Rational Torsion on the Generalized Jacobian of a Modular Curve With Cuspidal Modulus

Takao Yamazaki[1] and Yifan Yang[2]

Received: June 22, 2016
Revised: August 16, 2016

Communicated by Don Blasius

Abstract. We consider the generalized Jacobian $\widetilde{J}_0(N)$ of a modular curve $X_0(N)$ with respect to a reduced divisor given by the sum of all cusps on it. When N is a power of a prime ≥ 5, we exhibit that the group of rational torsion points $\widetilde{J}_0(N)(\mathbb{Q})_{\mathrm{Tor}}$ tends to be much smaller than the classical Jacobian.

2010 Mathematics Subject Classification: Primary 14H40; Secondary 11G16, 11F03, 14G35.
Keywords and Phrases: Generalized Jacobian, torsion points, modular units, cuspidal divisor class.

1 Introduction

1.1

Let N be a natural number and let $X_0(N)$ be the modular curve with respect to $\Gamma_0(N) = \{(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}) \in SL_2(\mathbb{Z}) \mid c \equiv 0 \bmod N\}$, which we regard as a smooth projective curve over $\mathbb{Q}$. Its Jacobian variety $J_0(N)$ is an important object in arithmetic geometry and is intensively studied by many authors. By the Mordell-Weil theorem, the group $J_0(N)(\mathbb{Q})$ of $\mathbb{Q}$-rational points on $J_0(N)$ is finitely generated, and hence its torsion subgroup $J_0(N)(\mathbb{Q})_{\mathrm{Tor}}$ is finite. The torsion subgroup contains an important subgroup $\mathscr{C}(N)$ generated by classes of $\mathbb{Q}$-rational divisors of degree 0 with support on cusps of $X_0(N)$, called the $\mathbb{Q}$-*rational cuspidal divisor class group*. (By Manin's theorem [4], divisors with support on cusps are of finite order in $J_0(N)$.) Ogg [6] conjectured and later Mazur [5] proved that when $N = p$ is a prime, the two groups $\mathscr{C}(p)$

[1]Supported by JSPS KAKENHI Grant (15K04773).
[2]Supported by Grant 102-2115-M-009-001-MY4 of the Ministry of Science and Technology, Taiwan (R.O.C.).

and $J_0(p)(\mathbb{Q})_{\mathrm{Tor}}$ coincide and are cyclic of order $(p-1)/(p-1,12)$. For general cases, it is still an open problem whether the two groups are equal, although the works of Lorenzini [3] and Ling [2] have given a partially affirmative answer to the problem. We summarize the results mentioned above in the theorem below. Here for $m \in \mathbb{Z}_{>0}$, we say two abelian groups are isomorphic *up to m-torsion* if they become isomorphic after tensoring with $\mathbb{Z}[1/m]$.

THEOREM 1.1.1 *Let p be a prime number and set $a := (p-1)/(p-1,12)$, $b := (p+1)/(p+1,12)$. Let n be a positive integer.*

1. *If $N = p$, then $J_0(p)(\mathbb{Q})_{\mathrm{Tor}} = \mathscr{C}(p)$ and is a cyclic group of order a. (Mazur [5, Theorem 1].)*
2. *Suppose $p \not\equiv 11 \bmod 12$. If $p \geq 5$ and $N = p^n$, then the three groups $J_0(p^n)(\mathbb{Q})_{\mathrm{Tor}}$, $\mathscr{C}(p^n)$, and $(\mathbb{Z}/a\mathbb{Z})^n \times (\mathbb{Z}/b\mathbb{Z})^{n-1}$ are isomorphic up to $2p$-torsion. (Lorenzini [3, Theorem 4.6].)*
3. *The previous statement (2) holds without the assumption $p \not\equiv 11 \bmod 12$ but up to $6p$-torsion (Ling [2, Theorem 4]).*
4. *Assume that $p \geq 5$. If n is even, then*

$$\mathscr{C}(p^n) \simeq (\mathbb{Z}/a\mathbb{Z})^n \times (\mathbb{Z}/b\mathbb{Z})^{n-1} \times \prod_{i=n/2}^{n-2} \mathbb{Z}/p^i\mathbb{Z} \times \prod_{i=(n/2)+1}^{n-1} \mathbb{Z}/p^i\mathbb{Z}.$$

   If n is odd, then

$$\mathscr{C}(p^n) \simeq (\mathbb{Z}/a\mathbb{Z})^n \times (\mathbb{Z}/b\mathbb{Z})^{n-1} \times \prod_{i=(n+1)/2}^{n-2} \mathbb{Z}/p^i\mathbb{Z} \times \prod_{i=(n+1)/2}^{n-1} \mathbb{Z}/p^i\mathbb{Z}.$$

   In particular, the order of $\mathscr{C}(p^n)$ is $a^n b^{n-1} p^{k_n}$, where

$$k_n = \begin{cases} (n-2)(3n-2)/4, & \text{if } n \text{ is even,} \\ (n-1)(3n-5)/4, & \text{if } n \text{ is odd.} \end{cases}$$

   (Ling [2, Theorem 1].)

REMARK 1.1.2 *Recently, Ohta [7] proved that $\mathscr{C}(N)$ and $J_0(N)(\mathbb{Q})_{\mathrm{Tor}}$ are isomorphic up to 2-torsion when N is the product of distinct primes different from 3.*

Let $C_0(N)$ be the closed subset of $X_0(N)$ consisting of all cusps. We regard $C_0(N)$ as an effective reduced divisor on $X_0(N)$. In this paper, we consider the *generalized Jacobian* $\widetilde{J}_0(N)$ of $X_0(N)$ with modulus $C_0(N)$ in the sense of Rosenlicht-Serre [8]. It should be as important as $J_0(N)$ in arithmetic geometry of modular curves, but somehow $\widetilde{J}_0(N)$ has not been studied much. We are interested in the group of $\mathbb{Q}$-rational points $\widetilde{J}_0(N)(\mathbb{Q})$ on $\widetilde{J}_0(N)$. Although it is not finitely generated (unless

$N = 1$), its torsion subgroup $\widetilde{J}_0(N)(\mathbb{Q})_{\mathrm{Tor}}$ is finite. In this paper we observe that $\widetilde{J}_0(N)(\mathbb{Q})_{\mathrm{Tor}}$ is unexpectedly smaller than $J_0(N)(\mathbb{Q})_{\mathrm{Tor}}$ by proving the following result, which shows a sharp contrast with Theorem 1.1.1. (For example, Mazur's theorem shows that the cardinality of $J_0(p)(\mathbb{Q})_{\mathrm{Tor}}$ grows linearly as p increases, but on the contrary, our result shows that the cardinality of $\widetilde{J}_0(p)(\mathbb{Q})_{\mathrm{Tor}}$ remains the same for all p.)

THEOREM 1.1.3 *Let p be a prime number and n be a positive integer.*

1. *If $N = p$, then $\widetilde{J}_0(p)(\mathbb{Q})_{\mathrm{Tor}}$ is a cyclic group of order 2.*
2. *Suppose $p \not\equiv 11 \bmod 12$. If $p \geq 5$ and $N = p^n$, then $\widetilde{J}_0(p^n)(\mathbb{Q})_{\mathrm{Tor}}$ is isomorphic to the trivial group up to $2p$-torsion.*
3. *The previous statement (2) holds without the assumption $p \not\equiv 11 \bmod 12$ but up to $6p$-torsion.*
4. *Assume that $p \geq 5$. Suppose that the conjecture $J_0(p^n)(\mathbb{Q})_{\mathrm{Tor}} = \mathscr{C}(p^n)$ is true. If n is even, then*

$$\widetilde{J}_0(p^n)(\mathbb{Q})_{\mathrm{Tor}} \simeq \prod_{i=0}^{(n/2)-1} \mathbb{Z}/(2p^i\mathbb{Z}) \times \prod_{i=1}^{n/2} \mathbb{Z}/(2p^i\mathbb{Z}).$$

If n is odd, then

$$\widetilde{J}_0(p^n)(\mathbb{Q})_{\mathrm{Tor}} \simeq \prod_{i=0}^{(n-1)/2} \mathbb{Z}/(2p^i\mathbb{Z}) \times \prod_{i=1}^{(n-1)/2} \mathbb{Z}/(2p^i\mathbb{Z}).$$

This result is actually a consequence of our main theorem (Theorem 1.3.1) below. However, before we state our main result, let us pause here to recall some basic facts about generalized Jacobian (cf. [8]).

1.2

Let C be a smooth projective geometrically connected curve over a field k, and J the Jacobian variety of C. We give ourselves distinct closed points $P_0, \ldots, P_n \in C$. We assume that P_n is a k-rational point. We consider the generalized Jacobian $\widetilde{J}$ of C with modulus $D = P_0 + \cdots + P_n$. There is an exact sequence

$$0 \to \mathbb{G}_m \to \bigoplus_{i=0}^{n} \mathrm{Res}_{k(P_i)/k}\mathbb{G}_m \to \widetilde{J} \to J \to 0$$

of commutative algebraic groups over k. Here $\mathrm{Res}_{k(P_i)/k}$ denotes the Weil restriction. We have $\mathrm{Res}_{k(P_n)/k}\mathbb{G}_m = \mathbb{G}_m$ since P_n is a k-rational point. As we have

$H^1(k, \mathrm{Res}_{k(P_i)/k}\mathbb{G}_m) = 0$ (by Hilbert 90 and Shapiro's lemma), it induces exact sequences of abelian groups

$$0 \to \bigoplus_{i=0}^{n-1} k(P_i)^\times \xrightarrow{\iota} \widetilde{J}(k) \to J(k) \to 0 \tag{1}$$

and

$$0 \to \bigoplus_{i=0}^{n-1} \mu(k(P_i)) \to \widetilde{J}(k)_{\mathrm{Tor}} \xrightarrow{\rho} J(k)_{\mathrm{Tor}} \xrightarrow{\delta} \bigoplus_{i=0}^{n-1} k(P_i)^\times \otimes \mathbb{Q}/\mathbb{Z}, \tag{2}$$

where we denote by $\mu(F)$ the group of all roots of unity in F for a field F.

REMARK 1.2.1 *Consider an effective divisor D' which has the same support as D (that is, $D' = \sum_{i=0}^n a_i P_i$ with $a_i \in \mathbb{Z}_{>0}$). One can consider the generalized Jacobian J' of C with modulus D'. Then there is a canonical surjection $J' \to \widetilde{J}$ whose kernel is unipotent. In particular, when k is of characteristic zero, we have an isomorphism $J'(k)_{\mathrm{Tor}} \to \widetilde{J}(k)_{\mathrm{Tor}}$ and hence there is nothing new in our problem.*

1.3

We return to the setting in §1.1. Let p be a prime number and let n be a positive integer. Then $C_0(p^n)$ consists of $n+1$ points $P_0, \ldots, P_n$, which we will arrange in such a way that the residue field $\mathbb{Q}(P_i)$ of P_i is the cyclotomic field $\mathbb{Q}(\mu_{p^{d(i)}})$ of degree $p^{d(i)}$ with $d(i) := \min(i, n-i)$ for each $i = 0, \ldots, n$. (See §3.1 for more details.) In particular, P_0 and P_n are $\mathbb{Q}$-rational. Then the map δ in (2) for $(k, C, D) = (\mathbb{Q}, X_0(p^n), C_0(p^n))$ reads

$$\delta : J_0(p^n)(\mathbb{Q})_{\mathrm{Tor}} \to \bigoplus_{i=0}^{n-1} \mathbb{Q}(\mu_{p^{d(i)}})^\times \otimes \mathbb{Q}/\mathbb{Z}, \quad d(i) = \min(i, n-i). \tag{3}$$

Thus, Theorem 1.1.3 follows from Theorem 1.1.1 and the following theorem, which is the main result of this article.

THEOREM 1.3.1 *Let $p \geq 5$ be a prime number and let n be a positive integer. Then the restriction of the map* (3) *to $\mathscr{C}(p^n)$ is injective.*

The proof of Theorem 1.3.1 will occupy almost all of the rest of this article and will be completed in §6. On the other hand, Theorem 1.3.1 does not admit a naive generalization to other values of level N. Indeed, in the last section §7 we shall observe the following result:

PROPOSITION 1.3.2 *Let p, q be two distinct prime numbers. (Then $C_0(pq)$ consists of four $\mathbb{Q}$-rational points.) If $p \equiv q \equiv 1 \bmod 12$, then the kernel of the restriction to $\mathscr{C}(pq)$ of*

$$\delta : J_0(pq)(\mathbb{Q})_{\mathrm{Tor}} \to (\mathbb{Q}^\times)^3 \otimes \mathbb{Q}/\mathbb{Z}$$

is a cyclic group of order $(p-1)(q-1)/24$.

In view of Ohta's result (see Remark 1.1.2), we find that $\widetilde{J}_0(pq)(\mathbb{Q})_{\mathrm{Tor}}$ is isomorphic to a cyclic group of order $(p-1)(q-1)/3$ up to 2-torsion. This shows another sharp contrast with Theorem 1.1.3. We are not able (but hoping) to find more conceptual reason for such difference.

Notation

Let $\overline{\mathbb{Q}}$ be an algebraic closure of $\mathbb{Q}$ and fix an embedding $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$. For $m \in \mathbb{Z}_{>0}$, we set $\zeta_m := e^{2\pi i/m} \in \overline{\mathbb{Q}}^\times$ and $\mu_m := \{\zeta_m^k \mid k \in \mathbb{Z}\} \subset \overline{\mathbb{Q}}^\times$. For an abelian group A, we write A_{Tor} for the subgroup of torsion elements of A. For a field F, we write $\mu(F) = (F^\times)_{\mathrm{Tor}}$.

2 Torsion rational points on generalized Jacobian

2.1

In this section, we use the notations introduced in §1.2. We always assume P_n is k-rational. We will give an explicit description of the map δ in (2) in Lemma 2.3.1 below. Take $x \in \bigoplus_{i=0}^{n-1} k(P_i)^\times$, $m \in \mathbb{Z}_{>0}$ and $a \in J(k)$ such that $ma = 0$. Then by definition we have $\delta(a) = x \otimes \frac{1}{m}$ if there is a lift $\widetilde{a} \in \widetilde{J}(k)$ of a such that $\iota(x) = m\widetilde{a}$, where ι is the map appearing in (1).

2.2

We recall some basic facts about the relative Picard group and generalized Jacobian (cf. [8, Chapter V]). Denote by K the function field of C. For a closed point P on C, we write K_P for the completion of K at P, O_P for the ring of integers in K_P, $t_P \in O_P$ for a (fixed) uniformizer, $U_P := (1 + t_P O_P)^\times$ for the group of principal units in O_P, and $k(P) := O_P/t_P O_P$ for the residue field at P.
Let $U := C \setminus |D|$ be the open complement of the divisor $D = P_0 + \cdots + P_n$. Let us consider the abelian group

$$\mathrm{Div}(C, D) := \mathrm{Div}(U) \oplus \bigoplus_{i=0}^{n} (K_{P_i}^\times / U_{P_i}).$$

We have a canonical map

$$K^\times \to \mathrm{Div}(C, D), \quad f \mapsto \Big(\mathrm{div}_U(f); (f \bmod U_{P_i})_{i=0}^n)\Big),$$

whose cokernel is by definition the *relative Picard group* $\mathrm{Pic}(C, D)$ of C relative to D. We also have a commutative diagram with exact rows

$$\begin{tikzcd}
0 \arrow[r] & K^\times \arrow[r] \arrow[d, equal] & \mathrm{Div}(C,D) \arrow[r] \arrow[d, "\alpha"] & \mathrm{Pic}(C,D) \arrow[r] \arrow[d, "\overline{\alpha}"] & 0 \\
k^\times \arrow[r, hook] & K^\times \arrow[r] & \mathrm{Div}(C) \arrow[r] & \mathrm{Pic}(C) \arrow[r] & 0,
\end{tikzcd}$$

where α is a canonical surjection given by

$$\Big(E; (f_i \bmod U_{P_i})_{i=0}^n\Big) \mapsto E + \sum_{i=0}^n \mathrm{ord}_{P_i}(f_i) P_i,$$

and $\overline{\alpha}$ is induced by α. Combined with isomorphisms

$$\ker(\alpha) \cong \bigoplus_{i=0}^n (O_{P_i}^\times / U_{P_i}) \cong \bigoplus_{i=0}^n k(P_i)^\times,$$

$$\bigoplus_{i=0}^n k(P_i)^\times/(k^\times) \cong \bigoplus_{i=0}^{n-1} k(P_i)^\times, \quad (c_i)_{i=0}^n \bmod (k^\times) \mapsto (c_i/c_n)_{i=0}^{n-1},$$

where $(k^\times)$ is the image of the diagonal map $k^\times \to \oplus_i k(P_i)^\times$, we obtain an exact sequence

$$0 \to \bigoplus_{i=0}^{n-1} k(P_i)^\times \to \mathrm{Pic}(C, D) \to \mathrm{Pic}(C) \to 0. \tag{4}$$

On the other hand, there are canonical isomorphisms

$$J(k) \cong \ker[\mathrm{Pic}(C) \overset{\deg}{\to} \mathbb{Z}],$$
$$\widetilde{J}(k) \cong \ker[\mathrm{Pic}(C, D) \overset{\overline{\alpha}}{\to} \mathrm{Pic}(C) \overset{\deg}{\to} \mathbb{Z}].$$

Then (1) is deduced from (4) by restriction. We also obtain

$$J(k)_{\mathrm{Tor}} \cong \mathrm{Pic}(C)_{\mathrm{Tor}}, \quad \widetilde{J}(k)_{\mathrm{Tor}} \cong \mathrm{Pic}(C, D)_{\mathrm{Tor}}.$$

2.3

We are now ready to describe explicitly the map δ from (2).

LEMMA 2.3.1 *Let $E = \sum_{i=0}^n a_i P_i \in \mathrm{Div}^0(C)$ be a degree zero divisor supported on D. Suppose that its class $[E]$ in $J(k)$ is killed by $m \in \mathbb{Z}_{>0}$ so that there is $f \in K^\times$ such that* $\mathrm{div}_C(f) = mE$. *Define*

$$\mathcal{E} := \Big((\frac{f}{t_{P_n}^{ma_n}})(P_n) (\frac{t_{P_i}^{ma_i}}{f})(P_i) \Big)_{i=0}^{n-1} \in \bigoplus_{i=0}^{n-1} k(P_i)^\times.$$

Then we have

$$\delta([E]) = \mathcal{E} \otimes \frac{1}{m} \quad \textit{in} \quad \bigoplus_{i=0}^{n-1} k(P_i)^\times \otimes \mathbb{Q}/\mathbb{Z}.$$

(Note that $\mathcal{E} \otimes \frac{1}{m}$ does not depend on the choices of t_{P_i} and f.)

Proof. We use the fact recalled in §2.1. Put $\widetilde{E} := (0; (t_{P_i}^{a_i})_{i=0}^n) \in \mathrm{Div}(C, D)$ so that $\alpha(\widetilde{E}) = E$. It suffices to prove that the class of $m\widetilde{E}$ in $\mathrm{Pic}(C, D)$ is the same as $\iota(\mathcal{E}) \in \widetilde{J}(k) \subset \mathrm{Pic}(C, D)$ (see (1) for the map ι). By definition, $\iota(\mathcal{E})$ is given by the class of $(0; (f^{-1}t_{P_i}^{ma_i})_{i=0}^n)$. Since $\mathrm{div}_C(f) = mE$, we have $\mathrm{div}_U(f) = 0$, and hence the class of $(0; (f^{-1}t_{P_i}^{ma_i})_{i=0}^n)$ agrees with that of $(0; (t_{P_i}^{ma_i})_{i=0}^n) = m\widetilde{E}$ in $\mathrm{Pic}(C, D)$. We are done. □

3 Preliminaries on modular curves

3.1

We return to the setting in §1.1. We take an integer $N > 1$ and consider the modular curve $X_0(N)$. Recall that $C_0(N)$ denotes the set of cusps on $X_0(N)$ so that we have a canonical bijection $C_0(N)(\mathbb{C}) \cong \Gamma_0(N)\backslash\mathbb{P}^1(\mathbb{Q})$. For each divisor $d > 0$ of N, there is a unique $Q_d \in C_0(N)$ such that the set of $\mathbb{C}$-rational points lying over Q_d is given by $\Gamma_0(N)$-orbits of $a/d \in \mathbb{P}^1(\mathbb{Q})$ with $a \in \mathbb{Z}$, $(a, d) = 1$. We call $Q_d \in C_0(N)$ the cusp of *level* d. The residue field of Q_d is $\mathbb{Q}(\zeta_m)$ with $m = (d, N/d)$, hence the degree of Q_d is $\phi(m)$, where ϕ denotes the Euler function. The classes of 0 and $\infty \in \mathbb{P}^1(\mathbb{Q})$ are $\mathbb{Q}$-rational and are of level 1 and N respectively.

We define

$$\begin{aligned} \mathscr{D}(N) &:= \{E \in \mathrm{Div}^0(X_0(N)) \mid |E| \subset C_0(N)\} \\ &= \langle Q_d - \phi((d, N/d))Q_N \mid d|N\rangle, \\ \mathscr{P}(N) &:= \mathscr{D}(N) \cap \mathrm{div}(\mathbb{Q}(X_0(N))^\times), \\ \mathscr{C}(N) &:= \mathscr{D}(N)/\mathscr{P}(N). \end{aligned} \tag{5}$$

As we recalled in the introduction, $\mathscr{C}(N)$ is a subgroup of $J_0(N)(\mathbb{Q})_{\mathrm{Tor}}$, hence finite.

3.2

We will use the Dedekind eta function to construct modular functions needed for our purpose. Here let us recall some well-known properties of the Dedekind eta function $\eta(\tau)$, where as usual τ is a variable on the upper half plane $\mathbb{H}$. We shall make use of the standard identification $X_0(N)(\mathbb{C}) \cong \Gamma_0(N)\backslash(\mathbb{H} \cup \mathbb{P}^1(\mathbb{Q}))$.

Proposition 3.2.1 ([1, Proposition 3.2.1]) *Let N be a positive integer. The product $h = \prod_{\delta|N} \eta(\delta\tau)^{r_\delta}$, $r_\delta \in \mathbb{Z}$, is a modular function on $X_0(N)$ if and only if the following conditions are satisfied:*

1. $\sum_{\delta|N} r_\delta = 0$,
2. $\prod_{\delta|N} \delta^{r_\delta}$ *is the square of a rational number,*
3. $\sum_{\delta|N} r_\delta \delta \equiv 0 \mod 24$*, and*
4. $\sum_{\delta|N} r_\delta (N/\delta) \equiv 0 \mod 24$.

We also remark that, if these conditions are satisfied, then h is defined over $\mathbb{Q}$ (see [1, p. 32, Remarque]).

LEMMA 3.2.2 ([1, PROPOSITION 3.2.8]) *Let N be a positive integer. Let d and δ be positive divisors of N. Then the order of $\eta(\delta\tau)$ at a cusp of level d is $a_N(d,\delta)/24$, where*

$$a_N(d,\delta) := \frac{N}{(d,N/d)}\frac{(d,\delta)^2}{d\delta}.$$

In particular, if $g(\tau) = \prod_{\delta|N}\eta(\delta\tau)^{r_\delta}$ is an eta-product satisfying the conditions in Proposition 3.2.1, then

$$\mathrm{div} g = \frac{1}{24}\sum_{d,\delta|N} r_\delta a_N(d,\delta)Q_d.$$

When $N = p^n$ is a prime power, the orders of $\eta(p^k\tau)$ at cusps can be summarized as follows.

COROLLARY 3.2.3 *Let p^n be a prime power.*

1. *If $m \geq n/2$, then the order of $\eta(p^k\tau)$ at a cusp of level p^m is*

$$\begin{cases} p^k/24, & \text{if } k \leq m, \\ p^{2m-k}/24, & \text{if } k > m. \end{cases}$$

2. *If $m < n/2$, then the order of $\eta(p^k\tau)$ at a cusp of level p^m is*

$$\begin{cases} p^{n-k}/24, & \text{if } m \leq k, \\ p^{n+k-2m}/24, & \text{if } m > k. \end{cases}$$

In order to obtain the Fourier expansion of an eta-product at a cusp, we should need the following transformation formula for the Dedekind eta function.

LEMMA 3.2.4 ([10, PP. 125–127]) *For*

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

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

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

and, for $c > 0$,

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

with

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

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

4 Cuspidal divisor class group

4.1

In §§4–6, we consider the case $N = p^n$, where p is a prime greater than or equal to 5 and n is a positive integer. We describe the group of modular units on $X_0(p^n)$ that gives us $\mathscr{P}(p^n)$ (see (5) for its definition).

PROPOSITION 4.1.1 *Let p^n be a prime power with $p \geq 5$ prime and $n \in \mathbb{Z}_{>0}$. Then the group $\mathscr{P}(p^n)$ is generated by the divisors of*

$$f(\tau) = \left(\frac{\eta(p\tau)}{\eta(\tau)}\right)^{24/(p-1,12)}, \qquad g_k(\tau) = \frac{\eta(p^{k+2}\tau)}{\eta(p^k\tau)}, \quad k = 0, \ldots, n-2.$$

The proof of this proposition will be given in §4.2. We first deduce a corollary that will be used later. For $i = 0, \ldots, n$, we write $P_i := Q_{p^i}$ for the cusp of level p^i (see §3.1).

COROLLARY 4.1.2 *Let p, n be as in Proposition 4.1.1.*

1. *The divisors $\operatorname{div}(f), \operatorname{div}(g_0), \ldots, \operatorname{div}(g_{n-2})$ form a free $\mathbb{Z}$-basis of $\mathscr{P}(p^n)$.*

2. *Let $c_0, \ldots, c_{n-2} \in \mathbb{Z}$ and write*

$$\operatorname{div}(f g_0^{c_0} g_1^{c_1} \ldots g_{n-2}^{c_{n-2}}) = \sum_{i=0}^{n} s_i P_i, \quad s_i \in \mathbb{Z}$$

in $\mathscr{D}(p^n)$. Then we have $(s_0, s_1, \ldots, s_n) = (p-1)/(p-1, 12)$.

Proof. (1) This is an immediate consequence of Proposition 4.1.1, since $\mathscr{P}(p^n)$ is a free $\mathbb{Z}$-module of rank n (as it is a finite index subgroup of $\mathscr{D}(p^n)$.)
(2) Put $a := (p-1)/(p-1, 12)$. By using Corollary 3.2.3 we first see that the order of g_k at any cusp is divisible by a for $k = 0, \ldots, n-2$. Hence, by (1), it suffices to show the statement for $c_0 = \cdots = c_{n-2} = 0$, which again follows from Corollary 3.2.3. □

In the proof of Proposition 4.1.1, we use the following elementary lemma. We omit its proof.

LEMMA 4.1.3 *Let $L_0 \subset \mathbb{R}^{n+1}$ be the lattice of rank n generated by the vectors of the form $(0, \ldots, 1, -1, 0, \ldots, 0)$. Let L_1 be a sublattice of L_0 of the same rank generated by $v_1, \ldots, v_n \in L_1$. Let $v_{n+1} = (c_1, \ldots, c_{n+1})$ be any vector such that $\sum_i c_i \neq 0$, and M be the $(n+1) \times (n+1)$ matrix whose ith row is v_i. Then we have*

$$(L_0 : L_1) = \left| \left(\sum_{i=1}^{n+1} c_i\right)^{-1} \det M \right|.$$

4.2 Proof of Proposition 4.1.1

Let L_0 be the lattice of rank n in $\mathbb{Z}^{n+1} = \bigoplus_{i=0}^n \mathbb{Z}e_i$ generated by vectors of the form $(0, \dots, 1, -1, 0, \dots, 0)$. Recall that $D_i := P_i - \phi((p^i, p^{n-i}))P_n$ $(i = 0, \dots, n-1)$ form a $\mathbb{Z}$-basis of $\mathscr{D}(p^n)$. Consider the natural group homomorphism $\lambda : \mathscr{D}(p^n) \to \mathbb{Z}^{n+1}$ defined by

$$\lambda(D_i) = \phi((p^i, p^{n-i}))e_i - \phi((p^i, p^{n-i}))e_n \qquad (i = 0, \dots, n-1).$$

Let $L_1 = \lambda(\mathscr{D}(p^n))$ be the image of $\mathscr{D}(p^n)$ under λ. It is a sublattice of L_0. Let $\mathscr{D}'$ be the group generated by the divisors of f and g_k and L_2 be the image of $\mathscr{D}'$ under λ. Then to show that the divisors of f and g_k generate $\mathscr{P}(p^n)$, it suffices to show that the index of L_2 in L_1 is equal to the divisor class number given in Part (4) of Theorem 1.1.1. To show that this indeed holds, we form 3 square matrices M, U, and V of dimension $n+1$. The first matrix $M = (M_{ij})_{i,j=0}^n$ is defined by

$$\begin{aligned} M_{ij} &= \text{the order of } \eta(p^i\tau) \text{ at cusps of level } p^j \\ &= \begin{cases} p^i/24, & \text{if } j \ge n/2 \text{ and } i \le j, \\ p^{2j-i}/24, & \text{if } j \ge n/2 \text{ and } i > j, \\ p^{n-i}/24, & \text{if } j < n/2 \text{ and } i \ge j, \\ p^{n+i-2j}/24, & \text{if } j < n/2 \text{ and } i < j. \end{cases} \end{aligned}$$

The second matrix U is a diagonal matrix with the diagonal entries being $\phi((p^i, p^{n-i}))$, $i = 0, \dots, n$. The third matrix V is

$$V = \begin{pmatrix} -c & c & 0 & 0 & \cdots & \cdots & 0 \\ -1 & 0 & 1 & 0 & \cdots & \cdots & 0 \\ 0 & -1 & 0 & 1 & \cdots & \cdots & 0 \\ \vdots & \vdots & & & & \vdots & \vdots \\ 0 & \cdots & \cdots & 0 & -1 & 0 & 1 \\ 1 & \cdots & \cdots & \cdots & 1 & 1 & 1 \end{pmatrix}, \qquad c = \frac{24}{(p-1, 12)}.$$

That is, if we associate to an eta-product $\prod_{i=0}^n \eta(p^i\tau)^{r_i}$ a vector $(r_0, \dots, r_n)$, then the first n rows of V are the vectors corresponding to the functions f and g_k, while the last row of V consists of 1's. Then the first n rows of the matrix VMU are precisely $\lambda(\mathrm{div} f)$ and $\lambda(\mathrm{div} g_k)$, $k = 0, \dots, n-2$. Now we claim that (see Theorem 1.1.1 for the definition of a and b)

1. $\det V = 24(-1)^n(n+1)/(p-1, 12)$,
2. $\det M = \begin{cases} (ab)^n p^{(n-1)(3n-1)/4}/24, & \text{if } n \text{ is odd}, \\ (ab)^n p^{n(3n-4)/4}/24, & \text{if } n \text{ is even}. \end{cases}$
3. $\det U = \prod_{i=0}^n \phi((p^i, p^{n-i}))$, and
4. the sum of the entries in the last row of VMU is $(n+1)p^{n-1}(p+1)/24$.

Assuming that the claims are true for the moment, let us complete the proof of the proposition.
It is clear that

$$(L_0 : L_1) = \prod_{i=0}^{n} \phi((p^i, p^{n-i})) = \det U. \tag{6}$$

By Lemma 4.1.3, we have

$$(L_0 : L_2) = C^{-1} |\det(VMU)|,$$

where C is the sum of the entries in the last row of VMU. By the four claims above,

$$\det(VMU) = (-1)^n \frac{(n+1)}{(p-1,12)} (ab)^n (\det U) \times \begin{cases} p^{(n-1)(3n-1)/4}, & \text{if } n \text{ is odd,} \\ p^{n(3n-4)/4}, & \text{if } n \text{ is even,} \end{cases}$$

and $C = (n+1)p^{n-1}(p+1)/24$. It follows that

$$(L_0 : L_2) = \frac{24(ab)^n \det U}{(p+1)(p-1,12)} \times \begin{cases} p^{(n-1)(3n-5)/4}, & \text{if } n \text{ is odd,} \\ p^{(n-2)(3n-2)/4}, & \text{if } n \text{ is even.} \end{cases}$$

Recall that the number b is defined to be $(p+1)/(p+1,12)$. Also we may check case by case that $(p-1,12)(p+1,12) = 24$. Therefore, the expression above can also be written as

$$(L_0 : L_2) = a^n b^{n-1} (\det U) \times \begin{cases} p^{(n-1)(3n-5)/4}, & \text{if } n \text{ is odd,} \\ p^{(n-2)(3n-2)/4}, & \text{if } n \text{ is even.} \end{cases}$$

Combining this with (6), we find that

$$(L_1 : L_2) = a^n b^{n-1} \times \begin{cases} p^{(n-1)(3n-5)/4}, & \text{if } n \text{ is odd,} \\ p^{(n-2)(3n-2)/4}, & \text{if } n \text{ is even,} \end{cases}$$

which agrees with the class number given in Part (4) of Theorem 1.1.1. Therefore, we conclude that the divisors of f and g_k, $k = 0, \ldots, n-2$ generate $\mathscr{P}(p^n)$. It remains to prove that the four claims are true.
Claims (1) and (3) are obvious. To prove Claim (2), we start by giving examples. Consider the case $n = 5$. The matrix M in this case is

$$\frac{1}{24} \begin{pmatrix} p^5 & p^3 & p & 1 & 1 & 1 \\ p^4 & p^4 & p^2 & p & p & p \\ p^3 & p^3 & p^3 & p^2 & p^2 & p^2 \\ p^2 & p^2 & p^2 & p^3 & p^3 & p^3 \\ p & p & p & p^2 & p^4 & p^4 \\ 1 & 1 & 1 & p & p^3 & p^5 \end{pmatrix}$$

We subtract the second column from the first column, the third column from the second column, the fourth column from the fifth column, and then the fifth column from the last column. The matrix becomes

$$\frac{1}{24}\begin{pmatrix} p^3(p^2-1) & p(p^2-1) & p & 1 & 0 & 0 \\ 0 & p^2(p^2-1) & p^2 & p & 0 & 0 \\ 0 & 0 & p^3 & p^2 & 0 & 0 \\ 0 & 0 & p^2 & p^3 & 0 & 0 \\ 0 & 0 & p & p^2 & p^2(p^2-1) & 0 \\ 0 & 0 & 1 & p & p(p^2-1) & p^3(p^2-1) \end{pmatrix},$$

with the determinant unchanged. Thus,

$$\det M = \frac{1}{24^6}p^{14}(p^2-1)^5 = \frac{1}{24}(ab)^5p^{14}.$$

In general, if n is an odd integer greater than 3, then a similar matrix manipulation (subtracting the second column from the first column, the third column from the second column, etc.) will produce a matrix of the form

$$\frac{1}{24}\begin{pmatrix} A_1 & B_1 & 0 \\ 0 & A_2 & 0 \\ 0 & B_2 & A_3 \end{pmatrix},$$

where A_1 is an upper-triangular matrix of dimension $(n-1)/2$ whose diagonal entries are $p^{n-2}(p^2-1), \dots, p^{(n-1)/2}(p^2-1)$, A_3 is a lower-triangular matrix of the same dimension whose diagonal entries are $p^{(n-1)/2}(p^2-1), \dots, p^{n-2}(p^2-1)$,

$$A_2 = \begin{pmatrix} p^{(n+1)/2} & p^{(n-1)/2} \\ p^{(n-1)/2} & p^{(n+1)/2} \end{pmatrix},$$

and B_i are some immaterial $(n-1)/2$-by-2 matrices. It follows that

$$\begin{aligned} \det M &= \frac{1}{24^{n+1}}p^{2((n-1)/2+(n+1)/2+\cdots+(n-2))}(p^2-1)^{n-1}(p^{n+1}-p^{n-1}) \\ &= \frac{1}{24}(ab)^n p^{(n-1)(3n-1)/4}. \end{aligned}$$

This proves Claim (2) for the case of odd n. The proof of the case of even n is similar. For the case $n = 4$, we have

$$M = \frac{1}{24}\begin{pmatrix} p^4 & p^2 & 1 & 1 & 1 \\ p^3 & p^3 & p & p & p \\ p^2 & p^2 & p^2 & p^2 & p^2 \\ p & p & p & p^3 & p^3 \\ 1 & 1 & 1 & p^2 & p^4 \end{pmatrix}.$$

Subtracting the second column from the first column, the third column from the second column, the fourth column from the last column, and then the third column from the fourth column, we obtain the matrix

$$\frac{1}{24}\begin{pmatrix} p^2(p^2-1) & p^2-1 & 1 & 0 & 0 \\ 0 & p(p^2-1) & p & 0 & 0 \\ 0 & 0 & p^2 & 0 & 0 \\ 0 & 0 & p & p(p^2-1) & 0 \\ 0 & 0 & 1 & p^2-1 & p^2(p-1) \end{pmatrix},$$

whose determinant is

$$\frac{1}{24^5}p^8(p^2-1)^4 = \frac{1}{24}(ab)^4p^8.$$

In general, a similar matrix manipulation yields a matrix of the form

$$\frac{1}{24}\begin{pmatrix} A_1 & B_1 & 0 \\ 0 & p^{n/2} & 0 \\ 0 & B_2 & A_2 \end{pmatrix},$$

where A_1 is an upper-triangular matrix of dimension $n/2$ with the diagonal entries being $p^{n-2}(p^2-1),\dots,p^{n/2-1}(p^2-1)$ and A_2 is a lower-triangular matrix of dimension $n/2$ with the diagonals being $p^{n/2-1}(p^2-1),\dots,p^{n-2}(p^2-1)$. Therefore,

$$\begin{aligned}\det M &= \frac{1}{24^{n+1}}p^{2((n/2-1)+n/2+\cdots+(n-2))+n/2}(p^2-1)^n \\ &= \frac{1}{24}(ab)^n p^{n(3n-4)/4}.\end{aligned}$$

This completes the proof of Claim (2).

To prove Claim (4), we first observe that since the last row of V consists of 1's, the sum of the entries in the last row of VMU is simply the sum of all entries in MU. Now the (i,j)-entry of MU is the order of $\eta(p^{i-1}\tau)$ at a cusp of level p^{j-1} times the number of such cusps. Therefore, the sum of the entries in the ith row of MU is the degree of $\mathrm{div}\eta(p^{i-1}\tau)$, which is equal to

$$\frac{1}{24}(\mathrm{SL}(2,\mathbb{Z}):\Gamma_0(p^n)) = \frac{1}{24}p^{n-1}(p+1).$$

(In general, the degree of the divisor of a modular form of weight k on $\Gamma_0(N)$ is $k(\mathrm{SL}(2,\mathbb{Z}) : \Gamma_0(N))/12$. Here the weight of the Dedekind eta function is $1/2$.) Hence the sum of the entries in the last row of VMU is $(n+1)p^{n-1}(p+1)/24$. This completes the proof of the proposition. □

5 Leading Fourier coefficients of modular units at cusps

5.1

In this section, we work out the leading Fourier coefficients of the modular functions $f(\tau)$ and g_k defined in Proposition 4.1.1 at cusps. To speak of such coefficients, we first need to choose uniformizers at cusps. Then the coefficients are canonically defined as an element of the residue fields of cusps, but we can calculate it after base change to $\mathbb{C}$. As cusps of the same level are Galois conjugates, for our purpose, we only need to calculate the leading coefficient at one of the $\mathbb{C}$-valued points of cusps of each level. In general, to define a local uniformizer at a cusp $\alpha \in \mathbb{P}^1(\mathbb{Q})$ of $X_0(N)$, we choose an element σ in $\mathrm{GL}^+(2, \mathbb{Q})$ such that $\sigma\infty = \alpha$. Let h be the smallest positive number such that

$$\sigma \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix} \sigma^{-1} \in \Gamma_0(N).$$

Then a local uniformizer at α is

$$q_\alpha = e^{2\pi i \sigma^{-1}\tau/h}.$$

5.2

We return to the case $N = p^n$, where p^n is a prime power with $p \geq 5$. For convenience, our choice of a cusp $\alpha_m \in \mathbb{P}(\mathbb{Q})$ of level p^m is

$$\alpha_m = \begin{cases} 1/p^m, & \text{if } m \geq n/2, \\ -1/p^m, & \text{if } m < n/2. \end{cases} \tag{7}$$

Then we can choose σ_m to be

$$\sigma_m = \begin{cases} \left(\begin{smallmatrix} 1 & 0 \\ p^m & 1 \end{smallmatrix}\right), & \text{if } m \geq n/2, \\ \begin{pmatrix} 0 & -1 \\ p^n & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ p^{n-m} & 1 \end{pmatrix} = \begin{pmatrix} -p^{n-m} & -1 \\ p^n & 0 \end{pmatrix}, & \text{if } m < n/2. \end{cases} \tag{8}$$

We summarize our discussion as a lemma:

LEMMA 5.2.1 *With the choice of σ_m given in* (8)*, the local uniformizer at the cusps α_m in* (7) *is*

$$e^{2\pi i \sigma_m^{-1}\tau}$$

for each m.

5.3

In the following lemma, we adopt the following notation

$$f(\tau)\big| \begin{pmatrix} a & b \\ c & d \end{pmatrix} := f\left(\frac{a\tau + b}{c\tau + d}\right),$$

which is slightly different from the usual meaning of the slash operator.

LEMMA 5.3.1 *Let p be an odd prime.*

1. If $k \le m$, then

$$\eta(p^k\tau)\Big| \begin{pmatrix} 1 & 0 \\ p^m & 1 \end{pmatrix} = e^{2\pi i/8} e^{-2\pi i p^{m-k}/24} \sqrt{\frac{p^m\tau+1}{i}}\eta(p^k\tau).$$

2. If $k \ge m$, then

$$\eta(p^k\tau)\Big| \begin{pmatrix} 1 & 0 \\ p^m & 1 \end{pmatrix} = e^{2\pi i p^{k-m}/24} \sqrt{\frac{p^m\tau+1}{p^{k-m}i}}\eta\left(\frac{p^m\tau+1}{p^{k-m}}\right).$$

Proof. If $k \le m$, we have

$$p^k\frac{\tau}{p^m\tau+1} = \begin{pmatrix} 1 & 0 \\ p^{m-k} & 1 \end{pmatrix} p^k\tau.$$

Hence, by Lemma 3.2.4, we find that

$$\begin{aligned}\eta(p^k\tau)\Big| \begin{pmatrix} 1 & 0 \\ p^m & 1 \end{pmatrix} &= \varepsilon(1,0,p^{m-k},1)\sqrt{\frac{p^m\tau+1}{i}}\eta(p^k\tau) \\ &= i^{(1-p^{m-k})/2} e^{2\pi i p^{m-k}/12}\sqrt{\frac{p^m\tau+1}{i}}\eta(p^k\tau),\end{aligned}$$

which yields the first statement of the lemma.
If $k \ge m$, we have

$$p^k\frac{\tau}{p^m\tau+1} = \begin{pmatrix} p^{k-m} & -1 \\ 1 & 0 \end{pmatrix} \frac{p^m\tau+1}{p^{k-m}}.$$

By Lemma 3.2.4 again, we have

$$\begin{aligned}\eta(p^k\tau)\Big| \begin{pmatrix} 1 & 0 \\ p^m & 1 \end{pmatrix} &= \varepsilon(p^{k-m},-1,1,0)\sqrt{\frac{p^m\tau+1}{p^{k-m}i}}\eta\left(\frac{p^m\tau+1}{p^{k-m}}\right) \\ &= e^{2\pi i p^{k-m}/24}\sqrt{\frac{p^m\tau+1}{p^{k-m}i}}\eta\left(\frac{p^m\tau+1}{p^{k-m}}\right).\end{aligned}$$

This proves the lemma. □

REMARK 5.3.2 *From Lemmas 5.2.1 and 5.3.1, we can easily deduce the orders of $\eta(p^k\tau)$ at each cusp, recovering the results in Corollary 3.2.3.*

5.4

We now use Lemma 5.3.1 to obtain the leading coefficients of modular functions at cusps. Here for an odd prime p, we let

$$p^* = e^{2\pi i(p-1)/4}p, \qquad \sqrt{p^*} = e^{2\pi i(p-1)/8}\sqrt{p}. \tag{9}$$

PROPOSITION 5.4.1 *Assume that p^n is a prime power with $p \ge 5$ and $n \ge 1$. Let*

$$f(\tau)=\left(\frac{\eta(p\tau)}{\eta(\tau)}\right)^{24/(p-1,12)}, \qquad g_k(\tau)=\frac{\eta(p^{k+2}\tau)}{\eta(p^k\tau)}, \quad k=0,\dots,n-2,$$

be the modular functions defined in Proposition 4.1.1.

1. *If $m \ge n/2$, then the leading Fourier coefficients of $f(\tau)$ and $g_k(\tau)$ with respect to the local uniformizer at $1/p^m$ chosen using* (8) *are*

$$\begin{cases} 1 & \text{for } f(\tau), \\ 1 & \text{for } g_k(\tau) \text{ with } k \le m-2, \\ (-1)^{(p-1)/2}e^{-2\pi iab/p}/\sqrt{p^*} & \text{for } g_{m-1}(\tau), \\ e^{-2\pi iab/p^{k+2-m}}/p & \text{for } g_k(\tau) \text{ with } k \ge m. \end{cases}$$

2. *If $m < n/2$, then the leading Fourier coefficients of $f(\tau)$ and $g_k(\tau)$ with respect to the local uniformizer at $-1/p^m$ chosen using* (8) *are*

$$\begin{cases} p^{-12/(p-1,12)} & \text{for } f(\tau) \text{ when } m=0, \\ e^{2\pi ia/p^m} & \text{for } f(\tau) \text{ when } m \ge 1, \\ 1/p & \text{for } g_k(\tau) \text{ with } k \ge m, \\ e^{2\pi iab/p}/\sqrt{p^*} & \text{for } g_{m-1}(\tau), \\ e^{2\pi iab/p^{m-k}} & \text{for } g_k(\tau) \text{ with } k \le m-2. \end{cases}$$

Proof. Consider the function $f(\tau)$ first. Since n is assumed to be at least 1, when $m \ge n/2$, we have $m \ge 1$ and the first part of Lemma 5.3.1 applies. We find that

$$\frac{\eta(p\tau)}{\eta(\tau)}\Big|\begin{pmatrix}1&0\\p^m&1\end{pmatrix}=e^{2\pi ip^{m-1}(p-1)/24}\frac{\eta(p\tau)}{\eta(\tau)}.$$

It follows that

$$f(\tau)\Big|\begin{pmatrix}1&0\\p^m&1\end{pmatrix}=f(\tau)$$

and the leading Fourier coefficient is 1. Similarly, if k is less than or equal to $m-2$, then the leading Fourier coefficient of $g_k(\tau)$ at the cusp $1/p^m$ is 1.
If $k=m-1$, then $k<m$ and $k+2=m+1>m$. By Lemma 5.3.1, we have

$$\eta(p^{m+1}\tau)\Big|\begin{pmatrix}1&0\\p^m&1\end{pmatrix}=e^{2\pi ip/24}\sqrt{\frac{p^m\tau+1}{pi}}\,\eta\left(\frac{p^m\tau+1}{p}\right),$$

$$\eta(p^{m-1}\tau)\Big|\begin{pmatrix}1&0\\p^m&1\end{pmatrix}=e^{2\pi i/8}e^{-2\pi ip/24}\sqrt{\frac{p^m\tau+1}{i}}\,\eta(p^{m-1}\tau),$$

and the leading coefficient of $g_{m-1}(\tau)$ at $1/p^m$ is

$$\frac{1}{\sqrt{p}}e^{2\pi i(p/12-1/8+1/24p)} = \frac{1}{\sqrt{p}}e^{2\pi i(p-1)/8}e^{-2\pi i(p^2-1)/24p} = \frac{(-1)^{(p-1)/2}}{\sqrt{p^*}}e^{-2\pi iab/p}.$$

(Here we remind the reader that the leading coefficient of $\eta((c\tau+d)/e)$ is $e^{2\pi id/24e}$.) When $k \geq m$, by Part (2) of Lemma 5.3.1,

$$\frac{\eta(p^{k+2}\tau)}{\eta(p^k\tau)}\Big| \begin{pmatrix} 1 & 0 \\ p^m & 1 \end{pmatrix} = \frac{1}{p}e^{2\pi ip^{k-m}(p^2-1)/24}\frac{\eta((p^m\tau+1)/p^{k+2-m})}{\eta((p^m\tau+1)/p^{k-m})},$$

whose leading Fourier coefficient is

$$\frac{1}{p}e^{2\pi i(1-p^2)/24p^{k+2-m}} = \frac{1}{p}e^{-2\pi iab/p^{k+2-m}}.$$

This completes the proof of the case of $m \geq n/2$.

We next consider the case $\alpha_m = -1/p^m$ with $m < n/2$. Recall that the choice of σ_m is given in (8). Noticing that

$$\eta(p^k\tau)\Big| \begin{pmatrix} 0 & -1 \\ p^n & 0 \end{pmatrix} = \eta(-1/p^{n-k}\tau) = \sqrt{\frac{p^{n-k}\tau}{i}}\eta(p^{n-k}\tau),$$

we have

$$g_k(\tau)\Big|\sigma_m = \frac{\eta(p^{k+2}\tau)}{\eta(p^k\tau)}\Big| \begin{pmatrix} 0 & -1 \\ p^n & 0 \end{pmatrix} \Big|\sigma_{n-m} = \frac{1}{pg_{n-k-2}(\tau)}\Big|\sigma_{n-m}.$$

Thus, using the results in Part (1), we find that the leading coefficients of $g_k(\tau)$ at the cusp $\alpha_m = -1/p^m$ are

$$\begin{cases} 1/p, & \text{if } k \geq m, \\ e^{2\pi iab/p}/\sqrt{p^*}, & \text{if } k = m-1, \\ e^{2\pi iab/p^{m-k}} & \text{if } k \leq m-2. \end{cases}$$

Finally, for the function $f(\tau)$, we have

$$f(\tau)\Big|\sigma_m = \frac{1}{p^{12/(p-1,12)}}\left(\frac{\eta(p^{n-1}\tau)}{\eta(p^n\tau)}\right)^{24/(p-1,12)}\Big|\sigma_{n-m}.$$

When $m \geq 1$, by Part (2) of Lemma 5.3.1,

$$\left(\frac{\eta(p^{n-1}\tau)}{\eta(p^n\tau)}\right)^{24/(p-1,12)}\Big|\sigma_{n-m} = p^{12/(p-1,12)}\left(\frac{\eta((p^{n-m}\tau+1)/p^{m-1})}{\eta((p^{n-m}\tau+1)/p^m)}\right)^{24/(p-1,12)}.$$

Thus, the leading coefficient of $f(\tau)$ at α_m is

$$\left(e^{2\pi i p^{-m}(p-1)/24}\right)^{24/(p-1,12)} = e^{2\pi i a/p^m}.$$

When $m = 0$, by Part (1) of Lemma 5.3.1,

$$\left(\frac{\eta(p^{n-1}\tau)}{\eta(p^n\tau)}\right)^{24/(p-1,12)}\Big|\sigma_n = \left(e^{2\pi i(1-p)/24}\frac{\eta(p^{n-1}\tau)}{\eta(p^n\tau)}\right)^{24/(p-1,12)}.$$

Thus, the leading coefficient of $f(\tau)$ at α_0 is $p^{-12/(p-1,12)}$. This completes the proof of the proposition. □

6 PROOF OF THEOREM 1.3.1

6.1

We keep to assume $N = p^n$, where $p \geq 5$ is a prime and n is a positive integer. As in §4, we write $P_i := Q_{p^i}$ for the cusp of level p^i for $i = 0, \dots, n$ (see §3.1). The residue field of P_i is given by

$$\mathbb{Q}(P_i) = \mathbb{Q}(\zeta_{p^{d(i)}}), \quad d(i) = \min(i, n-i).$$

Our task is to show the injectivity of the composition map

$$\mathscr{C}(p^n) \hookrightarrow J_0(p^n)(\mathbb{Q})_{\mathrm{Tor}} \xrightarrow{\delta} \bigoplus_{i=0}^{n-1} \mathbb{Q}(P_i)^\times \otimes \mathbb{Q}/\mathbb{Z}, \tag{10}$$

where δ is the map from (2).

LEMMA 6.1.1 *Let $p \geq 3$ be a prime and $m \in \mathbb{Z}_{>0}$. Then the maps*

$$\mathbb{Q}/\mathbb{Z} \to \mathbb{Q}^\times \otimes \mathbb{Q}/\mathbb{Z},\ x \mapsto p \otimes x,$$
$$\mathbb{Q}/\mathbb{Z} \to \mathbb{Q}(\zeta_{p^m})^\times \otimes \mathbb{Q}/\mathbb{Z},\ x \mapsto \sqrt{p^*} \otimes x,$$

are (split) injections. (See (9) *for the definition of $\sqrt{p^*}$.)*

Proof. Splitting is automatic because $\mathbb{Q}/\mathbb{Z}$ is injective. The first statement follows from the elementary fact that $\mathbb{Q}^\times$ is the direct sum of $\{\pm 1\}$ and the free abelian group on the set of all prime numbers. From this, the second statement is reduced to showing

$$\ker[\mathbb{Q}^\times \otimes (\mathbb{Q}/\mathbb{Z}) \to \mathbb{Q}(\zeta_{p^m})^\times \otimes (\mathbb{Q}/\mathbb{Z})] = \{0, p^* \otimes \frac{1}{2}\}. \tag{11}$$

The right hand side is contained in the left, because $\sqrt{p^*} \in \mathbb{Q}(\zeta_{p^m})$. Thus it suffices to show the left hand side of (11) is of order 2. Put $\mathbb{Q}/\mathbb{Z}(1) := \mu(\overline{\mathbb{Q}})$. In terms of Galois cohomology, this group can be rewritten as

$$\ker[H^1(\mathbb{Q}, \mathbb{Q}/\mathbb{Z}(1)) \to H^1(\mathbb{Q}(\zeta_{p^m}), \mathbb{Q}/\mathbb{Z}(1))],$$

which is then identified with

$$H^1(G, H^0(\mathbb{Q}(\zeta_{p^m}), \mathbb{Q}/\mathbb{Z}(1))), \quad G = \mathrm{Gal}(\mathbb{Q}(\zeta_{p^m})/\mathbb{Q})$$

by the inflation-restriction sequence. Note that $H^0(\mathbb{Q}(\zeta_{p^m}), \mathbb{Q}/\mathbb{Z}(1)) = \mu_{2p^m}$. Since $G \cong (\mathbb{Z}/p^m\mathbb{Z})^\times$ is a cyclic group, the order of $H^1(G, \mu_{2p^m})$ agrees with that of the Tate cohomology

$$\hat{H}^0(G, \mu_{2p^m}) := \frac{\{x \in \mu_{2p^m} \mid \sigma(x) = x \text{ for all } \sigma \in G\}}{\{\prod_{\sigma \in G} \sigma(x) \mid x \in \mu_{2p^m}\}}.$$

Direct computation shows that $\hat{H}^0(G, \mu_{2p^m})$ is of order two. This completes the proof of the lemma. □

6.2

Let Λ_i be the subgroup of $\mathbb{Q}(P_i)^\times/\mu(\mathbb{Q}(P_i))$ generated by p (resp. $\sqrt{p^*}$) for $i = 0$ (resp. for $i = 1, \ldots, n-1$). We also let

$$\Lambda := \bigoplus_{i=0}^{n-1} \Lambda_i \subset \bigoplus_{i=0}^{n-1} \mathbb{Q}(P_i)^\times/\mu(\mathbb{Q}(P_i)).$$

Proposition 5.4.1 and Lemma 2.3.1 show that the map δ in (10) factors as

$$\begin{tikzcd} \mathscr{C}(p^n) \arrow[r, "\widetilde{\delta}"] \arrow[dr, "(10)"'] & \Lambda \otimes \mathbb{Q}/\mathbb{Z} \arrow[d, hook] \\ & \bigoplus_{i=0}^{n-1} \mathbb{Q}(P_i)^\times \otimes \mathbb{Q}/\mathbb{Z}, \end{tikzcd} \tag{12}$$

where the right vertical injection is provided by Lemma 6.1.1. We are reduced to showing the injectivity of $\widetilde{\delta}$.

We choose a uniformizer t_{P_i} described in Lemma 5.2.1 at each cusp P_i. Using them, we define a homomorphism

$$\Delta : \mathscr{P}(p^n) \to \Lambda \tag{13}$$

by, for any $h \in K^\times$ such that $\mathrm{div}(h)$ is supported on $C_0(p^n)$,

$$\Delta(\mathrm{div}(h)) = \Big((\frac{h}{t_{P_n}^{\mathrm{ord}_{P_n}(h)}})(P_n)(\frac{t_{P_i}^{\mathrm{ord}_{P_i}(h)}}{h})(P_i) \Big)_{i=0}^{n-1} \in \Lambda \subset \bigoplus_{i=0}^{n-1} \mathbb{Q}(P_i)^\times/\mu(\mathbb{Q}(P_i)).$$

Note that the image of Δ is contained in Λ by Propositions 4.1.1 and 5.4.1. Note also that, unlike δ, this map depends on our choice of uniformizers t_{P_i}.

Recall that $a = (p-1)/(p-1, 12)$. Put $a' = 12/(p-1, 12)$.

Lemma 6.2.1 *1. The map Δ is injective.*

2. *The cokernel of* Δ *is a cyclic group of order* a' *generated by the class of* $\lambda := p \in \Lambda_0 \subset \Lambda$.

3. *There exist* $c_0, \dots, c_{n-2} \in \mathbb{Z}$ *such that* $a'\lambda = \Delta(\mathrm{div}(fg_0^{c_0} \dots g_{n-2}^{c_{n-2}}))$. *Here* $f, g_0, \dots, g_{n-2}$ *are functions introduced in Proposition 4.1.1.*

Proof. Recall from Corollary 4.1.2 (1) that $\mathrm{div}(f), \mathrm{div}(g_0), \dots, \mathrm{div}(g_{n-2})$ form a $\mathbb{Z}$-basis of $\mathscr{P}(p^n)$. Let us take a $\mathbb{Z}$-basis of $\Lambda = \oplus_{i=0}^{n-1}\Lambda_i$ given by the generators $\lambda = p \in \Lambda_0$ and $\sqrt{p^*} \in \Lambda_i$ for $i = 1, \dots, n-1$. Then Proposition 5.4.1 shows that the map Δ is represented by

$$\begin{pmatrix} a' & 0 & 0 & 0 & \dots & 0 \\ 1 & 1 & 0 & 0 & \dots & 0 \\ 1 & 2 & 1 & 0 & \dots & 0 \\ 1 & 2 & 2 & 1 & \dots & 0 \\ \vdots & & & & & \vdots \\ 1 & 2 & \dots & 2 & 2 & 1 \end{pmatrix}$$

from which the lemma follows. $\square$

6.3 Proof of Theorem 1.3.1

Recall from Lemma 6.2.1 (1) that the map Δ defined in (13) is injective. Since $\mathscr{P}(p^n)$ is of finite index in $\mathscr{D}(p^n)$ (see (5)), Δ has a unique extension

$$\widetilde{\Delta} : \mathscr{D}(p^n) \to \Lambda \otimes \mathbb{Q}.$$

which is also injective. By Lemma 2.3.1, we have a commutative diagram with exact rows

$$\begin{tikzcd} 0 \arrow[r] & \mathscr{P}(p^n) \arrow[r] \arrow[d, "\Delta"] & \mathscr{D}(p^n) \arrow[r] \arrow[d, "\widetilde{\Delta}"] & \mathscr{C}(p^n) \arrow[r] \arrow[d, "\widetilde{\delta}"] & 0 \\ 0 \arrow[r] & \Lambda \arrow[r] & \Lambda \otimes \mathbb{Q} \arrow[r] & \Lambda \otimes \mathbb{Q}/\mathbb{Z} \arrow[r] & 0. \end{tikzcd}$$

where $\widetilde{\delta}$ is from (12). We get an exact sequence

$$0 \to \ker(\widetilde{\delta}) \to \mathrm{Coker}(\Delta) \xrightarrow{\psi} \mathrm{Coker}(\widetilde{\Delta}). \tag{14}$$

It remains to show ψ is injective. In view of Lemma 6.2.1 (2), this amounts to showing that the image of $\lambda = p \in \Lambda_0 \subset \Lambda$ in $\mathrm{Coker}(\widetilde{\Delta})$ has order a'. Let $b > 0$ be a divisor of a' such that the image of $b\lambda$ vanishes in $\mathrm{Coker}(\widetilde{\Delta})$. This means that $\mathrm{div}(fg_0^{c_0} \dots g_{n-2}^{c_{n-2}}) = (a'/b)\mathcal{E}$ for some $\mathcal{E} \in \mathscr{D}(p^n)$, where $c_0, \dots, c_{n-2} \in \mathbb{Z}$ are taken from Lemma 6.2.1 (3). Since a and a' are relatively prime to each other, Corollary 4.1.2 (2) shows that b must be a'. This completes the proof. $\square$

7 The case of $N = pq$

7.1

In this section, we present an outline of the proof of Proposition 1.3.2. Since the proof goes similarly with Theorem 1.3.1, we will be brief and omit details. Let $N = pq$ where p, q are two distinct prime numbers such that $p \equiv q \equiv 1 \bmod 12$. We use Takagi's result [9, Theorem 5.1] that determines the order of $\mathscr{C}(N)$ for any square free N. Here we state it in the special case $N = pq, p, q \equiv 1 \mod 12$:

Proposition 7.1.1 (Takagi) *The order of $\mathscr{C}(pq)$ is given by $4abc$, where*

$$a = \frac{(p-1)(q+1)}{24},\ b = \frac{(p+1)(q-1)}{24},\ c = \frac{(p-1)(q-1)}{24}.$$

7.2 Proof of Proposition 1.3.2

There are exactly four cusps on $X_0(pq)$, all of which are $\mathbb{Q}$-rational. Their levels are $1, p, q, pq$ (see §3.1). We give their names as follows:

$$C_0(pq) = \{P_0 = Q_1,\ P_1 = Q_p, P_2 = Q_q, P_3 = Q_{pq}\}$$

so that we have a $\mathbb{Z}$-basis of $\mathscr{D}(pq)$ given by

$$D_1 = P_0 - P_3,\ D_2 = P_1 - P_3,\ D_3 = P_2 - P_3.$$

Using Proposition 7.1.1, one sees that the group $\mathscr{P}(pq)$ is generated by the divisors of

$$f_1 = \frac{\eta(\tau)\eta(q\tau)}{\eta(p\tau)\eta(pq\tau)},\ \ f_2 = \frac{\eta(\tau)\eta(p\tau)}{\eta(q\tau)\eta(pq\tau)},\ \ f_3 = \frac{\eta(\tau)\eta(pq\tau)}{\eta(p\tau)\eta(q\tau)}$$

by an argument similar to Proposition 4.1.1. Lemma 3.2.2 shows that the divisors of the functions f_1, f_2, f_3 are respectively given by

$$a(D_1 - D_2 + D_3),\ \ b(D_1 + D_2 - D_3),\ \ c(D_1 - D_2 - D_3).$$

Let $m \in \{1, p, q, pq\}$ and put $m' = pq/m$. Choose integers b and d such that $dm' - bm = 1$. Put

$$\sigma_m := \begin{pmatrix} m' & b \\ pq & dm' \end{pmatrix}.$$

Then σ_m normalizes $\Gamma_0(pq)$ and satisfies $\sigma_m\infty = 1/m$. We may take $e^{2\pi i \sigma_m^{-1}\tau}$ as a local uniformizer at the cusp of level m (cf. Lemma 5.2.1). With this choice, the leading coefficients of f_1, f_2, f_3, up to ± 1 signs, are given by the following table:

	P_0	P_1	P_2	P_3
f_1	p	1	p	1
f_2	q	q	1	1
f_3	1	1	1	1

Finally, by using Lemma 2.3.1, we find the kernel of $\mathscr{C}(pq) \hookrightarrow J_0(pq)(\mathbb{Q})_{\mathrm{Tor}} \xrightarrow{\delta} (\mathbb{Q}^\times)^3 \otimes \mathbb{Q}/\mathbb{Z}$ is a cyclic group of order c generated by the class of $D_1 - D_2 - D_3$. $\square$

Acknowledgement. The authors would like to thank the anonymous referee for the detailed comments.

References

[1] Gérard Ligozat. *Courbes modulaires de genre* 1. Société Mathématique de France, Paris, 1975. Bull. Soc. Math. France, Mém. 43, Supplément au Bull. Soc. Math. France Tome 103, no. 3.

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

[3] Dino J. Lorenzini. Torsion points on the modular Jacobian $J_0(N)$. *Compositio Math.*, 96(2):149–172, 1995.

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

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

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

[7] Masami Ohta. Eisenstein ideals and the rational torsion subgroups of modular Jacobian varieties II. *Tokyo J. Math.*, 37(2):273–318, 2014.

[8] Jean-Pierre Serre. *Algebraic groups and class fields*, volume 117 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1988. Translated from the French.

[9] 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.

[10] Heinrich Weber. *Lehrbuch der Algebra, Vol. III.* Chelsea, New York, 1961.

Takao Yamazaki
Mathematical Institute
Tohoku University
Aoba, Sendai 980-8578
Japan
ytakao@math.tohoku.ac.jp

Yifan Yang
Department of
Applied Mathematics
National Chiao Tung University
Hsinchu 300
Taiwan
yfyang@math.nctu.edu.tw