-i}&=\sum_{i=1}^{r-1} i(p^{r-i}-p^{r-i-1})=\sum_{i=1}^{r-1} ip^{r-i}-\sum_{i=1}^{r-1} ip^{r-i-1}\\
&=\sum_{i=1}^{r-1} ip^{r-i}-\sum_{i=2}^{r}(i-1)p^{r-i}\\
&=p^{r-1}-(r-1)+\sum_{i=2}^{r-1}(i-(i-1))p^{r-i}\\
&=-(r-1)+\sum_{i=1}^{r-1}p^{r-i}=\left(\frac{p^r-p}{p-1}\right)-r+1,
\end{aligned}$$

the above product is equal to

$$\left(\frac{(p-1)(p+1)}{24}\right)^{r-1} \cdot p^{(\frac{p^r-p}{p-1})-2r+3} \cdot \prod_{i=1}^{r} \prod_{\chi \neq \chi_0 \bmod p^i, even} \frac{1}{4} B_{2,\chi \bmod p^i}.$$

□

Next, we give a proof of Theorem 1.2.



PROOF OF THEOREM 1.2. All notations as before. Set

$$c_0 := \frac{1}{12},$$

and

$$c_i := \frac{1}{2} \sum_{s=0}^{\phi_i - 1} B_2\left(\frac{a^s}{p^i}\right)$$

for $i = 1, \ldots, r$.

For $i = r, r-1, \ldots, 1$, by Lemma 1 and Proposition 5, we know

$$\begin{aligned} \operatorname{div}\left(\prod_{j=0}^{\phi_i - 1} E_{a^j p^{r-i}}\right) = {} & p^r c_i\left(\frac{1}{p^r}\right) \\ & + \sum_{n=1}^{i-1} \sum_{t=0}^{\min\{2\phi_{r-n}, 2\phi_n\}} p^r c_{i-n}\left(\frac{1}{p^{r-n} b^t}\right) \\ & + \sum_{n=i}^{r-1} \sum_{t=0}^{\min\{2\phi_{r-n}, 2\phi_n\}} p^{r-n} \phi_i c_0\left(\frac{1}{p^{r-n} b^t}\right) \\ & + \phi_i c_0(1). \end{aligned}$$

Denote $\overrightarrow{\operatorname{div}\left(\prod_{j=0}^{\phi_i-1} E_{a^j p^{r-i}}\right)} \in \mathbb{R}^r$ by

$$\begin{cases} \overrightarrow{\operatorname{div}\left(\prod_{j=0}^{\phi_i-1} E_{a^j p^{r-i}}\right)}_1 = p^r c_i, \\ \overrightarrow{\operatorname{div}\left(\prod_{j=0}^{\phi_i-1} E_{a^j p^{r-i}}\right)}_{n+1} = p^r c_{i-n}, & \text{if } n = 1, \dots, i-1, \\ \overrightarrow{\operatorname{div}\left(\prod_{j=0}^{\phi_i-1} E_{a^j p^{r-i}}\right)}_{n+1} = p^{r-n}\phi_i c_0, & \text{if } n = i, \dots, r-1. \end{cases}$$

Let M mean the $r \times r$ matrix with row vectors

$$\overrightarrow{\operatorname{div}\left(\prod_{j=0}^{\phi_i-1} E_{a^j p^{r-i}}\right)}.$$

By Theorem 4.2 and Lemma 12(with the choice of $v_{r+1} = (0, \dots, 0, 1)$), we get that

$$h(\Gamma_0(p^r)) = \frac{12}{\gcd(\frac{p-1}{2}, 6)} |\det M|.$$

Thus, it remains to compute $|\det M|$. We have

$$|\det M| = \left| \det \begin{pmatrix} p^r c_r & p^r c_{r-1} & p^r c_{r-2} & \dots & p^r c_2 & p^r c_1 \\ p^r c_{r-1} & p^r c_{r-2} & p^r c_{r-3} & \dots & p^r c_1 & p\phi_{r-1} c_0 \\ p^r c_{r-2} & p^r c_{r-3} & p^r c_{r-4} & \dots & p^2\phi_{r-2} c_0 & p\phi_{r-2} c_0 \\ \vdots & \vdots & \vdots & \dots & \vdots & \vdots \\ p^r c_2 & p^r c_1 & p^{r-2}\phi_2 c_0 & \dots & p^2\phi_2 c_0 & p\phi_2 c_0 \\ p^r c_1 & p^{r-1}\phi_1 c_0 & p^{r-2}\phi_1 c_0 & \dots & p^2\phi_1 c_0 & p\phi_1 c_0 \end{pmatrix} \right|.$$

From Lemma 6, we know

$$c_i = p^{r-i} c_r$$

for $i = 1, \ldots, r$, and

$$c := p^r c_r = \frac{1-p}{24}.$$

Thus,

$$|\det M| = \left| \det \begin{pmatrix} c & pc & p^2c & \dots & p^{r-2}c & p^{r-1}c \\ pc & p^2c & p^3c & \dots & p^{r-1}c & p\phi_{r-1}c_0 \\ p^2c & p^3c & p^4c & \dots & p^2\phi_{r-2}c_0 & p\phi_{r-2}c_0 \\ \vdots & \vdots & \vdots & \dots & \vdots & \vdots \\ p^{r-2}c & p^{r-1}c & p^{r-2}\phi_2 c_0 & \dots & p^2\phi_2 c_0 & p\phi_2 c_0 \\ p^{r-1}c & p^{r-1}\phi_1 c_0 & p^{r-2}\phi_1 c_0 & \dots & p^2\phi_1 c_0 & p\phi_1 c_0 \end{pmatrix} \right|$$

$$= \left| \det \begin{pmatrix} c & pc & p^2c & \dots & p^{r-2}c & p^{r-1}c \\ 0 & 0 & 0 & \dots & 0 & -p^r c + p\phi_{r-1}c_0 \\ 0 & 0 & 0 & \dots & -p^r c + p^2\phi_{r-2}c_0 & -p^{r+1}c + p\phi_{r-2}c_0 \\ \vdots & \vdots & \vdots & \dots & \vdots & \vdots \\ 0 & 0 & -p^r c + p^{r-2}\phi_2 c_0 & \dots & -p^{2r-4}c + p^2\phi_2 c_0 & -p^{2r-3}c + p\phi_2 c_0 \\ 0 & -p^r c + p^{r-1}\phi_1 c_0 & -p^{r+1}c + p^{r-2}\phi_1 c_0 & \dots & -p^{2r-3}c + p^2\phi_1 c_0 & -p^{2r-2}c + p\phi_1 c_0 \end{pmatrix} \right|$$

$$= \left| c \prod_{i=1}^{r-1} (-p^r c + p^i \phi_{r-i} c_0) \right|$$

$$= \left| \left(\frac{1-p}{24}\right) \cdot \prod_{i=1}^{r-1} \left(-p^r \left(\frac{1-p}{24}\right) + p^i p^{r-i-1} \left(\frac{p-1}{24}\right) \right) \right|$$

$$= \left| \left(\frac{p-1}{24}\right) \cdot p^{(r-1)^2} \cdot \left(p \left(\frac{p-1}{24}\right) + \frac{p-1}{24} \right)^{r-1} \right|$$

$$= \left(\frac{p-1}{24}\right) \cdot p^{(r-1)^2} \cdot \left(\frac{(p+1)(p-1)}{24}\right)^{r-1}.$$

Therefore, we get

$$\begin{aligned} h(\Gamma_0(p^r)) &= \frac{12}{\gcd(\frac{p-1}{2}, 6)} |\det M| \\ &= \frac{\frac{p-1}{2}}{\gcd(\frac{p-1}{2}, 6)} \cdot p^{(r-1)^2} \cdot \left(\frac{(p+1)(p-1)}{24}\right)^{r-1} \\ &= \frac{p-1}{\gcd(p-1, 12)} \cdot p^{(r-1)^2} \cdot \left(\frac{(p+1)(p-1)}{24}\right)^{r-1}. \end{aligned}$$

□

Similarly, for $r = 1$, we have

THEOREM 4.3. *Let $p > 3$ be an odd prime, $n := [\Gamma : \Gamma_1(p)]$, and $k := [\Gamma_0(p) : \Gamma]$. Then*

$$h(\Gamma) = p^c \frac{n}{(6, n)} \prod_{\chi \neq \chi_0,\, \chi^k = \chi_0,\, \textit{even}} \frac{1}{4} B_{2,\chi},$$

where the product is taken over all even nonprincipal Dirichlet characters χ modulo p satisfying $\chi^k = \chi_0$, and

$$c = \begin{cases} 1 & \textit{if } \Gamma = \Gamma_1(p), \\ 0 & \textit{otherwise}. \end{cases}$$

(For $\Gamma = \Gamma_0(p)$, the product is empty and should be interpreted as 1.)

Bibliography

[1] Seng-Kiat Chua and San Ling. On the rational cuspidal subgroup and the rational torsion points of $J_0(pq)$. *Proc. Amer. Math. Soc.*, 125(8):2255–2263, 1997.

[2] Brian Conrad, Bas Edixhoven, and William Stein. $J_1(p)$ has connected fibers. *Doc. Math.*, 8:331–408 (electronic), 2003.

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

[4] S. Klimek. PhD thesis, University of California at Berkeley, 1975.

[5] Dan Kubert and Serge Lang. Units in the modular function field. I. *Math. Ann.*, 218(1):67–96, 1975.

[6] Dan Kubert and Serge Lang. Units in the modular function field. II. A full set of units. *Math. Ann.*, 218(2):175–189, 1975.

[7] Dan Kubert and Serge Lang. Units in the modular function field. III. Distribution relations. *Math. Ann.*, 218(3):273–285, 1975.

[8] Daniel Kubert and Serge Lang. Units in the modular function field. IV. The Siegel functions are generators. *Math. Ann.*, 227(3):223–242, 1977.

[9] Daniel S. Kubert and Serge Lang. The index of Stickelberger ideals of order 2 and cuspidal class numbers. *Math. Ann.*, 237(3):213–232, 1978.

[10] Daniel S. Kubert and Serge Lang. Units in the modular function field. V. Iwasawa theory in the modular tower. *Math. Ann.*, 237(2):97–104, 1978.

[11] Daniel S. Kubert and Serge Lang. *Modular units*, volume 244 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Science]*. Springer-Verlag, 1981.

[12] San Ling. On the $\mathbf{Q}$-rational cuspidal subgroup and the component group of $J_0(p^r)$. *Israel J. Math.*, 99:29–54, 1997.

[13] Ju. I. Manin. Parabolic points and zeta functions of modular curves. *Izv. Akad. Nauk SSSR Ser. Mat.*, 36:19–66, 1972.

[14] B. Mazur. Modular curves and the Eisenstein ideal. *Inst. Hautes Études Sci. Publ. Math.*, (47):33–186 (1978), 1977.

[15] Rick Miranda. *Algebraic curves and Riemann surfaces*, volume 5 of *Graduate Studies in Mathematics*. American Mathematical Society, 1995.

[16] Morris Newman. Construction and application of a class of modular functions. *Proc. London. Math. Soc. (3)*, 7:334–350, 1957.

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

[18] A. P. Ogg. Rational points on certain elliptic modular curves. In *Analytic number theory (Proc. Sympos. Pure Math., Vol XXIV, St. Louis Univ., St. Louis, Mo., 1972)*, pages 221–231. Amer. Math. Soc., 1973.

[19] A. P. Ogg. Diophantine equations and modular forms. *Bull. Amer. Math. Soc.*, 81:14–27, 1975.

[20] Goro Shimura. *Introduction to the arithmetic theory of automorphic functions*, volume 11 of *Publications of the Mathematical Society of Japan*. Princeton University Press, 1994.

[21] Glenn Stevens. *Arithmetic on modular curves*, volume 20 of *Progress in Mathematics*. Birkhäuser Boston Inc., 1982.

[22] Toshikazu Takagi. The cuspidal class number formula for the modular curves $X_0(M)$ with M square-free. *J. Algebra*, 193(1):180–213, 1997.

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

[24] Yifan Yang. Modular units and cuspidal divisor class groups of $X_1(N)$. *J. Algebra*, 322(2):514–553, 2009.

[25] Yifan Yang and Jeng-Daw Yu. Structure of the cuspidal rational torsion subgroup of $J_1(p^n)$. *J. London Math. Soc., to appear*.

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