TAIWANESE JOURNAL OF MATHEMATICS
Vol. 15, No. 3, pp. 1305-1323, June 2011
This paper is available online at http://www.tjm.nsysu.edu.tw/

CUSPIDAL $\mathbb{Q}$-RATIONAL TORSION SUBGROUP OF $J(\Gamma)$ OF LEVEL P

Yao-Han Chen

Abstract. For $p>3$ an odd prime, let Γ be a congruence subgroup between $\Gamma_1(p)$ and $\Gamma_0(p)$. In this article, 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 $\mathbb{Q}$.

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 $\mathbb{Q}(\mu_N)$, where μ_N is the group of Nth roots of unity, 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 article, we are interested in the arithmetic aspects of $X(\Gamma)$ and $J(\Gamma)$. In particular, suppose $X(\Gamma)$ is defined over $\mathbb{Q}$. Then 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.

Let $\mathfrak{C}(\Gamma)$ denote the $\mathbb{Q}$-rational cuspidal 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 [7]. In general, it is believed that the cuspidal rational torsion subgroup should be the whole rational torsion subgroup of $J(\Gamma)$. (For $\Gamma=\Gamma_1(p)$, the conjecture was formally stated in [2, Conjecture 6.2.2]).

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

Received January 3, 2010, accepted January 14, 2010.
Communicated by Winnie Li.
2000 *Mathematics Subject Classification*: Primary 11G16, 11G18; Secondary 11F03, 14G05.
Key words and phrases: Modular units, Modular curves, Jacobians, Siegel functions.

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 [9, 10] 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 [14], 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 [11] computed that $\mathfrak{C}(\Gamma_0(p))$ is cyclic of order $\frac{p-1}{(p-1,12)}$. Moreover, Ogg [12] conjectured and Mazur [8] proved that the full 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 [6] 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 Berkovic on the nontriviality of the Mordell-Weil group of some Eisenstein factors of $J(\Gamma_0(pq))$.

In this article, first we will prove the group of modular units on $X(\Gamma)$ that have divisors defined over $\mathbb{Q}$ is generated by Siegel functions for intermediate subgroups Γ between $\Gamma_1(p)$ and $\Gamma_0(p)$, and then we will give an explicit basis for this group. (The result is too complicated to be stated here. We refer the reader to Theorem 3 for details.) As an application, we determine the orders $h(\Gamma)$ of $\mathfrak{C}(\Gamma)$. (We note that it seems that our proof can be easily derived from the methods and results of Yang [16] at first glance. However and in fact, our proofs are independent on [16] and hard to derived from it directly).

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. *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.)

We remark that many mathematicians, for example, Klimek [3], Kubert and Lang [4], Yu [17], and Yang [16], have studied cuspidal $\mathbb{Q}$-rational torsion subgroups of $J(\Gamma)$. 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 [3], Kubert and Lang [4], Yu [17] 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 [17], Yu showed that for arbitrary level N, all modular units on $X(\Gamma_1(N))$ that have divisors supported on cusps lying over ∞ of $X(\Gamma_0(N))$ are generated by Siegel functions and then he computed the order of $\mathfrak{C}^{\infty}(\Gamma_1(N))$. In [16], 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 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 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 even if N is a prime power or square-free integer. (Please see the remark in the end of Sec. 2.1).

The rest of this article is organized as follows. In Section 2, we will recall some notion and properties about cuspidal $\mathbb{Q}$-rational torsion subgroups of Jacobians of modular curves and Siegel functions. In Section 3, we will prove our main result (Theorem 3). Then Theorem 1 is a consequence of Theorem 3. (The proof will appear after Theorem 3.)

2. 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.

2.1. 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 $\mathbb{Q}(\zeta_N)$, where ζ_N is a primitive Nth root of unity, and let $J(\Gamma)$ be the Jacobian variety of $X(\Gamma)$. We know the cusps

of $X(\Gamma)$ are rational over $\mathbb{Q}(\zeta_N)$. Herein, we suppose $X(\Gamma)$ is defined over $\mathbb{Q}$. The following lemma describes the action of the Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$ on the cusps in the case $N = p$ is a prime.

Lemma 1. *Let p be an odd prime, $n = [\Gamma : \Gamma_1(p)]$, and $k = [\Gamma_0(p) : \Gamma]$. Let a be a generator of $(\mathbb{Z}/p\mathbb{Z})^\times$. Then the cusps on $X(\Gamma)$ can be represented by*

$$a^i/p \qquad \text{and} \qquad 1/a^i,$$

for $i = 0, \ldots, k-1$. Moreover, for $0 \le j < p-1$ and $\sigma_{a^j} \in \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ defined by $\sigma_{a^j} : \zeta_p \mapsto \zeta_p^{a^j}$, we have

$$\sigma_{a^j}(a^i/p) = a^i/p, \qquad \sigma_{a^j}(1/a^i) = 1/a^{\overline{i-j}},$$

where $0 \le \overline{i-j} \le k-1$ such that $\overline{i-j} \equiv \widetilde{i-j} \mod k$ for $0 \le \widetilde{i-j} \le (p-1)/2 - 1$ and $\widetilde{i-j} \equiv \pm(i-j) \mod p-1$.

Proof. The cusps of $X(\Gamma_1(p))$ fall into two categories, one consisting of cusps $c/(dp)$, where $p \nmid c$, lying over ∞ of $X(\Gamma_0(p))$ and the other consisting of cusps c/d, where $p \nmid d$, lying over 0 of $X(\Gamma_0(p))$. Moreover, two cusps $c_1/(d_1p)$ and $c_2/(d_2p)$ with $p \nmid c_i$ are equivalent under $\Gamma_1(p)$ if and only if $c_1 \equiv \pm c_2 \mod p$. Likewise, two cusps c_1/d_1 and c_2/d_2 with $p \nmid d_i$ are equivalent under $\Gamma_1(p)$ if and only if $d_1 \equiv \pm d_2 \mod p$. Thus, there are totally $p-1$ inequivalent cusps of $X(\Gamma_1(p))$, represented by i/p and $1/i$ for $i = 1, \ldots, (p-1)/2$. In addition, a^i goes through the representatives $\{1, \ldots, (p-1)/2\}$ modulo p and ± 1 as i runs through $0, \ldots, (p-1)/2-1$, so we know that inequivalent cusps of $X(\Gamma_1(p))$ can be represented by a^i/p and $1/a^i$ for $i = 0, \ldots, (p-1)/2-1$. Because $\Gamma_0(p)/\Gamma_1(p)$ is cyclic, we can write

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

for some $\gamma = \left(\begin{smallmatrix} a^k & * \\ p & * \end{smallmatrix}\right)$. Thus, the inequivalent cusps of $X(\Gamma)$ can be represented by a^i/p and $1/a^i$ for $i = 0, \ldots, k-1$. For the second part of this lemma, it directly follows from [13, Theorem 1.3.1]. Note that $1/a^{\overline{i-j}}$ and $1/a^{\widetilde{i-j}}$ is equivalent under Γ. ∎

Note that since the cusps a^i/p are lying over ∞ of $X_0(p)$, we call them the ∞-*cusps*. Likewise, the cusps $1/a^i$ are lying over 0 of $X_0(p)$, and they are referred to as the 0-*cusps* of $X_0(p)$.

Let K be a subfield of $\mathbb{Q}(\zeta_p)$. A cusp P is said to be *defined over* K, if $P^\sigma = P$ for all $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_p)/K)$. 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 $k+1$ generated by the divisors*

$$a^0/p, a^1/p, \ldots, a^{k-1}/p \qquad \textit{and} \qquad \sum_{i=0}^{k-1} 1/a^i.$$

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

$$D = \sum_{i=0}^{k-1} m_i(a^i/p) + \sum_{i=0}^{k-1} n_i(1/a^i)$$

for some integers m_i and n_i. Let $\sigma_{a^j} \in \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$, where $j = 0, ..., p-1$. By above lemma,

$$D^{\sigma_{a^j}} = \sum_{i=0}^{k-1} m_i\sigma_{a^j}(a^i/p) + \sum_{i=0}^{k-1} n_i\sigma_{a^j}(1/a^i) = \sum_{i=0}^{k-1} m_i(a^i/p) + \sum_{i=0}^{k-1} n_i(1/a^{\overline{i-j}}),$$

where $\overline{i-j}$ is defined in above lemma. Because D is defined over $\mathbb{Q}$, i.e., $D^{\sigma_{a^j}} = D$ for all $\sigma_{a^j} \in \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$, we know n_i must be the same. Thus, D is generated by $\{a^i/p\}_{i=0}^{k-1}$ and $\sum_{i=0}^{k-1} 1/a^i$. Then, clearly, the $\mathbb{Q}$-rational cuspidal divisor group of $X(\Gamma)$ is a free abelian group of rank $k+1$. ∎

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 [7], 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 introduce the Siegel functions, which will be used to construct an explicit basis for the group of modular units.

Remark. Cusps of $X(\Gamma)$ lying over ∞ of $X(\Gamma_0(N))$ are defined over $\mathbb{Q}$. Thus, the subgroup $\mathfrak{C}^\infty(\Gamma)$, which is generated by the divisor classes of the differences of the cusps of $X(\Gamma)$ lying over ∞ of $X(\Gamma_0(N))$, is a subgroup of $\mathfrak{C}(\Gamma)$. However, $\mathfrak{C}^\infty(\Gamma)$ is not equal to $\mathfrak{C}(\Gamma)$ in general. (This follows from the coming examples and the references [3, 4], and [17].) For instance, consider $p = 41$, let Γ be the group corresponds to $k = 4$ and $n = 5$. We have

$$\mathfrak{C}^\infty(\Gamma) = \left\langle \{[(\frac{6^i}{p}) - (\infty)]\}_{i=0}^{3} \right\rangle$$

and

$$\mathfrak{C}(\Gamma) = \left\langle \{[(\frac{6^i}{p}) - (\infty)]\}_{i=0}^{3}, \sum_{i=0}^{3}[(\frac{1}{6^i}) - (\infty)] \right\rangle$$

but $\mathfrak{C}^\infty(\Gamma) \neq \mathfrak{C}(\Gamma)$ by Theorem 1 and Corollary 9. Consider another example $\Gamma_1(35)$. Cusps of $X_1(35)$ consist of ∞-cusps, 0-cusps, $1/5$-cusps, and $1/7$-cusps, where i-cusps are cusps of $X(\Gamma_1(35))$ lying over i of $X(\Gamma_0(35))$. Then we get $\mathfrak{C}^\infty(\Gamma_1(35))$ is generated by divisor classes $\{[(i/35)-(\infty)]\}_{1\le i\le 35/2:(i,35)=1}$. Moreover, $\mathfrak{C}(\Gamma_1(35))$ is generated by

$$\{[(i/35)-(\infty)]\}_{1\le i\le 35/2:(i,35)=1}, \sum_{1\le i\le 35/2:(i,35)=1}[(1/i)-(\infty)],$$

$$\sum_{1\le i<7:(i,35)=1}[(1/5i)-(\infty)], \sum_{1\le i<5:(i,35)=1}[(1/7i)-(\infty)],$$

and many other classes of $\mathbb{Q}$-rational cuspidal divisor of degree 0. We can see that $\mathfrak{C}(\Gamma_1(35))$ is potentially bigger than $\mathfrak{C}^\infty(\Gamma_1(35))$. Besides, it contains more kinds of divisor classes than the prime case. Moreover, as we mentioned before, it is unknown whether modular units on $X(\Gamma)$ that have divisors defined over $\mathbb{Q}$ are still generated by Siegel functions. Also, there is no information about the order of $\mathfrak{C}(\Gamma)$. Hence, it is not an easy job to study in the case of arbitrary level N even if N is a prime power or square-free integer.

2.2. Siegel functions

In this subsection we will introduce and discuss properties of Siegel functions we will use. (See Section 2 in [16] for details.)

Let

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

be the second Bernoulli polynomial. For a given integer N, as in [16] we consider a class of Siegel functions

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

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. [15, 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 $c > 0$,

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

where

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

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

Proposition 4. [5, Chapter 3], [15, Corollary 3]. *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. *Suppose that one has*

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

and

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

Then 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. [15, 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.

3. Main Results

3.1. Notations

Throughout this section, we let $p > 3$ be a prime and Γ be an intermediate group between $\Gamma_0(p)$ and $\Gamma_1(p)$. Suppose $X(\Gamma)$ is defined over $\mathbb{Q}$. Set $n := [\Gamma : \Gamma_1(p)]$ and $k := [\Gamma_0(p) : \Gamma]$. Let a be an even generator of $(\mathbb{Z}/p\mathbb{Z})^\times$. Note that we have

$$nk = [\Gamma_0(p) : \Gamma_1(p)] = \phi(p)/2 = (p-1)/2$$

and

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

for some

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

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 rational torsion subgroup of $J(\Gamma)$,

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

By Lemma 1, all cusps of $X(\Gamma)$ lying over ∞ of $X_0(p)$ are rational over $\mathbb{Q}$. In our approach, these cusps play an important role. Thus, we also introduce the following notations.

$\mathscr{D}^\infty(\Gamma) =$ the group of cuspidal divisors of degree 0 on $X(\Gamma)$ having divisors supported on cusps lying over ∞ of $X_0(p)$,

$\mathscr{F}^\infty(\Gamma) =$ the group of modular units on Γ that have divisors supported on cusps lying over ∞ of $X_0(p)$,

$\mathfrak{C}^\infty(\Gamma) = \mathscr{D}^\infty(\Gamma)/\mathrm{div}\mathscr{F}^\infty(\Gamma)$,

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

3.2. Reduction to the study of $\mathscr{F}^\infty(\Gamma)$ and $h^\infty(\Gamma)$

The main purpose of this subsection is to show that the problem of determining $\mathscr{F}(\Gamma)$ and $h(\Gamma)$ can be reduced to that of $\mathscr{F}^\infty(\Gamma)$ and $h^\infty(\Gamma)$.

Lemma 6. *Let f be a modular unit in $\mathscr{F}(\Gamma)$. Then f is of the form*

$$\prod_g E_g^{e_g},$$

where $12 | \sum_g e_g$.

Proof. Because $\mathscr{F}(\Gamma) \subseteq \mathscr{F}(\Gamma_1(p))$, it suffices to show the case $\mathscr{F}(\Gamma_1(p))$. Let P_i denote the cusps a^i/p and Q_i the cusps $1/a^i$. Because $f \in \mathscr{F}(\Gamma_1(p))$ has divisor defined over $\mathbb{Q}$, the orders of $\operatorname{div}(f)$ at Q_i, $i = 0, 1, \ldots, (p-1)/2 - 1$, must be the same. That is,

$$\operatorname{div}(f) = \sum_{i=0}^{(p-1)/2-1} c_i(P_i) + c \sum_{i=0}^{(p-1)/2-1} (Q_i)$$

for some integers c_i and c. Now by Lagrange's four square theorem, p is the sum of at most 4 squares, say $p = g_1^2 + \ldots + g_\ell^2$, where $\ell \leq 4$. Set

$$h = (E_{g_1} \ldots E_{g_\ell})^{12/\ell}.$$

By Proposition 4, h is a modular function on $\Gamma_1(p)$ whose poles and zeros are all at P_i and Q_i. Furthermore, the order of h at Q_i are all 1 by Proposition 5. Thus, $\operatorname{div}(f/h^c) = \operatorname{div}(f) - c\operatorname{div}(h)$ has support on P_i. By the works of [17, Theorem 4] or [16, Theorem1], we know f/h^c is of the form $\prod_{g'} E_{g'}^{e_{g'}}$ with $\sum_{g'} e_{g'} = 0$. Thus, $f = (h^c)\dot{(}f/h^c)$ is the form $\prod_g E_g^{e_g}$, where $12 | \sum_g e_g$. ∎

Lemma 7. *Let $p > 3$ be a prime, $n = [\Gamma : \Gamma_1(p)]$, and $k = [\Gamma_0(p) : \Gamma]$. Let a be an even generator of $(\mathbb{Z}/p\mathbb{Z})^\times$. Assume that $n > 1$. Then the function*

$$f_0 = (E_{a^0} E_{a^k} \ldots E_{a^{(n-1)k}})^{12/(6,n)}$$

is a modular unit in $\mathscr{F}(\Gamma)$. Moreover, f_0 is a generator of $\mathscr{F}(\Gamma)/\mathscr{F}^\infty(\Gamma)$.

Proof. First, we use Proposition 4 to show that f_0 is modular on $\Gamma_1(p)$. Because $n > 1$, we have $k < (p-1)/2$ and then $a^{2k} \not\equiv 1 \bmod p$. Thus,

$$\sum_{s=0}^{n-1} a^{2sk} \equiv (a^{2kn} - 1)(a^{2k} - 1)^{-1} \equiv 0 \mod p.$$

Hence, Condition (2) of Proposition 4 is satisfied. Condition (1) is trivial. Then f_0 is modular on $\Gamma_1(p)$. Next, we show f_0 is modular on Γ. As above discussion, we know $\sum_{s=0}^{n-1} 2a^{sk} \equiv 0 \bmod 2$ and $\sum_{s=0}^{n-1} 2a^{2sk} \equiv 0 \bmod 2p$. Then by using the transformation law of Proposition 3, we know

$$f_0(\gamma\tau) = \prod_{s=0}^{n-1} E_{a^{sk}}(\gamma\tau)^{12/(6,n)} = \left(E_{a^{nk}}(\tau) \prod_{s=1}^{n-1} E_{a^{sk}}(\tau) \right)^{12/(6,n)}.$$

Let

$$a^{nk} = -1 + up$$

for some integer u. Because $E_{a^{nk}} = (-1)^{u+1} E_{a^0}$, the above product is equal to

$$\left((-1)^{u+1} \prod_{s=0}^{n-1} E_{a^{sk}}(\tau)\right)^{12/(6,n)} = \left(\prod_{s=0}^{n-1} E_{a^{sk}}(\tau)\right)^{12/(6,n)} = f_0(\tau).$$

Thus, f_0 is modular on Γ. Note that by Proposition 5, f_0 has order $n/(6,n)$ at cusps $1/a^i$ for all $i = 0, \ldots, k-1$.

Now we want to show the second part of this lemma. Let $f \in \mathscr{F}(\Gamma)$. Because f is modular on Γ, by Lemma 6, we know

$$f = \prod_g E_g^{c_g},$$

where $12 | \sum_g c_g$. From $f(\gamma\tau) = f(\tau)$, we must have $c_{a^{ik}g} = c_g$ for all i, g. Hence, we can write

$$\begin{aligned} f &= E_{a^0}^{e_0} E_{a^1}^{e_1} \ldots E_{a^{k-1}}^{e_{k-1}} E_{a^k}^{e_0} E_{a^{1+k}}^{e_1} \ldots E_{a^{2k-1}}^{e_{k-1}} E_{a^{(n-1)k}}^{e_0} E_{a^{1+(n-1)k}}^{e_1} \ldots E_{a^{nk-1}}^{e_{k-1}} \\ &= \prod_{i=0}^{k-1} (E_{a^i} E_{a^{i+k}} \ldots E_{a^{i+(n-1)k}})^{e_i} \end{aligned}$$

for some integers e_i with $12 | (e_0 + \ldots + e_{k-1})n$.

First, we show that $2 | \sum_{i=0}^{k-1} e_i$. Because f is modular on Γ, we have

$$f(\tau) = f(\gamma\tau).$$

From $E_{a^{nk}} = (-1)^{u+1} E_{a^0}$, we know that $f(\gamma\tau)$ is equal to

$$(-1)^{e_0(u+1)} \prod_{i=1}^{k} \prod_{s=0}^{n-1} E_{a^{i+sk}}^{e_i}(\gamma\tau),$$

where we set

$$e_k := e_0.$$

Because a is even, as above discussions, this implies $\sum_{s=0}^{n-1} a^{2(i+sk)} \equiv 0 \mod 2p$, and $\sum_{s=0}^{n-1} a^{i+sk} \equiv 0 \mod 2$ for $i = 1, \ldots, k$. Then, by the transformation law of Proposition 3, the above product equals

$$(-1)^{e_0(u+1)} \left(\prod_{i=1}^{k} \prod_{s=1}^{n-1} E_{a^{i+sk}}^{e_i}(\tau)\right) \prod_{i=1}^{k} E_{a^{i+nk}}^{e_i}(\tau).$$

Because $a^{i+nk} = -a^i + a^i up$, from Proposition 3, we know $E_{a^{i+nk}} = (-1)^{a^i u+1} E_{a^i}$ and then the above product is equal to

$$(-1)^{e_0(u+1)} (-1)^{\sum_{i=1}^{k} e_i(a^i u+1)} \prod_{i=1}^{k} \prod_{s=0}^{n-1} E_{a^{i+sk}}^{e_i}(\tau) = (-1)^{\sum_{i=1}^{k} e_i(a^i u+1)} f(\tau),$$

Thus, $2 \mid \sum_{i=1}^{k} e_i(a^i u + 1)$. Moreover, because $2 \mid a$ implies $2 \mid \sum_{i=1}^{k} e_i a^i u$, we get $2 \mid \sum_{i=1}^{k} e_i = \sum_{i=0}^{k-1} e_i$.

Now we can show f_0 is a generator of $\mathscr{F}(\Gamma)/\mathscr{F}^{\infty}(\Gamma)$. Let P_i denote the cusps a^i/p and Q_i the cusps $1/a^i$. Then

$$\operatorname{div}(f) = \sum_{i=0}^{\frac{p-1}{2}-1} c_i(P_i) + \frac{n}{12}\left(\sum_{i=0}^{k-1} e_i\right) \sum_{i=0}^{\frac{p-1}{2}-1} (Q_i)$$

for some integers c_i. Let $e := \sum_{i=0}^{k-1} e_i$. Then $2 \mid e$ by above discussions. From Lemma 6, we know that

$$\frac{e \cdot \frac{n}{(6,n)}}{2 \cdot \frac{6}{(6,n)}} = \frac{en}{12} \in \mathbb{Z}.$$

If $2 \mid n$, because $(\frac{n}{(6,n)}, \frac{6}{(6,n)}) = 1$, $2 \mid e$, and $2 \nmid \frac{6}{(6,n)}$, we know $\frac{e(6,n)}{12} = \frac{e}{2 \cdot \frac{6}{(6,n)}} \in \mathbb{Z}$. If $2 \nmid n$, because $(\frac{n}{(6,n)}, \frac{6}{(6,n)}) = 1$, we also get $\frac{e(6,n)}{12} = \frac{e}{2 \cdot \frac{6}{(6,n)}} \in \mathbb{Z}$. Thus, the orders of f at Q_i are the same and are a multiple of $\frac{n}{(6,n)}$. Because f_0 has order $\frac{n}{(6,n)}$ at cusps Q_i for all $i = 0, \ldots, k-1$, we get

$$\operatorname{div}(f/f_0^{\frac{e(6,n)}{12}}) = \operatorname{div}(f) - \frac{e(6,n)}{12}\operatorname{div}(f_0) = \sum_{i=0}^{\frac{p-1}{2}-1} c_i'(P_i)$$

for some integers c_i'. Therefor, f_0 is a generator of $\mathscr{F}(\Gamma)/\mathscr{F}^{\infty}(\Gamma)$. ∎

3.3. A basis for $\mathscr{F}^{\infty}(\Gamma)$ and computation of $h^{\infty}(\Gamma)$

In view of Lemma 7, to determine $\mathscr{F}(\Gamma)$ and $h(\Gamma)$, it suffices to determine $\mathscr{F}^{\infty}(\Gamma)$ and $h^{\infty}(\Gamma)$. This will be achieved in this subsection.

We first describe a construction of modular functions belonging to $\mathscr{F}^{\infty}(\Gamma)$ for $\Gamma \neq \Gamma_1(p), \Gamma_0(p)$.

Lemma 8. *Let $p > 3$ be an odd prime, $n := [\Gamma : \Gamma_1(p)]$, and $k := [\Gamma_0(p) : \Gamma]$. Let a be an even generator of $(\mathbb{Z}/p\mathbb{Z})^{\times}$. Suppose $\Gamma \neq \Gamma_1(p), \Gamma_0(p)$. Then*

$$\frac{E_{a^i} E_{a^{i+k}} \ldots E_{a^{i+(n-1)k}}}{E_{a^{k-1}} E_{a^{k-1+k}} \ldots E_{a^{k-1+(n-1)k}}}$$

is a modular function in $\mathscr{F}^{\infty}(\Gamma)$ for all $i = 0, 1, \ldots, k-2$.

Proof. Given $0 < i < k-1$, by Proposition 5, we know $f_i := \prod_{s=0}^{n-1}(E_{a^{i+sk}}/E_{a^{k-1+sk}})$ has zeros and poles only at cusps of $X(\Gamma)$ lying over ∞ of $X(\Gamma_0(N))$.

It remains to show it is modular on Γ and then it is in $\mathscr{F}^{\infty}(\Gamma)$. First, we use Proposition 4 to show that it is modular on $\Gamma_1(p)$. Because $\Gamma \neq \Gamma_1(p)$, i.e. $n \neq 1$, we have $k < (p-1)/2$ and then $a^{2k} \not\equiv 1 \bmod p$. Thus,

$$a^{2i} + a^{2(i+k)} + \ldots + a^{2(i+(n-1)k)} \equiv a^{2i}(a^{2kn}-1)(a^{2k}-1)^{-1} \equiv 0 \mod p.$$

Also, $a^{2(k-1)} + a^{2(2k-1)} + \ldots + a^{2(nk-1)} \equiv 0 \bmod p$. Hence, Condition (2) of Proposition 4 is satisfied. Condition (1) is trivial. Then f_i is modular on $\Gamma_1(p)$.

Next, we want to show $f_i(\gamma\tau) = f_i(\tau)$. Because $2|a$, we see that

$$\sum_{s=0}^{n-1}(a^{i+sk} - a^{k-1+sk}) \equiv 0 \mod 2$$

and

$$\sum_{s=0}^{n-1}(a^{2(i+sk)} - a^{2(k-1+sk)}) \equiv 0 \mod 2p.$$

Then by the transformation law in Proposition 3, we know

$$f_i(\gamma\tau) = \prod_{s=0}^{n-1} \frac{E_{a^{i+sk+k}}}{E_{a^{k-1+sk+k}}}(\tau) = \frac{E_{a^{i+nk}}}{E_{a^{k-1+nk}}}(\tau) \prod_{s=1}^{n-1} \frac{E_{a^{i+sk}}}{E_{a^{k-1+sk}}}(\tau).$$

Let $a^{nk} = -1 + up$ for some integer u. Then $a^{j+nk} = -a^j + ua^j p$ for $j = 1, \ldots, k-1$. From Proposition 3, we know $E_{a^{j+nk}} = (-1)^{ua^j+1} E_{a^j}$. Thus,

$$\frac{E_{a^{i+nk}}}{E_{a^{k-1+nk}}} = (-1)^{u(a^i - a^{k-1})} \frac{E_{a^i}}{E_{a^{k-1}}}.$$

Because $2|(a^i - a^{k-1})$, this equals

$$\frac{E_{a^i}}{E_{a^{k-1}}}.$$

Then $f_i(\gamma\tau) = f(\tau)$. Therefore, f_i is in $\mathscr{F}^{\infty}(\Gamma)$.

For $i = 0$, we know $\prod_{s=0}^{n-1}(E_{a^{sk}}/E_{a^{k-1+sk}}) = (-1)^{u+1} \prod_{s=0}^{n-1}(E_{a^{k+sk}}/E_{a^{k-1+sk}})$ because $E_{a^{nk}} = (-1)^{u+1} E_{a^0}$. Then it is in $\mathscr{F}^{\infty}(\Gamma)$ by a similar discussion as above. ∎

Now we can give a basis for $\mathscr{F}^{\infty}(\Gamma)$ for $\Gamma \neq \Gamma_1(p), \Gamma_0(p)$. We remark that a basis for $\mathscr{F}^{\infty}(\Gamma_1(p))$ modulo $\mathbb{C}^{\times}$ is given by Yang in [16]. (Note that at first glance, it seems that it would be easy to get following theorem from [16]. However and actually, it is hard to get the results from [16] directly.)

Theorem 2. *Let $p > 3$ be an odd prime, $n := [\Gamma : \Gamma_1(p)]$, and $k := [\Gamma_0(p) : \Gamma]$. Let a be an even generator of $(\mathbb{Z}/p\mathbb{Z})^\times$. Suppose $\Gamma \neq \Gamma_1(p), \Gamma_0(p)$. Then*

$$\left\{ \frac{E_{a^i} E_{a^{i+k}} \dots E_{a^{i+(n-1)k}}}{E_{a^{k-1}} E_{a^{k-1+k}} \dots E_{a^{k-1+(n-1)k}}} \right\}_{i=0,\dots,k-2}$$

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

Proof. Let $f \in \mathscr{F}^\infty(\Gamma)$. Then $f \in \mathscr{F}^\infty(\Gamma_1(p))$. By the works of [17, Theorem 4] or [16, Theorem 1], we can write $f = \prod_g E_g^{e_g}$, where $\sum_g e_g = 0$. Because $f(\gamma\tau) = f(\tau)$, we must have $e_{a^{ik}g} = e_g$ for all i, g. Hence,

$$\begin{aligned} f &= E_{a^0}^{c_0} E_{a^1}^{c_1} \dots E_{a^{k-1}}^{c_{k-1}} E_{a^k}^{c_0} E_{a^{1+k}}^{c_1} \dots E_{a^{2k-1}}^{c_{k-1}} E_{a^{(n-1)k}}^{c_0} E_{a^{1+(n-1)k}}^{c_1} \dots E_{a^{nk-1}}^{c_{k-1}} \\ &= \prod_{i=0}^{k-2} \left(\frac{E_{a^i} E_{a^{i+k}} \dots E_{a^{i+(n-1)k}}}{E_{a^{k-1}} E_{a^{k-1+k}} \dots E_{a^{k-1+(n-1)k}}} \right)^{c_i} \end{aligned}$$

for some c_i with $\sum_{i=0}^{k-1} c_i = 0$. Thus, by above lemma, these functions form a basis for $\mathscr{F}^\infty(\Gamma)$ modulo $\mathbb{C}^\times$. ∎

Using the result above and a simple argument in linear algebra, we can easily compute the order $h^\infty(\Gamma) = |\mathfrak{C}^\infty(\Gamma)| = |\mathscr{D}^\infty(\Gamma)/\mathrm{div}\mathscr{F}^\infty(\Gamma)|$. Note that

$$h^\infty(\Gamma_1(p)) = p \prod_{\chi \neq \chi_0, \text{ even}} \frac{1}{4} B_{2,\chi},$$

where the product is taken over all even non-principal Dirichlet characters modulo p, is given by Klimek [3].

Corollary 9. *Let $p > 3$ be an odd prime and let $k := [\Gamma_0(p) : \Gamma]$.*

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

where the product is taken over all even non-principal Dirichlet characters χ modulo p satisfying $\chi^k = \chi_0$. (As before, when $\Gamma = \Gamma_0(p)$, the product is empty and is understood to equal 1.)

Before proving the corollary, we need the following elementary lemma from linear algebra. (For a proof, see [16, Lemma 6].)

Lemma 10. *Let $\Lambda \subset \mathbb{R}^n$ be the lattice of rank $n-1$ spanned by the vectors of the form $(0, \dots, 1, -1, 0, \dots, 0)$. Let Λ' be a sublattice of Λ of the same rank*

generated by $v_1, \ldots, v_{n-1} \in \Lambda$. *Let* $v_n = (c_1, \ldots, c_n)$ *be any vector such that* $\sum_i c_i \neq 0$, *and* M *be the* $n \times n$ *matrix whose* i*th row is* v_i. *Then we have*

$$(\Lambda : \Lambda') = \left| \left(\sum_{i=1}^{n} c_i \right)^{-1} \det M \right|.$$

Now we can start to prove Corollary 9. *Proof.* [Proof of Corollary 9] For all $i = 0, \ldots, k-1$, set

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

where $B_2(x) = \{x\}^2 - \{x\} + 1/6$. The inequivalent cusps of Γ lying over ∞ of $X_0(p)$ are $\{\frac{a^j}{p}\}_{j=0}^{k-1}$. Then, by Proposition 5, it is easy to see that for $i, j = 0, \ldots, k-1$, the order of $E_{a^i} E_{a^{i+k}} \ldots E_{a^{i+k(n-1)}}$ at $\frac{a^j}{p}$ is c_{i+j}. Thus, from Theorem 2 and Lemma 10, we know

$$\begin{aligned}
&h^{\infty}(\Gamma) \\
&= \left| (\sum_{i=0}^{k-1} c_i)^{-1} \det \begin{pmatrix} c_0 - c_{k-1} & c_1 - c_0 & \cdots & c_{k-2} - c_{k-3} & c_{k-1} - c_{k-2} \\ c_1 - c_{k-1} & c_2 - c_0 & \cdots & c_{k-1} - c_{k-3} & c_0 - c_{k-2} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ c_{k-2} - c_{k-1} & c_{k-1} - c_0 & \cdots & c_{k-4} - c_{k-3} & c_{k-3} - c_{k-2} \\ c_{k-1} & c_0 & \cdots & c_{k-3} & c_{k-2} \end{pmatrix} \right| \\
&= \left| (\sum_{i=0}^{k-1} c_i)^{-1} \det \begin{pmatrix} c_0 & c_1 & \cdots & c_{k-2} & c_{k-1} \\ c_1 & c_2 & \cdots & c_{k-1} & c_0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ c_{k-2} & c_{k-1} & \cdots & c_{k-4} & c_{k-3} \\ c_{k-1} & c_0 & \cdots & c_{k-3} & c_{k-2} \end{pmatrix} \right| \\
&= \left| (\sum_{i=0}^{k-1} c_i)^{-1} \det \begin{pmatrix} c_0 & c_1 & \cdots & c_{k-2} & c_{k-1} \\ c_{k-1} & c_0 & \cdots & c_{k-3} & c_{k-2} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ c_2 & c_3 & \cdots & c_0 & c_1 \\ c_1 & c_2 & \cdots & c_{k-1} & c_0 \end{pmatrix} \right|.
\end{aligned}$$

Let ξ be a primitive kth roots of unity, $\lambda_s = c_0 + c_1 \xi^s + \ldots + c_{k-1} \xi^{s(k-1)}$, and $v_s = (1, \xi^s, \ldots, \xi^{s(k-2)}, \xi^{s(k-1)})^t$ for $s = 0, \ldots, k-1$. It is easy to see that

$$\begin{pmatrix} c_0 & c_1 & \cdots & c_{k-2} & c_{k-1} \\ c_{k-1} & c_0 & \cdots & c_{k-3} & c_{k-2} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ c_2 & c_3 & \cdots & c_0 & c_1 \\ c_1 & c_2 & \cdots & c_{k-1} & c_0 \end{pmatrix} v_s = \lambda_s v_s.$$

Hence,

$$\det\begin{pmatrix} c_0 & c_1 & \cdots & c_{k-2} & c_{k-1} \\ c_{k-1} & c_0 & \cdots & c_{k-3} & c_{k-2} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ c_2 & c_3 & \cdots & c_0 & c_1 \\ c_1 & c_2 & \cdots & c_{k-1} & c_0 \end{pmatrix} = \prod_{s=0}^{k-1} \lambda_s = \prod_{s=0}^{k-1} \left(\sum_{t=0}^{k-1} c_t \xi^{st} \right).$$

Consider $\sum_{t=0}^{k-1} c_t \xi^{st}$ for each fixed s. Recall that $B_2(x)$ is an even and periodic function. Then it is easy to see that

$$\begin{aligned} \sum_{t=0}^{k-1} c_t \xi^{st} &= \frac{p}{2} \sum_{t=0}^{k-1} \sum_{r=0}^{n-1} \xi^{st} B_2\left(\frac{a^{t+rk}}{p}\right) = \frac{p}{2} \sum_{t=0}^{k-1} \sum_{r=0}^{n-1} \chi(a)^t B_2\left(\frac{a^{t+rk}}{p}\right) \\ &= \frac{p}{2} \sum_{t=0}^{kn-1} \chi(a^t) B_2\left(\frac{a^t}{p}\right) = \frac{1}{4} B_{2,\chi}, \end{aligned}$$

where χ is the Dirichlet character determined by $\chi(a) = \xi^s$. Therefore, we get

$$h^{\infty}(\Gamma) = \left| \prod_{s=1}^{k-1} \left(\sum_{t=0}^{k-1} c_t \xi^{st} \right) \right| = \prod_{\chi^k = \chi_0,\, \chi \neq \chi_0,\, \chi \text{ even}} \frac{1}{4} B_{2,\chi}.$$

This completes the proof of the corollary. ∎

3.4. A basis for $\mathscr{F}(\Gamma)$ and computation of $h(\Gamma)$

All notations are as before.

Combining Lemma 7 and Theorem 2, we immediately obtain the main result of this paper.

Theorem 3. *Let $p > 3$ be an odd prime, $n := [\Gamma : \Gamma_1(p)]$, and $k := [\Gamma_0(p) : \Gamma]$. Let a be an even generator of $(\mathbb{Z}/p\mathbb{Z})^{\times}$. Assume that $n > 1$. Then*

$$\left\{ \frac{E_{a^i} E_{a^{i+k}} \ldots E_{a^{i+(n-1)k}}}{E_{a^{k-1}} E_{a^{k-1+k}} \ldots E_{a^{k-1+(n-1)k}}} \right\}_{i=0,\ldots,k-2}$$

and

$$(E_{a^0} E_{a^k} \ldots E_{a^{(n-1)k}})^{12/(6,n)}$$

form a basis for $\mathscr{F}(\Gamma)$ modulo $\mathbb{C}^{\times}$. (For $\Gamma = \Gamma_0(p)$, it is understood that there are no functions of first form.)

Remark. When $n=(p-1)/2$ and $k=1$, i.e. $\Gamma=\Gamma_0(p)$,

$$(E_{a^0}E_{a^1}\dots E_{a^{((p-1)/2-1)}})^{12/(6,(p-1)/2)}=(\eta(\tau)/\eta(p\tau))^{24/(12,p-1)}$$

generates $\mathscr{F}(\Gamma_0(p))$ modulo $\mathbb{C}^\times$ and then it is easy to see $\mathfrak{C}(\Gamma_0(p))$ is cyclic of order $\frac{p-1}{(p-1,12)}$. Thus, our results recover Ogg's results in [11]. Also observe that for $n=1$ and $k=(p-1)/2$, i.e. $\Gamma=\Gamma_1(p)$, from the proof of Lemma 6, we can get a basis for $\mathscr{F}(\Gamma_1(p))$ modulo $\mathbb{C}^\times$ by joining the function $(E_{g_1}\dots E_{g_\ell})^{12/\ell}$ to the basis for $\mathscr{F}^\infty(\Gamma_1(p))$ modulo $\mathbb{C}^\times$ given in [16, Theorem 1].)

Finally, we want to compute $h(\Gamma)=|\mathfrak{C}(\Gamma)|$. Note that $h(\Gamma_0(p))=\frac{p-1}{(p-1,12)}$ is computed by Ogg [11]. (We also recover this result by above remark.)

Proof of Theorem 1. Let P_i denote the cusps a^i/p and Q_i the cusps $1/a^i$. Let D be a cuspidal divisor defined over $\mathbb{Q}$. Because D is defined over $\mathbb{Q}$, the orders of D at Q_i, $i=0,1,\dots,k-1$, must be the same. That is,

$$D=\sum_{i=0}^{k-1}c_i(P_i)+c\sum_{i=0}^{k-1}(Q_i)$$

for some integers c_i and c.

If $\Gamma=\Gamma_1(p)$, we consider the modular function $(E_{g_1}\dots E_{g_\ell})^{12/\ell}$ on $\Gamma_1(p)$ appeared in the proof of Lemma 6. It has orders 1 at Q_i for all i. Then, it is easy to see that for each cuspidal divisor D defined over $\mathbb{Q}$, there exists a cuspidal divisor D' with support on the ∞-cusps (i.e. $P_i=a^i/p$), such that $D-D'$ is principal. Thus, we know

$$h(\Gamma_1(p))=h^\infty(\Gamma_1(p))=p\prod_{\chi\neq\chi_0\text{ even}}\frac{1}{4}B_{2,\chi}.$$

For the cases $\Gamma\neq\Gamma_1(p),\Gamma_0(p)$, we consider $(E_{a^0}E_{a^k}\dots E_{a^{(n-1)k}})^{\frac{12}{(6,n)}}$. It is a modular unit in $\mathscr{F}(\Gamma)$. Also it has order $\frac{n}{(6,n)}$ at cusps Q_i for all $i=0,\dots,k-1$. Then, by the same token, we know that for each cuspidal divisor D defined over $\mathbb{Q}$ whose orders at Q_i are a multiple of $\frac{n}{(6,n)}$, there exists a cuspidal divisor D' with support on the ∞-cusps (i.e. P_i), such that $D-D'$ is principal. Moreover, for each $f\in\mathscr{F}(\Gamma)$, as in the proof of Lemma 7, we know that its orders at Q_i must be a multiple of $\frac{n}{(6,n)}$. Hence, we get that

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

This completes the proof of Theorem 1. ∎

3.5. Numerical Results

In this subsection, we give a table of numerical results, which describes the order $h(\Gamma)$ and the group structure of $\mathfrak{C}(\Gamma)$, where Γ is an intermediate subgroup

Table 1. The order $h(\Gamma)$ and the group structure of $\mathfrak{C}(\Gamma)$

p	k	n	$h(\Gamma)$	structure
11	1	5	5	cyclic
11	5	1	5	cyclic
13	1	6	1	cyclic
13	2	3	1	cyclic
13	3	2	1	cyclic
13	6	1	19	cyclic
17	1	8	2^2	cyclic
17	2	4	2^2	$[2, 2]$
17	4	2	2^2	cyclic
17	8	1	$2^3 \cdot 73$	cyclic
19	1	9	3	cyclic
19	3	3	3	cyclic
19	9	1	$3^2 \cdot 487$	cyclic
23	1	11	11	cyclic
23	11	1	$11 \cdot 37181$	cyclic
29	1	14	7	cyclic
29	2	7	$3 \cdot 7$	cyclic
29	7	2	$2^3 \cdot 7 \cdot 43$	$[2, 2, 602]$
29	14	1	$2^6 \cdot 3 \cdot 7 \cdot 43 \cdot 17837$	$[4, 4, 64427244]$
31	1	15	5	cyclic
31	3	5	$2^2 \cdot 5 \cdot 7$	$[2, 70]$
31	5	3	$5^2 \cdot 11$	$[5, 55]$
31	15	1	$2^2 \cdot 5^2 \cdot 7 \cdot 11 \cdot 2302381$	$[10, 1772833370]$
37	1	18	3	cyclic
37	2	9	$3 \cdot 5$	cyclic
37	3	6	$3 \cdot 7$	cyclic
37	6	3	$3 \cdot 5 \cdot 7 \cdot 37$	cyclic
37	9	2	$3^2 \cdot 7 \cdot 19 \cdot 577$	cyclic
37	18	1	$3^2 \cdot 5 \cdot 7 \cdot 19 \cdot 37 \cdot 73 \cdot 577 \cdot 17209$	cyclic
41	1	20	$2 \cdot 5$	cyclic
41	2	10	$2^3 \cdot 5$	cyclic
41	4	5	$2^4 \cdot 5 \cdot 13$	cyclic
41	5	4	$2 \cdot 5 \cdot 431$	cyclic
41	10	2	$2^3 \cdot 5 \cdot 31^2 \cdot 431$	cyclic
41	20	1	$2^4 \cdot 5 \cdot 13 \cdot 31^2 \cdot 431 \cdot 250183721$	cyclic
43	1	21	7	cyclic
43	3	7	$2^2 \cdot 7 \cdot 19$	$[2, 266]$
43	7	3	$7 \cdot 29 \cdot 463$	cyclic
43	21	1	$2^2 \cdot 7 \cdot 19 \cdot 29 \cdot 463 \cdot 1051 \cdot 416532733$	$[2, 1563552532984879906]$
47	1	23	23	cyclic
47	23	1	$23 \cdot 139 \cdot 82397087 \cdot 12451196833$	cyclic

between $\Gamma_1(p)$ and $\Gamma_0(p)$ for a prime $p \leq 50$. (Note that for $p = 5, 7$, the Jacobian is trivial.) As before, we let $n := [\Gamma : \Gamma_1(p)]$, and $k := [\Gamma_0(p) : \Gamma]$. Note that the cases $k = 1$ or $n = 1$ are covered by Ogg [16] and Yang [16], respectively. Herein, the notation $[d_1, \ldots, d_m]$ means that the group structure is $(\mathbb{Z}/d_1\mathbb{Z}) \times \ldots \times (\mathbb{Z}/d_m\mathbb{Z})$.

We give a example to explain our ideas about numerical computation.

Example. For $p = 41$, let Γ be the group corresponds to $k = 4$ and $n = 5$. We consider the $k \times k$ matrix

$$H = \begin{pmatrix} -6 & 7 & -2 & 0 \\ 1 & 5 & -1 & 0 \\ -1 & 6 & -7 & 0 \\ -59 & 25 & 1 & 5 \end{pmatrix}.$$

For $i = 0, \ldots, k-2$, the $i+1$th row of H represents the order of $\prod_{s=0}^{n-1}(E_{a^{i+sk}}/E_{a^{k-1+sk}})$ at the ∞-cusps a^j/p, $j = 0, \ldots, k-1$ and the 0-cusp 1. The kth row represents the orders of $(E_{a^0} \ldots E_{a^{(n-1)k}})^{12/(6,n)}$ at the ∞-cusps a^j/p, $j = 1, \ldots, k-1$, and the 0-cusp 1. Note that we only consider one 0-cusp because a $\mathbb{Q}$-rational cuspidal divisor has the same order at 0-cusps.Thus, H represents a basis of $\mathrm{div}_{\mathscr{F}}(\Gamma)$. Then the Smith normal form of H, which is

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1040 \end{pmatrix},$$

gives us the structure of $\mathfrak{C}(\Gamma)$.

Acknowledgments

The author would like to thank Professor Yifan Yang of the National Chiao Tung University for his advices. This work was done while the author was a visiting student at the Penn State University. The author would like to thank Professor Wen-Ching Li and the Penn State University for their warm hospitality. The visit was supported by the National Science Council of Taiwan.

References

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)** (1997), 2255-2263.
2. Conrad Brian, Edixhoven Bas and Stein William, $J_1(p)$ has connected fibers, *Doc. Math.*, **8** (2003), 331-408 (electronic).

3. S. Klimek, PhD thesis, University of California at Berkeley, 1975.
4. Daniel S. Kubert and Serge Lang, The index of Stickelberger ideals of order 2 and cuspidal class numbers, *Math. Ann.*, **237(3)** (1978), 213-232.
5. Daniel S. Kubert and Serge Lang, *Modular units*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Science], **244** Springer-Verlag, 1981.
6. San Ling, On the **Q**-rational cuspidal subgroup and the component group of $J_0(p^r)$, *Israel J. Math.*, **99** (1997), 29-54.
7. Ju. I. Manin, Parabolic points and zeta functions of modular curves, *Izv. Akad. Nauk SSSR Ser. Mat.*, **36** (1972), 19-66.
8. B. Mazur, Modular curves and the Eisenstein ideal, *Inst. Hautes Études Sci. Publ. Math.*, **47** (1977, 1978), 33-186.
9. Morris Newman, Construction and application of a class of modular functions, *Proc. London. Math. Soc.* (3), Proceedings of the London Mathematical Society. Third Series, **7** (1957), 334-350.
10. Newman, Morris, Construction and application of a class of modular functions. II, *Proc. London Math. Soc.* (3), Proceedings of the London Mathematical Society. Third Series, **9** (1959), 373-387.
11. A. P. Ogg, *Rational points on certain elliptic modular curves*, Analytic number theory (Proc. Sympos. Pure Math., Vol. XXIV, St. Louis Univ., St. Louis, Mo., 1972), Amer. Math. Soc., 1973, pp. 221-231.
12. A. P. Ogg, Diophantine equations and modular forms, *Bull. Amer. Math. Soc.*, **81** (1975), 14-27.
13. Daniel S. Kubert and Serge Lang, Units in the modular function field. V. Iwasawa theory in the modular tower, *Math. Ann.*, **237(2)** (1978), 97-104.
14. Toshikazu Takagi, The cuspidal class number formula for the modular curves $X_0(M)$ with M square-free, *J. Algebra*, **193(1)** (1997), 180-213.
15. Yifan Yang, Transformation formulas for generalized Dedekind eta functions, *Bull. London Math. Soc.*, **36(5)** (2004), 671-682.
16. Yifan Yang, Modular units and cuspidal divisor class groups of $X_1(N)$, *J. Algebra*, **322(2)** (2009), 514-553.
17. Jing Yu, A cuspidal class number formula for the modular curves $X_1(N)$, *Math. Ann.*, **252(3)** (1980), 197-216.

Yao-Han Chen
Department of Applied Mathematics
National Chiao Tung University
Hsinchu 300, Taiwan
E-mail: peace.am92g@nctu.edu.tw