J. London Math. Soc. (2) 82 (2010) 203–228
doi:10.1112/jlms/jdq013

Structure of the cuspidal rational torsion subgroup of $J_1(p^n)$

Yifan Yang and Jeng-Daw Yu

Abstract

Let p be a prime and let $J_1(p^n)$ denote the Jacobian of the modular curve $X_1(p^n)$. The Jacobian $J_1(p^n)$ contains a $\mathbb{Q}$-rational torsion subgroup generated by the cuspidal divisor classes $[(a/p^n) - (\infty)]$, where $p \nmid a$. In this paper, we determine the structure of the p-primary subgroup of this $\mathbb{Q}$-rational torsion subgroup in the case where p is a regular prime.

1. *Introduction and statements of results*

Let Γ be a congruence subgroup of $\mathrm{SL}(2,\mathbb{Z})$. The modular curve $X(\Gamma)$ and its Jacobian variety $J(\Gamma)$ are very important objects in number theory. For instance, the problem of determining all possible structures of a ($\mathbb{Q}$-)rational torsion subgroup of elliptic curves over $\mathbb{Q}$ is equivalent to that of determining whether the modular curves $X_1(N)$ have non-cuspidal rational points. Also, the celebrated theorem of Wiles and others shows that every elliptic curve over $\mathbb{Q}$ is a factor of the Jacobian $J_0(N)$. In the present paper, we are concerned with the arithmetic aspect of the Jacobian variety $J_1(N)$ of the modular curve $X_1(N)$. In particular, we will study the structure of the ($\mathbb{Q}$-)rational torsion subgroup of $J_1(N)$.

Recall that the modular curve $X_1(N)$ possesses a model over $\mathbb{Q}$ on which the cusp ∞ is a ($\mathbb{Q}$-)rational point (see [**11**, Chapter 6] for details). Thus, if P is another rational cusp, then the image of P under the cuspidal embedding $i_\infty : X_1(N) \to J_1(N)$ sending P to the divisor class $[(P) - (\infty)]$ will be a rational point on $J_1(N)$. Moreover, according to a result of Manin [**9**], the point $i_\infty(P)$ is of finite order. In other words, the rational torsion subgroup of $J_1(N)$ contains a subgroup generated by the image of rational cusps under i_∞. More generally, if D is a divisor of degree 0 defined over $\mathbb{Q}$ that is supported by cusps, then the divisor class of D gives us a rational torsion point on the Jacobian. We refer to the rational torsion subgroup arising in this way as the *cuspidal rational torsion subgroup* of $J_1(N)$. In general, it is believed that the cuspidal rational torsion subgroup should be the whole rational torsion subgroup. (For primes p, the conjecture was formally stated in [**1**, Conjecture 6.2.2]. The conjecture was verified for a few cases in the same paper.) Note that, for the case $J_0(p)$, the Jacobian of $X_0(p)$ of prime level p, Mazur [**10**, Theorem 1] has already shown that all rational torsion points are generated by the divisor class $[(0) - (\infty)]$.

On the aforementioned model of $X_1(N)$, all the cusps of type k/N with $(k,N) = 1$ are rational over $\mathbb{Q}$ (see, for example, [**12**, Theorem 1.3.1]). Moreover, if the level N is relatively prime to 6, then these cusps are the only rational cusps. Since these cusps are precisely those lying over ∞ of $X_0(N)$, for convenience, we shall call them the *∞-cusps*. Now suppose that we are given a divisor D of degree 0 supported by the ∞-cusps on $X_1(N)$. Then the order of the divisor class $[D]$ in $J_1(N)$ is simply the smallest positive integer m such that mD is a principal divisor, that is, the divisor of a modular function on $X_1(N)$. Therefore, to determine the group

Received 19 August 2008; revised 4 June 2009; published online 29 June 2010.

2000 *Mathematics Subject Classification* 11G18 (primary), 11F11, 14G35, 14H40 (secondary).

The first author's visit was supported by a fellowship of the Max-Planck-Institut. He was also partially supported by Grant 96-2628-M-009-014 of the National Science Council, Taiwan. The second author was supported in part by Professor N. Yui's Discovery Grant from NSERC, Canada.

structure of the cuspidal rational torsion subgroup of $J_1(N)$ generated by the ∞-cusps, it is vital to study the group of modular units on $X_1(N)$ having divisors supported on the ∞-cusps. (In the literature, if a modular function f on a congruence subgroup Γ has a divisor supported on cusps, then f is called a *modular unit*.)

In a series of papers [3–7], Kubert and Lang studied the group of modular units on $X(N)$ and $X_1(N)$. For the curves $X_1(N)$, in [8, Chapter 3] they showed that all modular units on $X_1(N)$ with divisors supported on the ∞-cusps are products of a certain class of Siegel functions (see Subsection 3.1 for details). Furthermore, in [7] they also determined the order of the torsion subgroup of $J_1(p^n)$ generated by the ∞-cusps for the case p is a prime greater than 3. (The case $N = p$ was first obtained in [2]). Then Yu [18] gave a formula for all positive integers N. (Note that all the results mentioned above dealt with modular units with divisors supported on the cusps lying over 0 of $X_0(N)$, instead of the ∞-cusps, but it is easy to translate the results using the Atkin–Lehner involution $\left(\begin{smallmatrix} 0 & -1 \\ N & 0 \end{smallmatrix}\right)$.)

In a very recent paper [17], we applied Yu's divisor class number formula to determine an explicit basis for the group of modular units on $X_1(N)$ with divisors supported on the ∞-cusps for any positive integer N. As applications, we used the basis to compute the group structure of the cuspidal rational torsion subgroup of $J_1(N)$ with divisors supported on the ∞-cusps. A remarkable discovery is that, when p is a regular prime, the structure of the p-primary subgroup of the cuspidal rational torsion subgroup of $J_1(p^n)$ seems to follow a simple pattern. (Recall that an odd prime p is said to be *regular* if p does not divide the numerators of the Bernoulli numbers $B_2, B_4, \dots, B_{p-3}$.)

More precisely, let p be a prime, let n be a positive integer and let $\mathscr{C}_1^\infty(p^n)$ be the subgroup of $J_1(p^n)$ generated by the ∞-cusps. Consider the endomorphism $[p] : \mathscr{C}_1^\infty(p^n) \to \mathscr{C}_1^\infty(p^n)$ defined by multiplication by p. Define the *p-rank* of $\mathscr{C}_1^\infty(p^n)$ to be the integer k such that the kernel of $[p]$ has p^k elements.

Conjecture (Yang [17]). Assume that p is a regular prime. Then the p-rank of $\mathscr{C}_1^\infty(p^n)$ is

$$\frac{1}{2}(p-1)p^{n-2} - 1$$

for prime power $p^n \geqslant 8$ with $n \geqslant 2$. More precisely, the number of copies of $\mathbb{Z}/p^{2k}\mathbb{Z}$ in the primary decomposition of $\mathscr{C}_1^\infty(p^n)$ is given by

$$\begin{cases} \frac{1}{2}(p-1)^2p^{n-k-2} - 1 & \text{if } p = 2 \text{ and } k \leqslant n-3, \\ \frac{1}{2}(p-1)^2p^{n-k-2} - 1 & \text{if } p \geqslant 3 \text{ and } k \leqslant n-2, \\ \frac{1}{2}(p-5) & \text{if } p \geqslant 5 \text{ and } k = n-1, \\ 0 & \text{else.} \end{cases}$$

and the number of copies of $\mathbb{Z}/p^{2k-1}\mathbb{Z}$ is given by

$$\begin{cases} 1 & \text{if } p = 2 \text{ and } k \leqslant n-3, \\ 1 & \text{if } p = 3 \text{ and } k \leqslant n-2, \\ 1 & \text{if } p \geqslant 5 \text{ and } k \leqslant n-1, \\ 0 & \text{otherwise.} \end{cases}$$

Example. For the primes $p = 2$, 3, 5, the above conjecture asserts that the p-parts of $\mathscr{C}_1^\infty(p^n)$ follow the pattern depicted in Table 1. Here the notation $(p^{e_1})^{n_1} \dots (p^{e_k})^{n_k}$ means that the primary decomposition of $\mathscr{C}_1^\infty(p^n)$ contains n_i copies of $\mathbb{Z}/p^{e_i}\mathbb{Z}$.

TABLE 1. *The p-primary part of* $\mathscr{C}_1^\infty(p^n)$.

p^n	p-primary subgroups
2^4	(2)
2^5	$(2)(2^2)(2^3)$
2^6	$(2)(2^2)^3(2^3)(2^4)(2^5)$
2^7	$(2)(2^2)^7(2^3)(2^4)^3(2^5)(2^6)(2^7)$
3^3	$(3)(3^2)$
3^4	$(3)(3^2)^5(3^3)(3^4)$
3^5	$(3)(3^2)^{17}(3^3)(3^4)^5(3^5)(3^6)$
3^6	$(3)(3^2)^{53}(3^3)(3^4)^{17}(3^5)(3^6)^5(3^7)(3^8)$
5^2	(5)
5^3	$(5)(5^2)^7(5^3)$
5^4	$(5)(5^2)^{39}(5^3)(5^4)^7(5^5)$
5^5	$(5)(5^2)^{199}(5^3)(5^4)^{39}(5^5)(5^6)^7(5^7)$

The main purpose of the present paper is to prove this conjecture.

THEOREM A. *The conjecture is true.*

We note that the assumption that p is a regular prime is crucial in the proof of Theorem A. This assumption is used to establish an exact formula for the p-rank of $\mathscr{C}_1^\infty(p^n)$ and to determine the kernel of the homomorphism $\mathscr{C}_1^\infty(p^n) \to \mathscr{C}_1^\infty(p^{n-1})$ induced from the covering $X_1(p^n) \to X_1(p^{n-1})$. At present, we do not know how to extend our method to the case of irregular primes.

On the other hand, it is possible to obtain a similar result for modular curves $X_1(p^nq^m)$, where q is another prime, under the assumption that the product

$$p\prod_{\chi}\frac{1}{4}B_{2,\chi}$$

of generalized Bernoulli numbers $B_{2,\chi}$ associated with even Dirichlet characters χ mod pq^m is a p-unit. For example, following the argument in the present paper, we can show that the 2-primary subgroup of the torsion subgroup of $J_1(3\cdot 2^n)$ generated by the ∞-cusps is isomorphic to

$$\prod_{k=1}^{n-2}(\mathbb{Z}/2^{2k}\mathbb{Z})^{2^{n-k-2}}.$$

However, we will not pursue this direction here because it does not constitute a significant extension of Theorem A and the proof of some key lemmas in these cases is much more complicated than the prime power cases. (For instance, it takes more than one page just to describe the basis for the group of modular units on $X_1(p^nq^m)$.)

REMARK. Note that in a recent work [**13**], Sun considered the ℓ-adic evaluation $v_\ell(|\mathscr{C}_1^\infty(Np^n)|)$ for a prime $\ell \neq p$. His result showed that there exists an integer ν such that

$$v_\ell(|\mathscr{C}_1^\infty(Np^n)|) = \tau p^{n-1} + \nu$$

for all sufficiently large n, where

$$\tau = \begin{cases} (p-1)\phi(N/\ell^{v_\ell(N)})(\ell^{v_\ell(N)-1}-1) & \text{if } \ell \mid N, \\ 0 & \text{if } \ell \nmid N. \end{cases}$$

This formula in particular implies that if $\ell^2 \nmid N$, then the ℓ-adic valuation of $|\mathscr{C}_1^\infty(Np^n)|$ eventually becomes a constant for all sufficiently large n. This result is comparable to Washington's theorem [14] on the boundedness of the ℓ-part of ideal class groups in a $\mathbb{Z}_p$ extension of an abelian number field.

The rest of the article is organized as follows. In Section 2, we describe our strategy in proving Theorem A. We will show that Theorem A will follow immediately from five properties of the divisor groups, namely, Propositions 1–5. In Section 3, we review our basis for the group of modular units on $X_1(N)$, which constitutes the cornerstone of our argument. In Section 4, we study the natural maps between the cuspidal groups in different levels. We then give the proof of the five propositions in Section 5.

2. *Outline of proof of Theorem A*

In this section, we first collect all the notation and conventions used throughout the paper. We then describe our strategy in proving Theorem A. Our arguments depend crucially on our explicit knowledge on the basis for the group of modular units on $X_1(N)$, which will be reviewed in Subsection 3.2.

2.1. *Notation and conventions*

Let p be a prime. We fix an integer α that generates $(\mathbb{Z}/p^{n+1}\mathbb{Z})^\times/\pm 1$ for all integers $n \geqslant 0$. Explicitly, for $p = 2$, we choose $\alpha = 3$, and for an odd prime p, we let α be an integer that generates $(\mathbb{Z}/p\mathbb{Z})^\times$ but satisfies $\alpha^{p-1} \not\equiv 1 \bmod p^2$. For $n \geqslant 0$, we define

X_n = the modular curve $X_1(p^{n+1})$,
C_n = the set of cusps of X_n lying over ∞ of $X_0(p^{n+1})$, that is, the set of ∞-cusps,
$\phi_n = |C_n| = \phi(p^{n+1})/2 = p^n(p-1)/2$,
$P_{n,k}$ = the cusp α^k/p^{n+1} in C_n,
$\mathscr{D}_n$ = the group of divisors of degree 0 on X_n having support on C_n,
$\mathscr{F}_n$ = the group of modular units on X_n having divisors supported on C_n,
$\mathscr{P}_n = \operatorname{div} \mathscr{F}_n$, the subgroup of principal divisors on X_n having support on C_n,
$\mathscr{C}_n = \mathscr{D}_n/\mathscr{P}_n$, the rational torsion subgroup of $J_1(p^{n+1})$ generated by C_n,
π_n = the canonical homomorphism from $\mathscr{D}_n$ to $\mathscr{D}_{n-1}$ induced from the covering

$$X_n \to X_{n-1},$$

ι_n = the embedding $\mathscr{D}_{n-1} \to \mathscr{D}_n$ defined by

$$\iota_n(P) = p \sum_{Q:\ \pi_n(Q)=P} Q.$$

Note that $P_{n,k}$ and $P_{n,m}$ represent the same cusp on X_n if and only if $k \equiv m \bmod \phi_n$. Then we have $C_n = \{P_{n,k} :\ k = 0, \dots, \phi_n - 1\}$, and

$$\pi_n(P_{n,k}) = P_{n-1,k}, \quad \iota_n(P_{n-1,k}) = p \sum_{h=0}^{p-1} P_{n,k+h\phi_{n-1}}.$$

Since we are mainly interested in the orders of a function at the ∞-cusps, for a modular function f on X_n, we introduce the notation $\operatorname{div}^\infty$ denoting the C_n-part

$$\operatorname{div}^\infty f = \sum_{P \in C_n} \operatorname{ord}_f(P) P$$

of the divisor of f.

Finally, the generalized Bernoulli numbers $B_{k,\chi}$ associated with a Dirichlet character χ mod N, not necessarily primitive, are defined by the series

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

In particular, we have

$$B_{2,\chi} = N\sum_{r=1}^{N}\chi(r)B_2\left(\frac{r}{N}\right) = N\sum_{r=1}^{N}\chi(r)\left(\frac{r^2}{N^2}-\frac{r}{N}+\frac{1}{6}\right).$$

Here $B_2(x) = \{x\}^2 - \{x\} + 1/6$ and $\{x\}$ denotes the fractional part of a real number x. The readers should be mindful that our definition differs from some other authors' definition. See the remark following Theorem E for details.

2.2. *Outline of proof of Theorem A*

In this section, we will describe our strategy in proving Theorem A.

Intuitively, just by looking at Table 1, one immediately realizes that if the conjecture is to hold, then the p-primary subgroup of $\mathscr{C}_n/\ker[p^2]$ must have the same structure as that of $\mathscr{C}_{n-1}$, where $[p^2]$ denotes the multiplication-by-p^2 homomorphism for an additive group, and one expects that there should be a canonical isomorphism between the p-primary subgroups of the two groups. The only sensible candidate for such an isomorphism is the one induced by the covering $X_n \to X_{n-1}$. To establish this isomorphism, we first show that π_n induces an isomorphism between the p-part of $\mathscr{C}_n = \mathscr{D}_n/\mathscr{P}_n$ and that of $\pi_n(\mathscr{D}_n)/\pi_n(\mathscr{P}_n) = \mathscr{D}_{n-1}/\pi_n(\mathscr{P}_n)$. We then show that the kernel of $[p^2]$ of the latter group is $\mathscr{P}_{n-1}/\pi_n(\mathscr{P}_n)$, and thereby establish the isomorphism. The following diagram illustrate the relations between various groups:

$$\begin{array}{ccc}
\mathscr{C}_n = \mathscr{D}_n/\mathscr{P}_n & \xrightarrow[p\text{-part}\,\simeq]{\pi_n} & \mathscr{D}_{n-1}/\pi_n(\mathscr{P}_n) \\
\Big\downarrow{\scriptstyle /\ker[p^2]} & & \Big\downarrow{\scriptstyle /\ker[p^2]} \\
\mathscr{C}_n/\ker[p^2] & \xrightarrow[p\text{-part}\,\simeq]{} & \mathscr{C}_{n-1} = \mathscr{D}_{n-1}/\mathscr{P}_{n-1}
\end{array}$$

Now assume that the isomorphism between the p-parts of $\mathscr{C}_n/\ker[p^2]$ and $\mathscr{C}_{n-1}$ is established. This would show that if the p-part of $\mathscr{C}_{n-1}$ is $\prod(\mathbb{Z}/p^{e_i}\mathbb{Z})^{r_i}$, then the p-part of $\mathscr{C}_n$ is $(\mathbb{Z}/p\mathbb{Z})^{s_1} \times (\mathbb{Z}/p^2\mathbb{Z})^{s_2} \times \prod(\mathbb{Z}/p^{e_i+2}\mathbb{Z})^{r_i}$ for some non-negative integers s_1 and s_2. If we can determine the p-ranks of $\mathscr{C}_{n-1}$ and $\mathscr{C}_n$ and the index of $\pi_n(\mathscr{P}_n)$ in $\mathscr{P}_{n-1}$, this will yield information about s_1+s_2 and s_1+2s_2, respectively, which in turn will give us the exact values of s_1 and s_2. Finally, if we know the structure of $\mathscr{C}_0$ ($\mathscr{C}_1$ for $p=3$ and $\mathscr{C}_2$ for $p=2$), then the structure of the p-primary subgroup of $\mathscr{C}_n$ is determined for all n.

In summary, to establish Theorem A, it suffices to prove the following propositions.

PROPOSITION 1. *If p is a regular prime, then p does not divide $|\mathscr{C}_0|$. Also, if $p=2$ and $p=3$, then $p \nmid |\mathscr{C}_1|$, and if $p=2$, then $p \nmid |\mathscr{C}_2|$.*

PROPOSITION 2. *Let p be a regular prime. If $p^{n+1} \geqslant 5$, then the p-rank of $\mathscr{C}_n$ is $p^{n-1}(p-1)/2 - 1$.*

PROPOSITION 3. *For all primes p, we have $\pi_n(\mathscr{P}_n) \subset \mathscr{P}_{n-1}$, and the index of $\pi_n(\mathscr{P}_n)$ in $\mathscr{P}_{n-1}$ is $p^{p^{n-1}(p-1)-3}$ if $p^{n+1} \geqslant 5$. Moreover, the structure of the factor group $\mathscr{P}_{n-1}/\pi_n(\mathscr{P}_n)$ is given by*

$$(\mathbb{Z}/p^2\mathbb{Z})^{p^{n-1}(p-1)/2-2} \times (\mathbb{Z}/p\mathbb{Z}).$$

PROPOSITION 4. *Assume that p is a regular prime. Then the p-part of $\mathscr{C}_n = \mathscr{D}_n/\mathscr{P}_n$ is isomorphic to the p-part of $\mathscr{D}_{n-1}/\pi_n(\mathscr{P}_n)$.*

PROPOSITION 5. *Let p be a prime. Then the kernel of the multiplication-by-p^2 endomorphism $[p^2]$ of $\mathscr{D}_{n-1}/\pi_n(\mathscr{P}_n)$ is $\mathscr{P}_{n-1}/\pi_n(\mathscr{P}_n)$.*

REMARK. We remark that the assumption that p is a regular prime is crucial in the proof of Propositions 1, 2 and 4. In fact, the assumption is a necessary and sufficient condition for the three propositions. For example, by carefully examining the proof of Proposition 2, one sees that if p is an irregular prime, then the p-rank of $\mathscr{C}_n$ is strictly greater than $p^{n-1}(p-1)/2-1$.

The proof of these propositions will be postponed until Section 5. Here let us formally complete the proof of Theorem A, assuming the truth of the propositions.

Proof of Theorem A. By Propositions 4 and 5, when p is a regular prime, we have

$$\begin{aligned} p\text{-part of } \mathscr{C}_n/\ker[p^2] &\simeq p\text{-part of } (\mathscr{D}_{n-1}/\pi_n(\mathscr{P}_n))/\ker[p^2] \\ &= p\text{-part of } (\mathscr{D}_{n-1}/\pi_n(\mathscr{P}_n))/(\mathscr{P}_{n-1}/\pi_n(\mathscr{P}_n)) \\ &\simeq p\text{-part of } \mathscr{D}_{n-1}/\mathscr{P}_{n-1} = \mathscr{C}_{n-1}, \end{aligned}$$

Thus, if the structure of the p-part of $\mathscr{C}_{n-1}$ is given by

$$\prod_{i=1}^{k}(\mathbb{Z}/p^{e_i}\mathbb{Z})^{r_i},$$

then, according to the structure theorem for finite abelian groups, the structure of the p-part of $\mathscr{C}_n$ is as follows:

$$(\mathbb{Z}/p\mathbb{Z})^{s_1} \times (\mathbb{Z}/p^2\mathbb{Z})^{s_2} \times \prod_{i=1}^{k}(\mathbb{Z}/p^{e_i+2}\mathbb{Z})^{r_i}$$

for some non-negative integers s_1 and s_2. Here the sum of r_i is what we call the p-rank of $\mathscr{C}_{n-1}$, and the sum of s_1, s_2 and r_i is the p-rank of $\mathscr{C}_n$. Using Proposition 2, we find that the integers s_1 and s_2 satisfy

$$s_1 + s_2 = \frac{1}{2}p^{n-2}(p-1)^2. \tag{1}$$

On the other hand, by Propositions 3 and 4, we know that

$$p\text{-part of } |\mathscr{C}_n|/|\mathscr{C}_{n-1}| = |\mathscr{P}_{n-1}/\pi_n(\mathscr{P}_n)| = p^{p^{n-1}(p-1)-3},$$

which, together with Proposition 2, implies that

$$s_1 + 2s_2 = (p^{n-1}(p-1)-3) - 2(p^{n-2}(p-1)/2-1) = p^{n-2}(p-1)^2 - 1.$$

Combining this with (1), we get $s_1 = 1$ and $s_2 = p^{n-2}(p-1)^2/2-1$. Finally, Proposition 1 shows that the p-part of $\mathscr{C}_0$ ($\mathscr{C}_1$ for $p=3$ and $\mathscr{C}_2$ for $p=2$) is trivial. Then an induction argument gives the claimed result. □

3. *Group of modular units on $X_1(N)$*

In this section, we will introduce our basis for the group $\mathscr{F}_n$, which is essential in our proof of Theorem A. The construction of our basis utilizes the Siegel functions.

3.1. *Siegel functions*

The Siegel functions are usually defined as products of the Klein forms and the Dedekind eta function. For our purpose, we only need to know that they have the following infinite product representation.

For a pair of rational numbers $(a_1, a_2) \in \mathbb{Q}^2 \backslash \mathbb{Z}^2$ and $\tau \in \mathbb{H}$, set $z = a_1\tau + a_2$, $q_\tau = e^{2\pi i\tau}$ and $q_z = e^{2\pi iz}$. Then the Siegel function $G_{(a_1,a_2)}(\tau)$ satisfies

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

where $B(x) = x^2 - x + 1/6$ is the second Bernoulli polynomial. To construct modular units on $X_1(N)$ with divisors supported on the ∞-cusps, we consider a special class of Siegel functions.

Given a positive integer N and an integer a not congruent to 0 mod N, we set

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

where $q = e^{2\pi i\tau}$. If the integer N is clear from the context, then we write E_a in place of $E_a^{(N)}$.

We now review the properties of E_a. The material is mainly taken from [**16**]. For more details see [**16**]. In the first lemma, we describe two simple, but yet very important, relations between Siegel functions of two different levels.

LEMMA 6. *Let M and N be two positive integers. Assume that $N = nM$ for some integer n. Let a be an integer not congruent to* 0 mod N. *Then*

$$E_{na}^{(N)}(\tau) = E_a^{(M)}(n\tau). \tag{2}$$

Moreover, for all integers a with $0 < a < M$, we have

$$N\sum_{k=0}^{n-1} B_2\left(\frac{kM+a}{N}\right) = MB_2\left(\frac{a}{M}\right), \tag{3}$$

and consequently

$$\prod_{k=0}^{n-1} E_{kM+a}^{(N)}(\tau) = E_a^{(M)}(\tau). \tag{4}$$

Proof. Relation (2) follows trivially from the definition of $E_g^{(N)}$. Property (3) can be verified by a direct computation. Relation (4) is an immediate consequence of (3) and the definition of $E_a^{(N)}$. □

The next lemma gives the transformation law for E_a under the action of matrices in $\Gamma_0(N)$.

LEMMA 7 [**16**, Corollary 2]. *For integers g not congruent to* 0 mod N, *the functions E_g satisfy*

$$E_{g+N} = E_{-g} = -E_g. \tag{5}$$

Moreover, let $\gamma = \left(\begin{smallmatrix} a & b \\ cN & d \end{smallmatrix}\right) \in \Gamma_0(N)$. *For* $c = 0$, *we have*

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

and, for $c > 0$, *we have*

$$E_g(\gamma\tau) = \epsilon(a, bN, c, d) e^{\pi i (g^2 ab/N - gb)} E_{ag}(\tau), \tag{6}$$

where

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

Remark. Note that Property (5) implies that there are only $\lceil (N-1)/2 \rceil$ essentially distinct E_g, indexed over the set $(\mathbb{Z}/N\mathbb{Z})/\pm 1 - \{0\}$. Hence, a product $\prod_g$ or a sum $\sum_g$ is understood to be running over $g \in (\mathbb{Z}/N\mathbb{Z})/\pm 1 - \{0\}$.

The functions E_g clearly have no poles or zeros in the upper half-plane. The next lemma describes the order of E_g at cusps of $X_1(N)$.

Lemma 8 [16, Lemma 2]. *The order of the function* E_g *at a cusp* 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.

The following theorem of Yu [18] characterizes the modular units on $X_1(N)$ with divisors supported at the ∞-cusps in terms of E_g.

Theorem B [18, Theorem 4]. *Let* N *be a positive integer. A modular function* f *on* $\Gamma_1(N)$ *has a divisor supported on the cusps* k/N, $(k, N) = 1$, *if and only if* $f = \prod_g E_g^{e_g}$ *with the exponents* e_g *satisfying the two conditions*

$$\sum_g g^2 e_g \equiv 0 \bmod \begin{cases} N & \text{if } N \text{ is odd}, \\ 2N & \text{if } N \text{ is even}, \end{cases} \tag{7}$$

and

$$\sum_{g \equiv \pm a \bmod N/p} e_g = 0 \tag{8}$$

for all prime factors p *of* N *and all integers* a.

Again, we remark that Theorem 4 of [18] was stated in the setting of modular units with the divisor supported on the 0-cusps, that is, the cusps lying over 0 of $X_0(N)$. Here we use the Atkin–Lehner involution $\left(\begin{smallmatrix} 0 & -1 \\ N & 0 \end{smallmatrix}\right)$ to get Theorem B from Yu's result.

3.2. *Basis for* $\mathscr{F}_n$

We now describe our basis for $\mathscr{F}_n$ constructed in [17]. The case of an odd prime p and the case of $p = 2$ are stated in Theorems C and D, respectively.

Theorem C [17, Theorem 2]. *Let* $n \geqslant 0$ *and let* $N = p^{n+1}$ *be an odd prime power. For a non-negative integer* ℓ, *we set* $\phi_\ell = \phi(p^{\ell+1})/2$. *Let* α *be a generator of the cyclic group* $(\mathbb{Z}/p^{n+1}\mathbb{Z})^\times/\pm 1$ *and let* β *be an integer such that* $\alpha\beta \equiv 1 \bmod p$. *Then a basis for* $\mathscr{F}_n \mod \mathbb{C}^\times$

is given by

$$
\begin{aligned}
f_i &= \frac{E_{\alpha^{i-1}} E^{\beta^2}_{\alpha^{i+\phi_{n-1}}}}{E_{\alpha^{i+\phi_{n-1}-1}} E^{\beta^2}_{\alpha^i}}, && i = 1, \dots, \phi_n - \phi_{n-1} - 1,\\
f_i &= \frac{E^p_{\alpha^{i-1}}}{E^p_{\alpha^{i+\phi_{n-1}-1}}}, && i = \phi_n - \phi_{n-1},\\
f_i &= \frac{E^{(p^n)}_{\alpha^{i-1}}(p\tau)}{E^{(p^n)}_{\alpha^{i+\phi_{n-2}-1}}(p\tau)}, && i = \phi_n - \phi_{n-1} + 1, \dots, \phi_n - \phi_{n-2},\\
&\vdots && \vdots\\
f_i &= \frac{E^{(p^2)}_{\alpha^{i-1}}(p^{n-1}\tau)}{E^{(p^2)}_{\alpha^{i+\phi_0-1}}(p^{n-1}\tau)}, && i = \phi_n - \phi_1 + 1, \dots, \phi_n - \phi_0,\\
f_i &= \frac{E^{(p)}_{\alpha^{i-1}}(p^n\tau)}{E^{(p)}_{\alpha^i}(p^n\tau)}, && i = \phi_n - \phi_0 + 1, \dots, \phi_n - 1.
\end{aligned}
$$

THEOREM D [17, Theorem 3]. *Let $n \geqslant 2$ and $N = 2^{n+1}$. Let $\alpha = 3$ be a generator of the cyclic group $(\mathbb{Z}/2^{n+1}\mathbb{Z})^\times/\pm 1$. For $\ell \geqslant 1$, set $\phi_\ell = \phi(2^{\ell+1})/2 = 2^{\ell-1}$. Then a basis for $\mathscr{F}_n$* mod $\mathbb{C}^\times$ *is given by*

$$
\begin{aligned}
f_i &= \frac{E_{\alpha^{i-1}} E_{\alpha^{i+\phi_{n-1}}}}{E_{\alpha^i} E_{\alpha^{i+\phi_{n-1}-1}}}, && i = 1, \dots, \phi_n - \phi_{n-1} - 1,\\
f_i &= \frac{E^2_{\alpha^{i-1}}}{E^2_{\alpha^{i+\phi_{k-1}-1}}}, && i = \phi_n - \phi_{n-1},\\
f_i &= \frac{E^{(2^n)}_{\alpha^{i-1}}(2\tau)}{E^{(2^n)}_{\alpha^{i+\phi_{n-2}-1}}(2\tau)}, && i = \phi_n - \phi_{n-1} + 1, \dots, \phi_n - \phi_{n-2},\\
&\vdots && \vdots\\
f_i &= \frac{E^{(8)}_{\alpha^{i-1}}(2^{n-2}\tau)}{E^{(8)}_{\alpha^i}(2^{n-2}\tau)}, && i = \phi_n - 1.
\end{aligned}
$$

The proofs of these two theorems use the following divisor class number formula of Kubert, Lang and Yu, which will also be used in the present paper. Note that the cases $p \geqslant 5$ were proved in [7], while the cases $p = 2$ and $p = 3$ were settled in [18]. In the same paper [18], Yu also obtained a divisor class number formula for general N, although the general result is not needed in the present paper.

THEOREM E [7, Theorem 3.4; 18, Theorem 5]. *Let $N = p^{n+1}$ be a prime power greater than 4. We have the divisor class number formula*

$$
|\mathscr{C}_n| = p^{L(p)} \prod_{\chi \neq \chi_0 \text{ even}} \frac{1}{4} B_{2,\chi}, \tag{9}
$$

where

$$L(p)=\begin{cases}p^{n-1}-2n+2 & \text{if } N=p^n \text{ and } p \text{ is odd},\\ 2^{n-1}-2n+3 & \text{if } N=2^n\geqslant 8,\end{cases}$$

and the product runs over all even non-principal Dirichlet characters modulo p^{n+1}.

Remark. We should remark that the definition of generalized Bernoulli numbers used in [7, 18] is different from ours; namely, if an even Dirichlet character $\chi \mod N$ has a conductor f, then their definition is given by

$$\frac{1}{2}\sum_{r=1}^{f}\frac{\chi_f(r)te^{rt}}{e^{ft}-1}=\sum_{k=0}^{\infty}B_{2,\chi}\frac{t^k}{k!},$$

where χ_f is the Dirichlet character modulo f that induces χ. When N is a prime power p^n and χ is not principal, the two definitions differ by a $1/2$ factor.

Moreover, the readers are reminded that there were slight errors in the original statement of [18, Theorem 5]. See the discussion following Theorem B of [17] for details.

4. *Properties of* π_n *and* ι_n

Throughout this section, we follow the notation specified in Subsection 2.1. The main results in this section are Lemmas 11 and 15, which state that π_n maps a principal divisor to a principal divisor, and that if $\iota_n(D)$ is a principal divisor, then D itself is principal. In addition, in Lemma 12 we will prove the converse of Lemma 15, that is, if D is a principal divisor in $\mathscr{D}_{n-1}$, then $\iota_n(D)$ is a principal divisor.

The first lemma is rather trivial, but it plays a crucial role in the proof of Proposition 5.

Lemma 9. *We have*

$$\pi_n\circ\iota_n=[p^2], \tag{10}$$

the multiplication-by-p^2 *endomorphism of* $\mathscr{D}_{n-1}$

Proof. The proof is obvious. □

In the next lemma we compute the image of the divisor of $E_g^{(p^{n+1})}$ under π_n. Here we recall that the notation $\operatorname{div}^\infty f$ means the C_n-part of the divisor of f.

Lemma 10. *Let* g *be an integer. For* $g\not\equiv 0 \mod p^{n+1}$, *we have*

$$\pi_n(\operatorname{div}^\infty E_g^{(p^{n+1})})=\begin{cases}\operatorname{div}^\infty E_g^{(p^n)} & \text{if } p\nmid g,\\ p^2\operatorname{div}^\infty E_{g/p}^{(p^n)} & \text{if } p\mid g.\end{cases}$$

Proof. By Lemma 8, we have

$$\operatorname{div}^\infty E_g^{(p^{n+1})}=\frac{p^{n+1}}{2}\sum_{k=0}^{\phi_n-1}B_2\left(\frac{g\alpha^k}{p^{n+1}}\right)P_{n,k}.$$

Recall that $\pi_n(P_{n,k}) = \pi_n(P_{n,h})$ if and only if $h \equiv k \mod \phi_{n-1}$. Thus, we have

$$\pi_n(\operatorname{div}^\infty E_g^{(p^{n+1})}) = \frac{p^{n+1}}{2} \sum_{k=0}^{\phi_{n-1}-1} P_{n-1,k} \sum_{h=0}^{p-1} B_2\left(\frac{g\alpha^{k+h\phi_{n-1}}}{p^{n+1}}\right).$$

Now assume that p does not divide g; then as h goes through 0 to $p-1$, the residue classes of $g\alpha^{k+h\phi_{n-1}} \bmod p^{n+1}$ go through $g\alpha^k, g\alpha^k + p^n, \dots, g\alpha^k + (p-1)p^n$. Hence, by equation (3), we find that

$$\pi_n(\operatorname{div}^\infty E_g^{(p^{n+1})}) = \frac{p^n}{2} \sum_{k=0}^{\phi_{n-1}-1} B_2\left(\frac{g\alpha^k}{p^n}\right) P_{n-1,k} = \operatorname{div}^\infty E_g^{(p^n)}.$$

When $p \mid g$, all $g\alpha^{k+h\phi_{n-1}}$ are congruent to $g\alpha^k \bmod p^{n+1}$. Therefore, we have

$$\pi_n(\operatorname{div}^\infty E_g^{(p^{n+1})}) = p^2 \cdot \frac{p^n}{2} \sum_{k=0}^{\phi_{n-1}-1} B_2\left(\frac{(g/p)\alpha^k}{p^n}\right) P_{n-1,k} = p^2 \operatorname{div}^\infty E_{g/p}^{(p^n)}.$$

This proves the lemma. □

LEMMA 11. *Assume that $n \geqslant 1$. If D is a principal divisor in $\mathscr{D}_n$, then $\pi_n(D)$ is a principal divisor in $\mathscr{D}_{n-1}$.*

More precisely, if f_i, with $i = 1, \dots, \phi_n - 1$, is the basis for $\mathscr{F}_n$ given in Theorem C, then for $p \geqslant 3$ we have

$$\pi_n(\operatorname{div} f_i) = \begin{cases} 0, & i = 1, \dots, \phi_n - \phi_{n-1}, \\ \operatorname{div} \dfrac{E_{\alpha^{i-1}}^{(p^n)}(\tau)^{p^2}}{E_{\alpha^{i+\phi_{n-2}-1}}^{(p^n)}(\tau)^{p^2}}, & i = \phi_n - \phi_{n-1} + 1, \dots, \phi_n - \phi_{n-2}, \\ \quad\vdots & \quad\vdots \\ \operatorname{div} \dfrac{E_{\alpha^{i-1}}^{(p^2)}(p^{n-2}\tau)^{p^2}}{E_{\alpha^{i+\phi_0-1}}^{(p^2)}(p^{n-2}\tau)^{p^2}}, & i = \phi_n - \phi_1 + 1, \dots, \phi_n - \phi_0, \\ \operatorname{div} \dfrac{E_{\alpha^{i-1}}^{(p)}(p^{n-1}\tau)^{p^2}}{E_{\alpha^i}^{(p)}(p^{n-1}\tau)^{p^2}}, & i = \phi_n - \phi_0 + 1, \dots, \phi_n - 1. \end{cases}$$

A similar result also holds for $p = 2$.

Proof. Here we prove that the case p is an odd prime; the proof of the case $p = 2$ is similar, and is omitted.

We first show that $\pi_n(\operatorname{div} f_i) = 0$ for $i = 1, \dots, \phi_n - \phi_{n-1}$. By Lemma 10, we have

$$\pi_n(\operatorname{div}^\infty E_{\alpha^{i-1}}^{(p^{n+1})}) = \operatorname{div}^\infty E_{\alpha^{i-1}}^{(p^n)}, \qquad \pi_n(\operatorname{div}^\infty E_{\alpha^{i+\phi_{n-1}-1}}^{(p^{n+1})}) = \operatorname{div}^\infty E_{\alpha^{i+\phi_{n-1}-1}}^{(p^n)}.$$

However, since $\alpha^{\phi_{n-1}} \equiv 1 \mod p^n$, we have $E_{\alpha^{i-1}}^{(p^n)} = \pm E_{\alpha^{i+\phi_{n-1}-1}}^{(p^n)}$ by Lemma 7. It follows that

$$\pi_n(\operatorname{div} f_i) = \pi_n(\operatorname{div}^\infty f_i) = \pi_n(\operatorname{div}^\infty E_{\alpha^{i-1}}^{(p^{n+1})} / E_{\alpha^{i+\phi_{n-1}-1}}^{(p^{n+1})}) = 0$$

for $i = 1, \dots, \phi_n - \phi_{n-1}$.

For $i = \phi_n - \phi_{n-1} + 1, \dots, \phi_n - \phi_{n-2}$, by (2) we have

$$f_i = E_{\alpha^{i-1}}^{(p^n)}(p\tau) / E_{\alpha^{i+\phi_{n-2}-1}}^{(p^n)}(p\tau) = E_{p\alpha^{i-1}}^{(p^{n+1})}(\tau) / E_{p\alpha^{i+\phi_{n-2}-1}}^{(p^{n+1})}(\tau).$$

By Lemma 10, we have

$$\pi_n(\operatorname{div} f_i) = \pi_n(\operatorname{div}^\infty f_i) = \operatorname{div}^\infty \frac{E^{(p^n)}_{\alpha^{i-1}}(\tau)^{p^2}}{E^{(p^n)}_{\alpha^{i+\phi_{n-2}-1}}(\tau)^{p^2}}.$$

Using the criteria given in Theorem B, we find the last function is in $\mathscr{F}_{n-1}$ and

$$\pi_n(\operatorname{div} f_i) = \operatorname{div} \frac{E^{(p^n)}_{\alpha^{i-1}}(\tau)^{p^2}}{E^{(p^n)}_{\alpha^{i+\phi_{n-2}-1}}(\tau)^{p^2}}.$$

This proves the case $i = \phi_n - \phi_{n-1} + 1, \dots, \phi_n - \phi_{n-2}$. The remaining cases $i = \phi_n - \phi_{n-2} + 1, \dots, \phi_n - 1$ can be proved in the same way. This gives us the lemma. □

In the next few lemmas, we will establish the fact that $D \in \mathscr{D}_{n-1}$ is principal if and only if $\iota_n(D) \in \mathscr{D}_n$ is principal.

LEMMA 12. *If D is a principal divisor in $\mathscr{D}_{n-1}$, then $\iota_n(D)$ is a principal divisor in $\mathscr{D}_n$.*

Proof. Let f^* be one of the functions in the basis of $\mathscr{F}_{n-1}$ given in Theorem C (or Theorem D if $p = 2$). Define $f(\tau) = f^*(p\tau)$. From the explicit description of the basis, we see that $f(\tau)$ is either one or a product of the functions appearing in our basis for $\mathscr{F}_n$. We now show that $\operatorname{div} f = \iota_n(f^*)$.

Assume that $f^*(\tau) = \prod_g E^{(p^n)}_g(\tau)^{e_g}$. For a cusp $\alpha^k/p^{n+1} \in C_n$, we choose a matrix $\sigma = \left(\begin{smallmatrix} \alpha^k & b \\ p^{n+1} & d \end{smallmatrix}\right)$ in $\Gamma_0(p^{n+1})$. Then we have

$$E^{(p^n)}_g(p\sigma\tau) = E^{(p^n)}_g\left(\begin{pmatrix} \alpha^k & pb \\ p^n & d \end{pmatrix}(p\tau)\right).$$

Using Lemma 7, we find

$$E^{(p^n)}_g(p\sigma\tau) = \epsilon E^{(p^n)}_{\alpha^k g}(p\tau)$$

for some root of unity ϵ, and consequently the order of $E^{(p^n)}_g(p\tau)$ at α^k/p^{n+1} is given by

$$p \cdot \frac{p^n}{2} B_2\left(\frac{\alpha^k g}{p^n}\right),$$

which is the same as p times the order of $E^{(p^n)}_g(\tau)$ at α^k/p^n. From this, we conclude that $\operatorname{div} f = \iota_n(\operatorname{div} f^*)$. This proves the lemma. □

The proof of the converse statement is more difficult. It relies on the next two lemmas.

LEMMA 13. *Let $N \geqslant 4$ be a prime power, let $m = \phi(N)/2$ and let a_i, with $1 \leqslant i \leqslant m$, be the integers in the range $1 \leqslant a_i \leqslant N/2$ such that $(a_i, N) = 1$. Let M be the $m \times m$ matrix which has an (i,j)th entry that is $NB_2(a_i a_j^{-1}/N)/2$, where a_j^{-1} denotes the multiplicative inverse of a_j mod N. Then we have*

$$\det M = \prod_\chi \frac{1}{4} B_{2,\chi} \neq 0,$$

where χ runs over all even characters modulo N.

Proof. The proof of

$$\det M = \prod_{\chi} \frac{1}{4} B_{2,\chi}$$

can be found in [**17**, Lemma 7], and will not be repeated here. To see why the determinant is non-zero, by a straightforward computation we observe that

$$B_{2,\chi_0} = \frac{1}{6}(1-p) \neq 0, \tag{11}$$

where χ_0 is the principal character. Also, Theorem E in particular implies that

$$\prod_{\chi \neq \chi_0 \text{ even}} B_{2,\chi} \neq 0.$$

Therefore, we conclude that $\det M \neq 0$. □

LEMMA 14. *Assume that $p^{n+1} \geqslant 5$. Assume that $f(\tau) = \prod_g E_g^{(p^{n+1})}(\tau)^{e_g}$ is a modular unit in $\mathscr{F}_n$, where $g \in (\mathbb{Z}/p^{n+1}\mathbb{Z})^\times / \pm 1$. Suppose that, for each integer k, the orders of $f(\tau)$ at $\alpha^{k+h\phi_{n-1}}/p^{n+1}$ take the same values for all $h = 0, \ldots, p-1$. Then we have $e_g = 0$ for all g satisfying $p \nmid g$.*

Proof. By Lemma 8, if $p \mid g$, then the orders of E_g at $\alpha^{k+h\phi_{n-1}}/p^{n+1}$, with $h = 0, \ldots, p-1$, are all $p^{n+1}B_2(\alpha^k(g/p)/p^n)/2$. Therefore, if $f(\tau) = \prod_g E_g^{(p^{n+1})}(\tau)^{e_g}$ has the same order at $\alpha^{k+h\phi_{n-1}}/p^{n+1}$ for all $h = 0, \ldots, p-1$ for any fixed k, then the partial product $\prod_{p\nmid g} E_g^{e_g}$ also has the same property. Now given k, let us assume that the order of $\prod_{p\nmid g} E_g^{e_g}$ at $\alpha^{k+h\phi_{n-1}}/p^{n+1}$ is A. Then, by Lemma 8, we have

$$pA = \sum_{h=0}^{p-1} \sum_{p\nmid g, g\leqslant p^{n+1}/2} e_g \frac{p^{n+1}}{2} B_2\left(\frac{g\alpha^{k+h\phi_{n-1}}}{p^{n+1}}\right).$$

Then, by (3) in Lemma 6, we have

$$pA = \sum_{p\nmid g} e_g \frac{p^n}{2} B_2\left(\frac{g\alpha^k}{p^n}\right) = \sum_{g\leqslant p^n/2, p\nmid g} \frac{p^n}{2} B_2\left(\frac{g\alpha^k}{p^n}\right) \sum_{h=0}^{p-1} e_{g+hp^n}.$$

Now since $f(\tau)$ is assumed to be in $\mathscr{F}_n$, by Theorem B, we have $\sum_{h=0}^{p-1} e_{g+hp^n} = 0$ for all g. Therefore, we have $A = 0$. This is true for all α^k/p^{n+1}. In other words, we have

$$\sum_{g\leqslant p^{n+1}/2, p\nmid g} e_g B_2\left(\frac{g\alpha^k}{p^{n+1}}\right) = 0$$

for all non-negative integers k. Now write $g = \alpha^j$ and consider the square matrix which has an (j,k)-entry that is $B_2(\alpha^{j+k-2}/p^{n+1})$. By Lemma 13, the determinant of this matrix is non-zero. Therefore, all e_g, $p \nmid g$, are equal to 0. This completes the proof. □

With the above lemmas, we are now ready to prove the converse to Lemma 12.

LEMMA 15. *Assume that p is a prime and $n \geqslant 1$ is an integer such that $p^n \geqslant 5$. Let D be a divisor in $\mathscr{D}_{n-1}$. If $\iota_n(D) \in \mathscr{D}_n$ is principal, then D is a principal divisor in $\mathscr{D}_{n-1}$.*

Proof. Let

$$D = \sum_{k=0}^{\phi_{n-1}-1} n_k P_{n-1,k} \in \mathscr{D}_{n-1}.$$

Assume that $\iota_n(D)$ is principal; that is, assume that there exists a function $f(\tau) = \prod_g E_g^{(p^{n+1})}(\tau)^{e_g} \in \mathscr{F}_n$ such that

$$\operatorname{div} f = p \sum_{k=0}^{\phi_{n-1}-1} \sum_{h=0}^{p-1} n_k P_{n,k+h\phi_{n-1}}.$$

In other words, we have

$$\frac{p^{n+1}}{2} \sum_g e_g B_2\left(\frac{g\alpha^{k+h\phi_{n-1}}}{p^{n+1}}\right) = pn_k$$

for all h for a given k. Since $\iota_n(D)$ has the same order at $\alpha^{k+h\phi_{n-1}}/p^{n+1}$ for all $h = 0, \dots, p-1$ for a fixed k, we have $e_g = 0$ whenever $p \nmid g$ by Lemma 14. Thus, we have

$$\frac{p^n}{2} \sum_{p|g} e_g B_2\left(\frac{(g/p)\alpha^k}{p^n}\right) = n_k,$$

which in turn implies that the function

$$f^*(\tau) = \prod_{p|g} E_{g/p}^{(p^n)}(\tau)^{e_g}$$

satisfies $\operatorname{div} f^* = D$. It remains to show that f^* is a modular unit contained in $\mathscr{F}_{n-1}$, that is, that f^* satisfies conditions (7) and (8) of Theorem B.

Since $f \in \mathscr{F}_n$, by Theorem B, the exponents e_g satisfy

$$\sum_{g \equiv \pm ap \bmod p^n} e_g = 0$$

for all a. The same exponents e_g then satisfy

$$\sum_{g:\ g/p \equiv \pm a \bmod p^{n-1}} e_g = 0,$$

which is condition (8) for the level $N = p^n$. It remains to consider condition (7).

Observe that $\iota_n(D)$ is a multiple of p, whence we have

$$p \left| \sum_{p|g} e_g \frac{p^{n+1}}{2} B_2\left(\frac{g\alpha^k}{p^{n+1}}\right) \right. \tag{12}$$

for all k. We first consider the cases $p \geqslant 3$. Setting $k = 0$ in (12), we have

$$\sum_{p|g} e_g (g^2 - gp^{n+1}) \equiv 0 \mod p^{n+2},$$

or equivalently

$$\sum_{p|g} e_g (g/p)^2 \equiv 0 \mod p^n.$$

In other words, f^* satisfies the quadratic condition (7) of Theorem B. This settles the cases $p \geqslant 3$.

For $p = 2$, we see that equation (12) with $k = 0$ yields

$$\sum_{2|g} e_g (g^2 - 2^{n+1} g) \equiv 0 \mod 2^{n+3},$$

that is,

$$\sum_{2|g} e_g \left((g/2)^2 - 2^n(g/2)\right) \equiv 0 \bmod 2^{n+1}.$$

Partition the sum $\sum_g e_g(g/2)$ into two parts $\sum_{g\equiv 0 \bmod 4}$ and $\sum_{g\equiv 2 \bmod 4}$. For the terms with $4|g$, we clearly have

$$\sum_{g\equiv 0 \bmod 4} e_g(g/2) \equiv 0 \bmod 2.$$

For the terms with $g \equiv 2 \bmod 4$, we have

$$\sum_{g\equiv 2 \bmod 4} e_g(g/2) \equiv \sum_{g\equiv 2 \bmod 4} e_g \bmod 2.$$

Since e_g satisfy condition (8) for $N = 2^{n+1}$, we must have

$$\sum_{g\equiv 2 \bmod 4} e_g = 0.$$

Therefore, we have

$$\sum_{2|g} e_g(g/2) \equiv 0 \bmod 2.$$

It follows that

$$\sum_{2|g} e_g(g/2)^2 \equiv \sum_{2|g} e_g \left((g/2)^2 - 2^n(g/2)\right) \equiv 0 \bmod 2^{n+1},$$

which is (7) for $N = 2^n$. This proves the case $p = 2$, and the proof of the lemma is complete. □

From Lemmas 12 and 15, we immediately get the following corollary.

COROLLARY 16. *The homomorphism ι_n induces an embedding $\iota_n^* : \mathscr{C}_{n-1} \to \mathscr{C}_n$ given by $\iota_n^*([D]) = [\iota_n(D)]$.*

5. *Proof of Propositions*

5.1. *Proof of Proposition* 1

LEMMA 17. *Let $p \geqslant 3$ be an odd prime. Let ω be a generator of the group of Dirichlet characters modulo p. Then we have the congruence*

$$p \prod_{i=1}^{(p-1)/2-1} B_{2,\omega^{2i}} \equiv \begin{cases} -\displaystyle\prod_{i=1}^{(p-1)/2-2} \frac{B_{2i+2}}{i+1} \bmod p & \text{if } p \geqslant 5, \\ -1 \bmod 3 & \text{if } p = 3, \end{cases}$$

where $B_{2,\omega^{2i}}$ are the generalized Bernoulli numbers and B_{2i+2} are Bernoulli numbers.

Proof. The case $p = 3$ can be verified directly. We now assume that $p \geqslant 5$.

Since the product is a rational number, we may regard ω as the Teichmüller character $\omega : \mathbb{Z}_p^\times \to \mu_{p-1}$ from $\mathbb{Z}_p^\times$ to the group of $(p-1)$st roots of unity in $\mathbb{Z}_p$ characterized by $\omega(a) \equiv a$

mod p for all $a \in \mathbb{Z}_p^\times$. For $2i \neq p-3$ it is well known that $B_{2,\omega^{2i}}$ is contained in $\mathbb{Z}_p$ and satisfies

$$B_{2,\omega^{2i}} \equiv \frac{B_{2i+2}}{i+1} \bmod p.$$

(For a proof, follow the argument in [**15**, Corollary 5.15].) Also, for $2i = p-3$, we have

$$pB_{2,\omega^{p-3}} = \sum_{a=1}^{p-1} \omega^{-2}(a)(a^2 - pa + p^2/6) \equiv \sum_{a=1}^{p-1} \omega^{-2}(a)a^2 \equiv \sum_{a=1}^{p-1} 1 \equiv -1 \bmod p.$$

Then the lemma follows. □

Proof of Proposition 1. The cases $p = 2$ and $p = 3$ can be easily seen from the fact that the modular curves $X_1(8)$ and $X_1(9)$ have genus zero. Now assume that $p \geqslant 5$. By Theorem E, the order of the divisor group $\mathscr{C}_0$ is given by

$$|\mathscr{C}_0| = p \prod_{i=1}^{(p-3)/2} \frac{1}{4} B_{2,\omega^{2i}}.$$

Using Lemma 17, we obtain

$$|\mathscr{C}_0| \equiv -\frac{1}{4^{(p-3)/2}} \prod_{i=1}^{(p-5)/2} \frac{B_{2i+2}}{i+1} \bmod p.$$

By the assumption that p is a regular prime, none of $B_4, \dots, B_{p-3}$ is divisible by p. Therefore, p does not divide $|\mathscr{C}_0|$. □

5.2. *Proof of Proposition* 2

Among the five propositions, this proposition is perhaps the most complicated to prove.

Recall that, given a free $\mathbb{Z}$-module Λ of finite rank r with basis $\{a_1, \dots, a_r\}$ and a submodule Λ' generated by $b_1, \dots, b_s$ with $b_i = \sum r_{ij} a_j$, the standard method to determine the group structure of Λ/Λ' is to compute the Smith normal form of the matrix (r_{ij}). Then the p-rank of the group Λ/Λ' is simply the number of diagonals in the Smith normal form that are divisible by p. Thus, in order to prove Proposition 2, we need to know very precisely the linear dependence over $\mathbb{F}_p$ among the divisors of modular units generating $\mathscr{F}_n$. In the first two lemmas, we will show that the divisors of the first $\phi_n - \phi_{n-1}$ functions in the basis for $\mathscr{F}_n$ are linearly independent over $\mathbb{F}_p$.

Lemma 18. *Let p be a prime and let $n \geqslant 1$ be an integer such that $p^{n+1} \geqslant 5$. Let α be a generator of $(\mathbb{Z}/p^{n+1}\mathbb{Z})^\times / \pm 1$. Let f_i, with $i = 1, \dots, \phi_n - 1$, be the basis for $\mathscr{F}_n$ given in Theorem C or Theorem D. Let $M = (m_{ij})$ be the square matrix of size $\phi_n - \phi_{n-1}$ such that m_{ij} is the order of f_i at the cusp α^{j-1}/p^{n+1}. Then we have*

$$\det M = \epsilon p \prod_{\chi \text{ even primitive}} \frac{1}{4} B_{2,\chi},$$

where χ runs over all even primitive Dirichlet characters modulo p^{n+1} and ϵ is either 1 or -1.

Proof. Let $A = (a_{ij})$ be the $\phi_n \times \phi_n$ matrix with $a_{ij} = p^{n+1}B_2(\alpha^{i+j-2}/p^{n+1})/2$, which is the order of $E_{\alpha^{i-1}}$ at $P_{n,j-1} = \alpha^{j-1}/p^{n+1}$. Define

$$V_1 = \begin{pmatrix} I & -I & 0 & \cdots & \cdots & \cdots \\ 0 & I & -I & \cdots & \cdots & \cdots \\ \vdots & \vdots & & & \vdots & \vdots \\ \cdots & \cdots & \cdots & I & -I & 0 \\ \cdots & \cdots & \cdots & 0 & I & -I \\ I & I & \cdots & \cdots & I & I \end{pmatrix},$$

where the matrix consists of p^2 blocks, each of which is of size $\phi_{n-1} \times \phi_{n-1}$, and I is the identity matrix of dimension ϕ_{n-1}. Let β be an integer such that $\alpha\beta \equiv 1 \bmod p$. Set also

$$V_2 = \begin{pmatrix} 1 & -\beta^2 & 0 & \cdots & \cdots & \cdots \\ 0 & 1 & -\beta^2 & \cdots & \cdots & \cdots \\ \vdots & \vdots & & & \vdots & \vdots \\ \cdots & \cdots & \cdots & 1 & -\beta^2 & 0 \\ \cdots & \cdots & \cdots & 0 & p & 0 \\ 0 & 0 & \cdots & \cdots & 0 & I \end{pmatrix},$$

where the identity matrix at the lower right corner has dimension ϕ_{n-1}. Then, for $i = 1, \ldots, \phi_n - \phi_{n-1}$, the (i,j)-entry of the matrix V_2V_1A is the order of f_i at $P_{n,j-1}$, while for $i = \phi_n - \phi_{n-1} + 1, \ldots, \phi_n$, the (i,j)-entry of V_2V_1A is

$$\frac{p^{n+1}}{2} \sum_{h=0}^{p-1} B_2\left(\frac{\alpha^{i+j+h\phi_{n-1}-2}}{p^{n+1}}\right).$$

By equation (3) in Lemma 6, this is equal to

$$\frac{p^n}{2} B_2\left(\frac{\alpha^{i+j-2}}{p^n}\right). \tag{13}$$

Observe that $B_2(\alpha^{i+j-2}/p^n) = B_2(\alpha^{i+j+k\phi_{n-1}-2}/p^n)$ for all integers k; that is, V_2V_1A takes the form

$$V_2V_1A = \begin{pmatrix} \text{order of } f_i \text{ at } \alpha^{j-1}/p^{n+1} \\ \text{for } i = 1, \ldots, \phi_n - \phi_{n-1} \\ A' & A' & \cdots & \cdots & A' & A' \end{pmatrix},$$

where A' is a square matrix of size ϕ_{n-1} which has an (i,j)-entry that is given by (13).

Now let

$$U_1 = \begin{pmatrix} I & 0 & \cdots & \cdots & 0 & I \\ 0 & I & \cdots & \cdots & 0 & I \\ \vdots & \vdots & & & \vdots & \vdots \\ \vdots & \vdots & & & \vdots & \vdots \\ 0 & 0 & \cdots & \cdots & I & I \\ 0 & 0 & \cdots & \cdots & 0 & I \end{pmatrix},$$

and consider $V_2V_1AU_1$. For $i = 1, \ldots, \phi_n - \phi_{n-1}$ and $j = \phi_n - \phi_{n-1} + 1, \ldots, \phi_n$, the (i,j)-entry of $V_2V_1AU_1$ is given by

$$\sum_{h=0}^{p-1} (\text{order of } f_i \text{ at } P_{n,j+h\phi_{n-1}-1}).$$

By Lemma 11, this sum is equal to 0. In other words,

$$V_2V_1AU_1=\begin{pmatrix} & & & & 0\\ & & & & 0\\ & M & & & \vdots\\ & & & & 0\\ & & & & 0\\ A' & \cdots & \cdots & \cdots & A' & pA' \end{pmatrix},$$

where M is the $(\phi_n-\phi_{n-1})\times(\phi_n-\phi_{n-1})$ matrix specified in the lemma. This shows that

$$\det(V_2V_1AU_1)=p^{\phi_{n-1}}(\det M)(\det A').$$

On the other hand, by Lemma 13, we have

$$\det A=\pm\prod_{\chi \bmod p^{n+1}}\frac{1}{4}B_{2,\chi},\quad \det A'=\pm\prod_{\chi \bmod p^{n}}\frac{1}{4}B_{2,\chi}.$$

Also,

$$\det V_1=p^{\phi_{n-1}},\quad \det V_2=p,\quad \det U_1=1.$$

Combining everything, we conclude that

$$\det M=\pm p\prod_{\chi \bmod p^{n+1}}\frac{1}{4}B_{2,\chi}\Bigg/\prod_{\chi \bmod p^{n}}\frac{1}{4}B_{2,\chi}=\pm p\prod_{\chi \text{ even primitive mod } p^{n+1}}\frac{1}{4}B_{2,\chi},$$

as claimed in the lemma. □

Here we give an example to exemplify the above argument.

EXAMPLE. Consider the case $p=3$ and $n=2$. We choose $\alpha=2$ and $\beta=-1$. With the notation as above, we have

$$A=\frac{1}{108}\begin{pmatrix} 191 & 143 & 59 & -61 & -109 & 23 & -97 & -37 & -121\\ 143 & 59 & -61 & -109 & 23 & -97 & -37 & -121 & 191\\ 59 & -61 & -109 & 23 & -97 & -37 & -121 & 191 & 143\\ -61 & -109 & 23 & -97 & -37 & -121 & 191 & 143 & 59\\ -109 & 23 & -97 & -37 & -121 & 191 & 143 & 59 & -61\\ 23 & -97 & -37 & -121 & 191 & 143 & 59 & -61 & -109\\ -97 & -37 & -121 & 191 & 143 & 59 & -61 & -109 & 23\\ -37 & -121 & 191 & 143 & 59 & -61 & -109 & 23 & -97\\ -121 & 191 & 143 & 59 & -61 & -109 & 23 & -97 & -37 \end{pmatrix},$$

where the (i,j)-entry is $27B_2(2^{i+j-2}/27)/2$,

$$V_2=\begin{pmatrix} 1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 1 & -1 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 1 & -1 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 1 & -1 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 1 & -1 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 3 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix},\quad V_1=\begin{pmatrix} 1 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0\\ 0 & 1 & 0 & 0 & -1 & 0 & 0 & 0 & 0\\ 0 & 0 & 1 & 0 & 0 & -1 & 0 & 0 & 0\\ 0 & 0 & 0 & 1 & 0 & 0 & -1 & 0 & 0\\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & -1 & 0\\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & -1\\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0\\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0\\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

Then

$$V_2V_1A = \begin{pmatrix} 0 & 2 & 0 & 1 & -2 & 4 & -1 & 0 & -4 \\ 2 & 0 & 1 & -2 & 4 & -1 & 0 & -4 & 0 \\ 0 & 1 & -2 & 4 & -1 & 0 & -4 & 0 & 2 \\ 1 & -2 & 4 & -1 & 0 & -4 & 0 & 2 & 0 \\ -2 & 4 & -1 & 0 & -4 & 0 & 2 & 0 & 1 \\ 4 & -8 & -5 & -5 & 7 & 7 & 1 & 1 & -2 \\ a & b & c & a & b & c & a & b & c \\ b & c & a & b & c & a & b & c & a \\ c & a & b & c & a & b & c & a & b \end{pmatrix}, \quad \begin{aligned} a &= 11/36 = 9B_2(1/9)/2, \\ b &= -1/36 = 9B_2(2/9)/2, \\ c &= -13/36 = 9B_2(4/9)/2. \end{aligned}$$

Here the first six rows are the orders of

$$\frac{E_1E_{11}}{E_2E_8}, \quad \frac{E_2E_5}{E_4E_{11}}, \quad \frac{E_4E_{10}}{E_8E_5}, \quad \frac{E_8E_7}{E_{11}E_{10}}, \quad \frac{E_{11}E_{13}}{E_5E_7}, \quad \frac{E_5^3}{E_{13}^3}$$

at the cusps $2^{j-1}/27$. Then the matrices U_1 and $V_2V_1AU_1$ are

$$U_1 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}, \quad V_2V_1AU_1 = \begin{pmatrix} 0 & 2 & 0 & 1 & -2 & 4 & 0 & 0 & 0 \\ 2 & 0 & 1 & -2 & 4 & -1 & 0 & 0 & 0 \\ 0 & 1 & -2 & 4 & -1 & 0 & 0 & 0 & 0 \\ 1 & -2 & 4 & -1 & 0 & -4 & 0 & 0 & 0 \\ -2 & 4 & -1 & 0 & -4 & 0 & 0 & 0 & 0 \\ 4 & -8 & -5 & -5 & 7 & 7 & 0 & 0 & 0 \\ a & b & c & a & b & c & 3a & 3b & 3c \\ b & c & a & b & c & a & 3b & 3c & 3a \\ c & a & b & c & a & b & 3c & 3a & 3b \end{pmatrix}.$$

We find

$$\det M = \det \begin{pmatrix} 0 & 2 & 0 & 1 & -2 & 4 \\ 2 & 0 & 1 & -2 & 4 & -1 \\ 0 & 1 & -2 & 4 & -1 & 0 \\ 1 & -2 & 4 & -1 & 0 & -4 \\ -2 & 4 & -1 & 0 & -4 & 0 \\ 4 & -8 & -5 & -5 & 7 & 7 \end{pmatrix} = -5833 = -3 \prod_{\chi \text{even primitive mod} 27} \frac{1}{4} B_{2,\chi}.$$

LEMMA 19. *Let p be a regular prime and let $n \geqslant 1$ be an integer. Then we have*

$$p \prod_{\chi \text{ even primitive}} \frac{1}{4} B_{2,\chi} \equiv 1 \bmod p,$$

where the product runs over all even primitive Dirichlet characters modulo p^{n+1}.

Proof. First of all, for any non-trivial even Dirichlet character χ we have

$$\sum_{a=1}^{p^{n+1}} \chi(a) = 0$$

and

$$\sum_{a=1}^{p^{n+1}} a\chi(a) = \frac{1}{2} \sum_{a=1}^{p^{n+1}} \big(a\chi(a) + (p^{n+1} - a)\chi(p^{n+1} - a)\big) = \frac{p^{n+1}}{2} \sum_{a=1}^{p^{n+1}} \chi(a) = 0.$$

Thus, we have

$$B_{2,\chi} = p^{n+1} \sum_{a=1}^{p^{n+1}} \left(\frac{a^2}{p^{2n+2}} - \frac{a}{p^{n+1}} + \frac{1}{6} \right) \chi(a) = \frac{1}{p^{n+1}} \sum_{a=1}^{p^{n+1}} \chi(a) a^2. \tag{14}$$

Now we consider that the case p is an odd regular prime first.

Fix a generator α of the multiplicative group $(\mathbb{Z}/p^{n+1}\mathbb{Z})^\times$. For a non-negative integer m, write $r(m) = \lfloor \alpha^m / p^{n+1} \rfloor$ and $s(m) = \alpha^m / p^{n+1} - r(m)$. We have

$$p^{n+1} s(m)^2 = \frac{\alpha^{2m}}{p^{n+1}} - 2\alpha^m r(m) + p^{n+1} r(m)^2$$

Therefore, if a is the integer in the range $0 < a < p^{n+1}$ such that $\alpha^m \equiv a \bmod p^{n+1}$, then

$$\frac{a^2}{p^{n+1}} - \frac{\alpha^{2m}}{p^{n+1}} = -2\alpha^m r(m) + p^{n+1} r(m)^2 \tag{15}$$

is an integer. Denote this integer by $\delta(m)$. Then, by (14), we may write

$$\begin{aligned} B_{2,\chi} &= \frac{1}{p^{n+1}} \sum_{a=1}^{p^{n+1}} \chi(a) a^2 \\ &= \frac{1}{p^{n+1}} \sum_{m=0}^{p^n(p-1)-1} \chi(\alpha^m) \alpha^{2m} + \sum_{m=0}^{p^n(p-1)-1} \chi(\alpha^m) \delta(m) \\ &= \frac{1 - \alpha^{2p^n(p-1)}}{p^{n+1}(1 - \chi(\alpha)\alpha^2)} + \sum_{m=0}^{p^n(p-1)-1} \chi(\alpha^m) \delta(m). \end{aligned} \tag{16}$$

Note that the number $(1 - \alpha^{2p^n(p-1)})/p^{n+1}$ is an integer. Therefore, $(1 - \chi(\alpha)\alpha^2) B_{2,\chi}$ is an algebraic integer.

Let ω and θ denote the Dirichlet characters satisfying

$$\omega(\alpha) = \zeta_{p-1}, \qquad \theta(\alpha) = \zeta_{p^n},$$

respectively, where $\zeta_m = e^{2\pi i/m}$. Set $\chi_{ij} = \omega^{2i}\theta^j$. Then the set of even primitive Dirichlet characters modulo p^{n+1} is precisely

$$\{\chi_{ij} = \omega^{2i}\theta^j : \ 0 \leqslant i < (p-1)/2, \ 0 \leqslant j < p^n, \ p \nmid j\}.$$

From (16), for all j not divisible by p, we have

$$\begin{aligned} &(1 - \omega^{2i}(\alpha)\alpha^2) B_{2,\omega^{2i}} - (1 - \chi_{ij}(\alpha)\alpha^2) B_{2,\chi_{ij}} \\ &\quad = (1 - \omega^{2i}(\alpha)\alpha^2) \sum_{m=0}^{p^n(p-1)-1} \omega^{2i}(\alpha^m)\delta(m) - (1 - \chi_{ij}(\alpha)\alpha^2) \sum_{m=0}^{p^n(p-1)-1} \chi_{ij}(\alpha^m)\delta(m) \\ &\quad = (1 - \omega^{2i}(\alpha)\alpha^2) \sum_{m=0}^{p^n(p-1)-1} \omega^{2i}(\alpha^m)\delta(m)(1 - \theta^j(\alpha^m)) \\ &\qquad - \omega^{2i}(\alpha)\alpha^2(1 - \theta^j(\alpha)) \sum_{m=0}^{p^n(p-1)-1} \chi_{ij}(\alpha^m)\delta(m) \\ &\quad \equiv 0 \mod 1 - \zeta_{p^n}. \end{aligned}$$

(Note that when $i = 0$, we find that $\omega^0 = \chi_0$ is principal, and (14) does not hold in this case. However, the difference is p^n times a p-unit, and the above congruence still holds.) In other

words,

$$\prod_{j=1,\, p\nmid j}^{p^n} (1-\chi_{ij}(\alpha)\alpha^2)B_{2,\chi_{ij}} \equiv \big((1-\omega^{2i}(\alpha)\alpha^2)B_{2,\omega^{2i}}\big)^{p^{n-1}(p-1)} \bmod 1-\zeta_{p^n}.$$

It follows that

$$\begin{aligned}\prod_{\chi \text{ even primitive}} (1-\chi(\alpha)\alpha^2)B_{2,\chi} &= \prod_{i=0}^{(p-1)/2-1} \prod_{j=1,\, p\nmid j}^{p^n} (1-\chi_{ij}(\alpha)\alpha^2)B_{2,\chi_{ij}} \\ &\equiv \left(\prod_{i=0}^{(p-1)/2-1} (1-\omega^{2i}(\alpha)\alpha^2)B_{2,\omega^{2i}}\right)^{p^{n-1}(p-1)} \bmod 1-\zeta_{p^n}.\end{aligned}$$

Now consider the product in the last expression. We have

$$\prod_{i=0}^{(p-1)/2-1} (1-\omega^{2i}(\alpha)\alpha^2) = 1-\alpha^{p-1}.$$

Since α is a generator for $(\mathbb{Z}/p^{n+1}\mathbb{Z})^\times$, we have $1-\alpha^{p-1}=pu$ for some integer u relatively prime to p. Also, according to (11) and Lemma 17, we have

$$p\prod_{i=0}^{(p-1)/2-1} B_{2,\omega^{2i}} \equiv \begin{cases} -\dfrac{1}{6}\displaystyle\prod_{i=1}^{(p-1)/2-2} \frac{B_{2i+2}}{i+1} \bmod p & \text{if } p\geqslant 5, \\ -1 & \text{if } p=3. \end{cases}$$

By the assumption that p is a regular prime, this product is relatively prime to p. Therefore, we have

$$\left(\prod_{i=0}^{(p-1)/2-1} (1-\omega^{2i}(\alpha)\alpha^2)B_{2,\omega^{2i}}\right)^{p-1} \equiv 1 \bmod p,$$

and consequently

$$\prod_{\chi \text{ even primitive}} (1-\chi(\alpha)\alpha^2)B_{2,\chi} \equiv 1 \bmod 1-\zeta_{p^n}.$$

Since the product is a rational integer, the congruence actually holds modulo p. Finally, because α is a generator of $(\mathbb{Z}/p^{n+1}\mathbb{Z})^\times$, there exists an integer u relatively prime to p such that $\alpha^{p^k(p-1)} \equiv 1-up^{k+1} \bmod p^{k+2}$ for all $k\geqslant 0$. Thus,

$$\prod_{\chi \text{ even primitive}} (1-\chi(\alpha)\alpha^2) = \frac{1-\alpha^{p^n(p-1)}}{1-\alpha^{p^{n-1}(p-1)}} = \frac{up^{n+1}+\cdots}{up^n+\cdots} \equiv p \bmod p^2. \tag{17}$$

From this we conclude that

$$p\prod_{\chi \text{ even primitive}} \frac{1}{4}B_{2,\chi} \equiv 1 \bmod p.$$

This completes the proof of the case where p is an odd regular prime.

Now consider the case $p=2$ with $n\geqslant 2$. Choose $\alpha=3$ to be a generator of $(\mathbb{Z}/2^{n+1}\mathbb{Z})^\times/\pm 1$. Set $\zeta=e^{2\pi i/2^{n-1}}$, and let θ be the Dirichlet character satisfying $\theta(-1)=1$ and $\theta(3)=\zeta$. Then the set of even primitive Dirichlet characters modulo 2^{n+1} is given by

$$\{\theta^j :\ 1\leqslant j\leqslant 2^{n-1},\ 2\nmid j\}.$$

Since θ is even, we have

$$\frac{1}{4}B_{2,\theta^j} = \frac{2^{n+1}}{2} \sum_{a\in(\mathbb{Z}/2^{n+1}\mathbb{Z})^\times/\pm 1} \theta^j(a) B_2\left(\frac{a}{2^{n+1}}\right).$$

By a similar calculation as before, we find that if θ^j is not principal, then

$$\frac{1}{4}B_{2,\theta^j} = \frac{1}{2^{n+2}} \sum_{a\in(\mathbb{Z}/2^{n+1}\mathbb{Z})^\times/\pm 1} \theta^j(a) a^2.$$

Now for a non-negative integer m, define

$$\delta(m) = -\frac{3^{2m}}{2^{n+1}} + 2^{n+1}\left\{\frac{3^m}{2^{n+1}}\right\}^2$$

as in (15). Following the computation in (16), we get

$$\frac{1}{4}B_{2,\theta^j} = \frac{1-3^{2^n}}{2^{n+2}(1-9\zeta^j)} + \frac{1}{2}\sum_{m=0}^{\phi(2^{n+1})/2-1} \theta^j(3^m)\delta(m).$$

Now we have $3^{2^n} = (1+8)^{2^{n-1}} \equiv 1 + 2^{n+2} \bmod 2^{n+3}$. Also, from (15), we see that $\delta(m)$ is always even. Thus, $(1-9\zeta^j)B_{2,\theta^j}/4$ is an algebraic integer. By the same argument as before, we find

$$\frac{1-9}{4}B_{2,\chi_0} - \frac{1-9\zeta^j}{4}B_{2,\theta^j} \equiv 0 \bmod 1-\zeta,$$

for all odd j, and thus

$$\prod_{\chi \text{ even primitive}} \frac{1-9\chi(3)}{4}B_{2,\chi} \equiv 1 \bmod 2.$$

Finally, from (17), we have

$$\prod_{\chi \text{ even primitive}} (1-9\chi(3)) \equiv 2 \bmod 4.$$

This proves the case $p = 2$. □

Proof of Proposition 2. Let α be a generator of $(\mathbb{Z}/p^{n+1}\mathbb{Z})^\times/\pm 1$. Specifically, for $p = 2$, we set $\alpha = 3$ and, for an odd prime p, we let α be an integer such that α generates $(\mathbb{Z}/p\mathbb{Z})^\times$, but $\alpha^{p-1} \not\equiv 1 \bmod p^2$. Let f_i, with $i = 1, \dots, \phi_n - 1$, be the generators of $\mathscr{F}_n$ given in Theorem C or Theorem D. Let M be the $(\phi_n - 1) \times \phi_n$ matrix which has an (i,j)-entry that is the order of f_i at α^{j-1}/p^{n+1}. Let U and V be the unimodular matrices such that $M' = UMV$ is in the Smith normal form; that is, if $M' = (m_{ij})$, then we have the following:

(1) $m_{11}|m_{22}|\dots$;
(2) $m_{ij} = 0$ if $i \neq j$.

Also ($m_{ii} \neq 0$ for all i since the rank of M is $\phi_n - 1$.) Then the p-rank of $\mathscr{C}_n$ is equal to the number of m_{ii} that are divisible by p. In other words, if we consider M as a matrix over $\mathbb{F}_p$, then our p-rank is actually equal to

$$\phi_n - 1 - (\text{the rank of } M \text{ over } \mathbb{F}_p).$$

We now determine the rank of M over $\mathbb{F}_p$.

From Lemmas 18 and 19, we know that the first $\phi_n - \phi_{n-1}$ rows of M are linearly independent over $\mathbb{F}_p$. Thus, the rank of M over $\mathbb{F}_p$ is at least $\phi_n - \phi_{n-1} = p^{n-1}(p-1)^2/2$. It remains to prove that the remaining rows are all linearly dependent of the first $\phi_n - \phi_{n-1}$ rows modulo p.

We first consider row $\phi_n - \phi_{n-1} + 1$ to row $\phi_n - \phi_0$. (For $p = 2$, consider row $\phi_n - \phi_{n-1} + 1$ to row $\phi_n - \phi_2$.) Let ℓ be an integer between 1 and $n-1$. (For $p = 2$, let $1 \leqslant \ell \leqslant n-3$.) By Theorems C and D, for i from $\phi_n - \phi_{n-\ell} + 1$ to $\phi_n - \phi_{n-\ell-1}$, the ith row of M is the divisor of the function

$$f_i = E^{(p^{n-\ell+1})}_{\alpha^{i-1}}(p^\ell\tau)/E^{(p^{n-\ell+1})}_{\alpha^{i+\phi_{n-\ell-1}-1}}(p^\ell\tau),$$

which by Lemma 8 is given by

$$p^\ell \cdot \frac{p^{n-\ell+1}}{2} \sum_{k=0}^{\phi_n-1} \left(B_2\left(\frac{\alpha^{i+k-1}}{p^{n-\ell+1}}\right) - B_2\left(\frac{\alpha^{i+\phi_{n-\ell-1}+k-1}}{p^{n-\ell+1}}\right)\right) P_{n,k}. \tag{18}$$

Now $\alpha^{\phi_{n-\ell-1}} \equiv -(1 + up^{n-\ell}) \bmod p^{n-\ell+1}$ for some integer u not divisible by p. (For $p = 2$, we have $\alpha^{\phi_{n-\ell-1}} \equiv 1 + 2^{n-\ell} \bmod 2^{n-\ell+1}$ instead when $n - \ell \geqslant 3$.) Then a straightforward calculation gives

$$\frac{p^{n-\ell+1}}{2}\left(B_2\left(\frac{\alpha^{i+k-1}}{p^{n-\ell+1}}\right) - B_2\left(\frac{\alpha^{i+\phi_{n-\ell-1}+k-1}}{p^{n-\ell+1}}\right)\right) \equiv -\frac{u\alpha^{2(i+k-1)}}{p} \bmod 1.$$

This shows that if $\ell \geqslant 2$, then the divisor of f_i for i from $\phi_n - \phi_{n-\ell} + 1$ to $\phi_n - \phi_{n-\ell-1}$ is divisible by p. For such ℓ, the rows do not contribute anything to the rank of M over $\mathbb{F}_p$.

When $\ell = 1$, the above computation shows that the ith row of M for i from $\phi_n - \phi_{n-1} + 1$ to $\phi_n - \phi_{n-2}$ is congruent to

$$-u\alpha^{2(i-1)}(1, \alpha^2, \alpha^4, \ldots, \alpha^{2\phi_n-2}) \bmod p.$$

On the other hand, the $(\phi_n - \phi_{n-1})$th row of M is the divisor of

$$E^p_{\alpha^{\phi_n-\phi_{n-1}-1}}/E^p_{\alpha^{\phi_n-1}}.$$

By a similar computation, we find that it is congruent to

$$-u\alpha^{2(\phi_n-\phi_{n-1}-1)}(1, \alpha^2, \alpha^4, \ldots, \alpha^{2\phi_n-2}).$$

From this we see that row $\phi_n - \phi_{n-1} + 1$ to row $\phi_n - \phi_0$ of M are all multiples of the $(\phi_n - \phi_{n-1})$th row of M mod p.

Finally, for $i = \phi_n - \phi_0 + 1, \ldots, \phi_n - 1$, we find that the ith row is congruent to the 0 vector. Therefore, the rank of M over $\mathbb{F}_p$ is precisely $\phi_n - \phi_{n-1}$. We conclude that the p-rank of $\mathscr{C}_n$ is given by

$$\phi_n - 1 - (\phi_n - \phi_{n-1}) = \phi_{n-1} - 1 = p^{n-1}(p-1)/2 - 1.$$

This completes the proof of the proposition. □

5.3. *Proof of Proposition* 3

Let f_i, with $i = 1, \ldots, \phi_n - 1$, denote the basis for $\mathscr{F}_n$ given in Theorem C or Theorem D and let f'_i, with $i = 1, \ldots, \phi_{n-1} - 1$, be the basis for $\mathscr{F}_{n-1}$. By Lemma 11, we have

$$\pi_n(\operatorname{div} f_i) = 0$$

for $i = 1, \ldots, \phi_n - \phi_{n-1}$, and

$$\begin{pmatrix} \operatorname{div} f'_1 \\ \vdots \\ \operatorname{div} f'_{\phi_{n-1}-1} \end{pmatrix} = \frac{1}{p^2}\begin{pmatrix} R & 0 \\ 0 & I \end{pmatrix}\begin{pmatrix} \pi_n(\operatorname{div} f_{\phi_n-\phi_{n-1}+1}) \\ \vdots \\ \pi_n(\operatorname{div} f_{\phi_n-1}) \end{pmatrix}, \tag{19}$$

where I is the identity matrix of size $\phi_{n-2}-1$ and

$$R=\begin{pmatrix} 1 & -\beta^2 & 0 & \cdots & \cdots & \cdots \\ 0 & 1 & -\beta^2 & \cdots & \cdots & \cdots \\ \vdots & & & & & \vdots \\ \cdots & \cdots & \cdots & 1 & -\beta^2 & 0 \\ \cdots & \cdots & \cdots & 0 & 1 & -\beta^2 \\ \cdots & \cdots & \cdots & 0 & 0 & p \end{pmatrix}$$

is a square matrix of size $\phi_{n-1}-\phi_{n-2}$ which has superdiagonals that are all $-\beta^2$ and which has diagonals that are all 1, except for the last one, which is p. Therefore, the index of $\pi_n(\mathscr{P}_n)$ in $\mathscr{P}_{n-1}$ is given by

$$p^{2(\phi_{n-1}-1)-1}=p^{p^{n-1}(p-1)-3}.$$

The structure of the factor group $\mathscr{P}_{n-1}/\pi_n(\mathscr{P}_n)$ can be easily seen from the matrix above. This completes the proof of the proposition.

5.4. *Proof of Proposition* 4

Consider the group homomorphism

$$\pi:\ \mathscr{D}_n\to\pi_n(\mathscr{D}_n)/\pi_n(\mathscr{P}_n)=\mathscr{D}_{n-1}/\pi_n(\mathscr{P}_n)$$

sending $D\in\mathscr{D}_n$ to the coset $\pi_n(D)+\pi_n(\mathscr{P}_n)$. The homomorphism is clearly onto, and the kernel is the group $\ker\pi=\mathscr{P}_n+\ker\pi_n$. Thus, we have

$$\mathscr{D}_n/(\mathscr{P}_n+\ker\pi_n)\simeq\mathscr{D}_{n-1}/\pi_n(\mathscr{P}_n).$$

Now the group on the left-hand side is isomorphic to

$$\mathscr{D}_n/(\mathscr{P}_n+\ker\pi_n)\simeq(\mathscr{D}_n/\mathscr{P}_n)\big/((\mathscr{P}_n+\ker\pi_n)/\mathscr{P}_n).$$

Therefore, to prove that the p-part of $\mathscr{C}_n=\mathscr{D}_n/\mathscr{P}_n$ is isomorphic to that of $\mathscr{D}_{n-1}/\pi_n(\mathscr{P}_n)$, it suffices to show that the order of $(\mathscr{P}_n+\ker\pi_n)/\mathscr{P}_n$ is not divisible by p.

From the definition of π_n, it is easy to see that the kernel of π_n is generated by divisors of the form

$$D=P_{n,k}-P_{n,k+\phi_{n-1}}.$$

Let f_i, with $i=1,\dots,\phi_n-1$, be the basis for $\mathscr{F}_n$ given in Theorem C or Theorem D. If we write D as a linear combination

$$D=\sum_{i=1}^{\phi_n-1}r_i\operatorname{div}f_i,\quad r_i\in\mathbb{Q},$$

of $\operatorname{div}f_i$, then the order of $D+\mathscr{P}_n$ in the divisor class group $\mathscr{C}_n$ divides the least common multiple of the denominators of r_i. We need to show that this number is not divisible by p.

We first prove that $r_i=0$ for $i=\phi_n-\phi_{n-1}+1,\dots,\phi_n-1$. By Lemma 11, we have

$$0=\pi_n(D)=\sum_{i=\phi_n-\phi_{n-1}+1}^{\phi_n-1}r_i\pi_n(\operatorname{div}f_i).\tag{20}$$

Let $A=\left(\begin{smallmatrix}R&0\\0&I\end{smallmatrix}\right)$ be the square matrix of size $\phi_{n-1}-1$ in (19). Then we have

$$\begin{pmatrix}\pi_n(\operatorname{div}f_{\phi_n-\phi_{n-1}+1})\\ \vdots\\ \pi_n(\operatorname{div}f_{\phi_n-1})\end{pmatrix}=p^2A^{-1}\begin{pmatrix}\operatorname{div}f_1'\\ \vdots\\ \operatorname{div}f_{\phi_{n-1}-1}'\end{pmatrix},$$

where f'_i, with $i = 1, \ldots, \phi_{n-1} - 1$, is the basis for $\mathscr{F}_{n-1}$ given in Theorem C or Theorem D, and (20) can be written as

$$0 = p^2(r_{\phi_n-\phi_{n-1}+1}, \ldots, r_{\phi_n-1})A^{-1} \begin{pmatrix} \operatorname{div} f'_1 \\ \vdots \\ \operatorname{div} f'_{\phi_{n-1}-1} \end{pmatrix}.$$

Since $\operatorname{div} f'_i$ are linearly independent over $\mathbb{Q}$, we must have

$$(r_{\phi_n-\phi_{n-1}+1}, \ldots, r_{\phi_n-1})A^{-1} = (0, \ldots, 0).$$

It follows that $r_i = 0$ for all $i = \phi_n - \phi_{n-1} + 1, \ldots, \phi_n - 1$, and

$$D = \sum_{i=1}^{\phi_n-\phi_{n-1}} r_i \operatorname{div} f_i.$$

Now, without loss of generality, we may assume that the integer k in $D = P_{n,k} - P_{n,k+\phi_{n-1}}$ satisfies $0 < k < \phi_n - 2\phi_{n-1}$. (Let b and d be integers such that $\alpha d - bp^{n+1} = 1$. Note that if a modular unit $f(\tau) \in \mathscr{F}_n$ has a divisor mD for some integer m, then the function $f((\alpha\tau + b)/(p^{n+1}\tau + d))$ has a divisor $m(P_{n,k-1} - P_{n,k+\phi_{n-1}-1})$. Thus $P_{n,k} - P_{n,k+\phi_{n-1}}$ and $P_{n,k-1} - P_{n,k+\phi_{n-1}-1}$ have the same order in the divisor class group $\mathscr{C}_n$.) Let M be the square matrix of size $\phi_n - \phi_{n-1}$ which has an (i, j)-entry that is the order of f_i at $P_{n,j-1}$. Then the order of D in the divisor class group $\mathscr{C}_n$ will divide the determinant of the matrix M. By Lemmas 18 and 19 and the assumption that p is a regular prime, the determinant of M is not divisible by p. This shows that the order of $D + \mathscr{P}_n$ in $\mathscr{C}_n$ is not divisible by p, and therefore $|(\mathscr{P}_n + \ker \pi_n)/\mathscr{P}_n|$ is not divisible by p. This proves the proposition.

5.5. *Proof of Proposition* 5

By Proposition 3, we see that $\mathscr{P}_{n-1}/\pi_n(\mathscr{P}_n)$ is clearly contained in $\ker[p^2]$. Now suppose that $D + \pi_n(\mathscr{P}_n) \in \mathscr{D}_{n-1}/\pi_n(\mathscr{P}_n)$ is in the kernel of $[p^2]$. We have $p^2 D \in \pi_n(\mathscr{P}_n)$. With (10), this can be written as $\pi_n(\iota_n(D)) \in \pi_n(\mathscr{P}_n)$, or equivalently

$$\iota_n(D) \in \mathscr{P}_n + \ker \pi_n.$$

Let f_i, with $i = 1, \ldots, \phi_n - 1$, be the basis for $\mathscr{F}_n$ given in Theorem C or Theorem D. By Lemma 11, we have $\operatorname{div} f_i \in \ker \pi_n$ for $i = 1, \ldots, \phi_n - \phi_{n-1}$. Hence,

$$\iota_n(D) = \sum_{i=\phi_n-\phi_{n-1}+1}^{\phi_n-1} m_i \operatorname{div} f_i + D'$$

for some integers m_i and some divisor D' in $\ker \pi_n$. Now note that if we define an inner product $\langle \cdot, \cdot \rangle$ on $\mathscr{D}_n$ by

$$\langle c_0 P_{n,0} + c_1 P_{n,1} + \ldots, d_0 P_{n,0} + d_1 P_{n,1} + \ldots \rangle = c_0 d_0 + c_1 d_1 + \ldots,$$

then, for $i = \phi_n - \phi_{n-1} + 1, \ldots, \phi_n - 1$, $\operatorname{div} f_i$ is in the orthogonal complement of $\ker \pi_n$. The same thing is also true for $\iota_n(D)$ for any $D \in \mathscr{D}_{n-1}$. It follows that the divisor D' above is actually 0 and we have $\iota_n(D) \in \mathscr{P}_n$. Finally, by Lemma 15, the fact that $\iota_n(D)$ is principal implies that D itself is principal. This completes the proof of the proposition.

Acknowledgements. The authors would like to thank Professor Jing Yu for his interest in this work. The authors are also very thankful to the referee for a thorough and careful reading of the manuscript. Part of the work was done while the first author was visiting the Max-Planck-Institut für Mathematik at Bonn. He would like to thank the institute for providing a stimulating research environment.

References

1. B. Conrad, B. Edixhoven and W. Stein, '$J_1(p)$ has connected fibers', *Doc. Math.* 8 (2003) 331–408 (electronic).
2. P. E. Klimek, 'Modular functions on $\Gamma_1(N)$', PhD Thesis, University of California, Berkeley, 1975.
3. D. S. Kubert and S. Lang, 'Units in the modular function field. I', *Math. Ann.* 218 (1975) 67–96.
4. D. S. Kubert and S. Lang, 'Units in the modular function field. II. A full set of units', *Math. Ann.* 218 (1975) 175–189.
5. D. S. Kubert and S. Lang, 'Units in the modular function field. III. Distribution relations', *Math. Ann.* 218 (1975) 273–285.
6. D. S. Kubert and S. Lang, 'Units in the modular function field. IV. The Siegel functions are generators', *Math. Ann.* 227 (1977) 223–242.
7. D. S. Kubert and S. Lang, 'The index of Stickelberger ideals of order 2 and cuspidal class numbers', *Math. Ann.* 237 (1978) 213–232.
8. D. S. Kubert and S. Lang, *Modular units*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Science] 244 (Springer, New York, 1981).
9. Ju. I. Manin, 'Parabolic points and zeta functions of modular curves', *Izv. Akad. Nauk SSSR Ser. Mat.* 36 (1972) 19–66.
10. B. Mazur, 'Modular curves and the Eisenstein ideal', *Publ. Math. Inst. Hautes Études Sci.* 47 (1978) 33–186.
11. G. Shimura, *Introduction to the arithmetic theory of automorphic functions*, Publications of the Mathematical Society of Japan 11 (Princeton University Press, Princeton, NJ, 1994) Reprint of the 1971 original, Kano Memorial Lecture 1.
12. G. Stevens, *Arithmetic on modular curves*, Progress in Mathematics 20 (Birkhäuser, Boston, MA, 1982).
13. H.-S. Sun, 'Cuspidal class number of a tower of modular curves $X_1(Np^n)$', *Math. Ann.*, to appear. DOI: 10.1007/s00208-010-0505-7.
14. L. C. Washington, 'The non-p-part of the class number in a cyclotomic $\mathbf{Z}_p$-extension', *Invent. Math.* 49 (1978) 87–97.
15. L. C. Washington, *Introduction to cyclotomic fields*, 2nd edn, Graduate Texts in Mathematics 83 (Springer, New York, 1997).
16. Y. Yang, 'Transformation formulas for generalized Dedekind eta functions', *Bull. London Math. Soc.* 36 (2004) 671–682.
17. Y. Yang, 'Modular units and cuspidal divisor class groups of $X_1(N)$', *J. Algebra* 322 (2009) 514–553.
18. J. Yu, 'A cuspidal class number formula for the modular curves $X_1(N)$' *Math. Ann.* 252 (1980) 197–216.

Yifan Yang
Department of Applied Mathematics
National Chiao Tung University
Hsinchu 300
Taiwan
ROC

yfyang@math.nctu.edu.tw

Jeng-Daw Yu
Department of Mathematics
National Taiwan University
Taipei
Taiwan
ROC

jdyu@math.ntu.edu.tw