ISRAEL JOURNAL OF MATHEMATICS 99 (1997), 29–54

ON THE Q-RATIONAL CUSPIDAL SUBGROUP AND THE COMPONENT GROUP OF $J_0(p^r)$

BY

SAN LING

Department of Mathematics, National University of Singapore, Singapore 119260
e-mail: matlings@nus.sg

ABSTRACT

For $p \geq 3$ a prime, we compute the $\mathbf{Q}$-rational cuspidal subgroup $C(p^r)$ of the Jacobian $J_0(p^r)$ of the modular curve $X_0(p^r)$. This result is then applied to determine the component group Φ_{p^r} of the Néron model of $J_0(p^r)$ over $\mathbf{Z}_p$. This extends results of Lorenzini [7]. We also study the action of the Atkin–Lehner involution on the p-primary part of $C(p^r)$, as well as the effect of degeneracy maps on the component groups.

1. Introduction

Let p be a prime number, and for any positive integer r, let $X_0(p^r)$ denote the classical modular curve over $\mathbf{Q}$. Let $J_0(p^r)$ denote the Jacobian variety of $X_0(p^r)$, also defined over $\mathbf{Q}$.

Let $C(p^r)$ denote the $\mathbf{Q}$-rational cuspidal subgroup of $J_0(p^r)$. This is the subgroup of $\mathbf{Q}$-rational points of $J_0(p^r)$ generated by the divisor classes of divisors of degree 0 on $X_0(p^r)$, whose components are cusps. Manin [8] has shown that the classes of all such cuspidal divisors are of finite order, so $C(p^r)$ is a finite abelian group. When $r = 1$, the group $C(p)$ was computed by Ogg [10]. For any prime p, $C(p)$ is cyclic of order $\frac{p-1}{(p-1,12)}$.

For $p \geq 5$, let a and b be defined as

$$a \stackrel{\text{def}}{=} \frac{p-1}{(p-1,12)} \qquad \text{and} \qquad b \stackrel{\text{def}}{=} \frac{p+1}{(p+1,12)}.$$

Received June 1, 1995 and in revised form August 19, 1995

Then $(a,b)=1$ and $ab=\frac{p^2-1}{24}$.

For arbitrary r, but with the constraint $p \not\equiv 11 \bmod 12$, Lorenzini [7] showed that the prime-to-$2p$ part $C(p^r)^{(2p)}$ of $C(p^r)$ is isomorphic to the prime-to-2 part of $(\mathbf{Z}/a\mathbf{Z})^r \times (\mathbf{Z}/b\mathbf{Z})^{r-1}$.

In this article, we compute $C(p^r)$ *entirely* for *all* primes $p \geq 3$, using a rather elementary method of relating cuspidal divisors with modular functions.

For a finite abelian group G and an integer n, let G_n denote the n-primary part of G and let $G^{(n)}$ denote the prime-to-n part of G, so that $G = G_n \oplus G^{(n)}$.

We also let $w = w_{p^r}$ denote the Atkin–Lehner involution on $J_0(p^r)$ (see subsection 3.2 for definition). Let $C(p^r)_p^+$ be the image of $(w+1)$: $C(p^r)_p \to C(p^r)_p$, and let $C(p^r)_p^-$ be the image of $(w-1)$: $C(p^r)_p \to C(p^r)_p$. We prove in this article:

THEOREM 1: *Let $p \geq 5$ be a prime and let $r \geq 1$ be a positive integer.*

(i) *The groups $C(p^r)_p^+$ and $C(p^r)_p^-$ are given as follows:*

- $C(p)_p^+ = C(p^2)_p^+ = C(p)_p^- = C(p^2)_p^- \simeq 0$,
- $C(p^3)_p^+ = 0, C(p^3)_p^- \simeq \mathbf{Z}/p^2\mathbf{Z}$,
- *if $r \geq 4$, r even,*

$$\begin{aligned} C(p^r)_p^+ &\simeq \mathbf{Z}/p^{\frac{r}{2}}\mathbf{Z} \times \mathbf{Z}/p^{\frac{r}{2}+1}\mathbf{Z} \times \cdots \times \mathbf{Z}/p^{r-3}\mathbf{Z} \times \mathbf{Z}/p^{r-2}\mathbf{Z} \\ &= \prod_{i=\frac{r}{2}}^{r-2} \mathbf{Z}/p^i\mathbf{Z}, \\ C(p^r)_p^- &\simeq \mathbf{Z}/p^{\frac{r}{2}+1}\mathbf{Z} \times \mathbf{Z}/p^{\frac{r}{2}+2}\mathbf{Z} \times \cdots \times \mathbf{Z}/p^{r-2}\mathbf{Z} \times \mathbf{Z}/p^{r-1}\mathbf{Z} \\ &= \prod_{i=\frac{r}{2}+1}^{r-1} \mathbf{Z}/p^i\mathbf{Z}, \end{aligned}$$

- *if $r \geq 4$, r odd,*

$$\begin{aligned} C(p^r)_p^+ &\simeq \mathbf{Z}/p^{\frac{r+1}{2}}\mathbf{Z} \times \mathbf{Z}/p^{\frac{r+3}{2}}\mathbf{Z} \times \cdots \times \mathbf{Z}/p^{r-3}\mathbf{Z} \times \mathbf{Z}/p^{r-2}\mathbf{Z} \\ &= \prod_{i=\frac{r+1}{2}}^{r-2} \mathbf{Z}/p^i\mathbf{Z}, \\ C(p^r)_p^- &\simeq \mathbf{Z}/p^{\frac{r+1}{2}}\mathbf{Z} \times \mathbf{Z}/p^{\frac{r+3}{2}}\mathbf{Z} \times \cdots \times \mathbf{Z}/p^{r-2}\mathbf{Z} \times \mathbf{Z}/p^{r-1}\mathbf{Z} \\ &= \prod_{i=\frac{r+1}{2}}^{r-1} \mathbf{Z}/p^i\mathbf{Z}. \end{aligned}$$

(ii) *The* $\mathbf{Q}$*-rational cuspidal subgroup* $C(p^r)$ *of* $J_0(p^r)$ *is given by:*

$$\begin{aligned} C(p^r)^{(p)} &\simeq (\mathbf{Z}/a\mathbf{Z})^r \times (\mathbf{Z}/b\mathbf{Z})^{r-1}, \\ C(p^r)_p &= C(p^r)_p^+ \times C(p^r)_p^-. \end{aligned}$$

After some preliminary discussion in Section 2, we prove Theorem 1(ii) in Section 3. The proof of Theorem 1(i) follows in Section 4. The proof for the case $p = 3$ is similar, so we leave it to the reader. We simply state the results here.

THEOREM 2: *The* $\mathbf{Q}$*-rational cuspidal subgroup* $C(3^r)$ *of* $J_0(3^r)$ *is given by:*

- $C(3) = C(3^2) = 0$,
- $C(3^3) \simeq \mathbf{Z}/3\mathbf{Z}$,
- *if* $r \geq 4$, r *even,*

$$\begin{aligned} C(3^r) \simeq & \mathbf{Z}/3^{\frac{r}{2}-1}\mathbf{Z} \times \mathbf{Z}/3^{\frac{r}{2}}\mathbf{Z} \times \mathbf{Z}/3^{\frac{r}{2}}\mathbf{Z} \times \cdots \\ & \times \mathbf{Z}/3^{r-3}\mathbf{Z} \times \mathbf{Z}/3^{r-3}\mathbf{Z} \times \mathbf{Z}/3^{r-2}\mathbf{Z} \\ = & \prod_{i=\frac{r}{2}-1}^{r-3} \mathbf{Z}/3^i\mathbf{Z} \times \prod_{i=\frac{r}{2}}^{r-2} \mathbf{Z}/3^i\mathbf{Z}, \end{aligned}$$

- *if* $r \geq 4$, r *odd,*

$$\begin{aligned} C(3^r) &\simeq \mathbf{Z}/3^{\frac{r-1}{2}}\mathbf{Z} \times \mathbf{Z}/3^{\frac{r-1}{2}}\mathbf{Z} \times \cdots \times \mathbf{Z}/3^{r-3}\mathbf{Z} \times \mathbf{Z}/3^{r-3}\mathbf{Z} \times \mathbf{Z}/3^{r-2}\mathbf{Z} \\ &= \prod_{i=\frac{r-1}{2}}^{r-3} \mathbf{Z}/3^i\mathbf{Z} \times \prod_{i=\frac{r-1}{2}}^{r-2} \mathbf{Z}/3^i\mathbf{Z}. \end{aligned}$$

We have not been able to determine completely $C(2^r)$ $(r \geq 1)$. The reason is that we are not sure if all possible relations governing the generators have been found (cf. subsection 2.2).

Regarding $J_0(p^r)$ as an abelian variety over $\mathbf{Q}_p$, let $\mathcal{J}_0(p^r)$ denote the Néron model of $J_0(p^r)$ over $\mathbf{Z}_p$, let $\mathcal{J}_0(p^r)_s$ denote the special fibre of $\mathcal{J}_0(p^r)$, and let Φ_{p^r} denote the component group of $\mathcal{J}_0(p^r)_s$.

In [7], Lorenzini showed that, for $p \geq 5$ a prime, the reduction map $\pi_r\colon C(p^r)^{(6)} \to \Phi_{p^r}^{(6)}$ is surjective. He also showed that

(i) Φ_{p^r} contains a subgroup isomorphic to $\mathbf{Z}/a\mathbf{Z} \times (\mathbf{Z}/b\mathbf{Z})^{r-1}$;

(ii) when $p \not\equiv 11 \bmod 12$, $\Phi_{p^r}^{(p)} \simeq \mathbf{Z}/a\mathbf{Z} \times (\mathbf{Z}/b\mathbf{Z})^{r-1}$;

(iii) when $p \not\equiv 11 \bmod 12$, $|(\Phi_{p^r})_p| = \begin{cases} p^{2s^2} & \text{if } r = 2s+1, \\ p^{2s(s-1)} & \text{if } r = 2s. \end{cases}$

As Theorem 1 gives a description for $C(p^r)$, we use Theorem 1 and surjectivity of π_r to compute $\Phi_{p^r}^{(6p)}$ for *all* primes $p \geq 5$, and to give an upper bound for $|(\Phi_{p^r})_p|$ when $p \equiv 11 \bmod 12$.

THEOREM 3: *Let $p \geq 5$ be a prime. Then*

(i) *$\Phi_{p^r}^{(6p)}$ is isomorphic to the prime-to-6p part of $(\mathbf{Z}/a\mathbf{Z}) \times (\mathbf{Z}/b\mathbf{Z})^{r-1}$;*

(ii) *if $p \equiv 11 \bmod 12$, $|(\Phi_{p^r})_p| \leq \begin{cases} p^{s(3s-1)} & r = 2s+1, \\ p^{(s-1)(3s-1)} & r = 2s. \end{cases}$*

In particular, $(\Phi_p)_p = (\Phi_{p^2})_p = 0$.

We note that Theorem 3(ii) follows immediately as a corollary of Theorem 1 and the surjectivity of $\pi_r \colon C(p^r)^{(6)} \to \Phi_{p^r}^{(6)}$.

Theorem 1.4 of [7] furnishes us with the group structure of $(\Phi_{p^r})_p^+$ and $(\Phi_{p^r})_p^-$ (defined to be the images of $(w+1)$ and $(w-1)$, respectively, on $(\Phi_{p^r})_p$) when $p \equiv 1 \bmod 12$. If we are able to compute $(\Phi_{p^r})_p$ explicitly for all primes $p \geq 5$, it would be interesting to understand how the kernel of the map $\pi_r \colon C(p^r) \to \Phi_{p^r}$ reduces in the connected component of the Néron model.

Let J_{p^r} denote the torsion subgroup of $J_0(p^r)(\mathbf{Q})$. With Theorem 1 at hand, an argument similar to the one in [7], 4.8 and 4.9 gives a complete description of $J_{p^r}^{(6p)}$ for *all* primes $p \geq 5$ (cf. (1) below).

THEOREM 4: *Let $p \geq 5$ be a prime, and let $\ell \neq 2, 3, p$ be another prime. Then*

$$(J_{p^r})_\ell = C(p^r)_\ell \simeq \ \ell\text{-primary part of } (\mathbf{Z}/a\mathbf{Z})^r \times (\mathbf{Z}/b\mathbf{Z})^{r-1}.$$

If $r = 2$, the statement also holds for $\ell = 3$.

Proof: The proof of this fact is essentially contained in [7], 4.8 and 4.9, so we only give a sketch. Theorem 2.3 of [7] shows that the reduction map $\pi_r \colon C(p^r)_\ell \to (\Phi_{p^r})_\ell$ is surjective for such ℓ.

Given $u \in (J_{p^r})_\ell$, there exists a $c \in C(p^r)_\ell$ such that $\pi_r(u) = \pi_r(c)$. By [7] 4.8, $u \in C(p^r)_\ell$.

When $r = 2$ and $\ell = 3$, the map π_r is also surjective (Lemma 4.2 of [7]). ∎

Theorem 4 may be regarded as a generalisation of [7], Theorem 4.6, which states that for $p \geq 5$, $p \not\equiv 11 \bmod 12$, we have

$$(1) \qquad J_{p^r}^{(2p)} = C(p^r)^{(2p)} \simeq \text{ prime-to-2 part of } (\mathbf{Z}/a\mathbf{Z})^r \times (\mathbf{Z}/b\mathbf{Z})^{r-1}.$$

ACKNOWLEDGEMENT: The author thanks Bas Edixhoven for helpful email messages and Dino Lorenzini for useful suggestions and discussions. He is also grateful to the referee for detailed comments which helped improve the presentation of the paper.

2. Relationship between modular functions and cuspidal divisors

2.1 THE DEDEKIND η-FUNCTIONS AND CUSPIDAL DIVISORS. Let N be a positive integer, and let δ denote a positive divisor of N. Let $\mathbf{r} = (r_\delta)$ be a family of rational numbers $r_\delta \in \mathbf{Q}$ indexed by all the positive divisors δ of N. Let

$$g_{\mathbf{r}} = \prod_{\delta|N} \eta_\delta^{r_\delta} \tag{2}$$

be made up from the Dedekind η-functions, where $\eta_\delta(z) \stackrel{\text{def}}{=} \eta(\delta z)$. As η is a complex function, we regard an nth root $\eta^{1/n}$ of η as a power series in $\exp(2\pi i z)$ with rational coefficients (cf. [11], Section 4). The function $g_{\mathbf{r}}$ in (2) may be regarded as a holomorphic function on the Poincaré upper half-plane.

The following proposition is well-known:

PROPOSITION 1: *The function $g_{\mathbf{r}}$ in (2) is a modular function on the modular curve $X_0(N)$, defined over $\mathbf{Q}$, i.e., $g_{\mathbf{r}} \in \mathbf{Q}(X_0(N))$, if and only if the following conditions are satisfied:*

(0) *all the r_δ are rational integers;*

(1) $\sum_{\delta|N} r_\delta \cdot \delta \equiv 0 \bmod 24$;

(2) $\sum_{\delta|N} r_\delta \cdot \frac{N}{\delta} \equiv 0 \bmod 24$;

(3) $\sum_{\delta|N} r_\delta = 0$;

(4) $\prod_{\delta|N} \delta^{r_\delta}$ *is the square of a rational number.*

Cf. [3], Proposition 3.2.1, p. 32, Remarque, or [4], Proposition 1.

As representatives of the cusps of $X_0(N)$, we use as in [10] the vectors $\binom{x}{d}$, where $d|N$, $d > 0$ and $(x, d) = 1$ with x taken modulo $(d, N/d)$. We say that such a cusp $\binom{x}{d}$ is **of level** d, and it is defined over $\mathbf{Q}(\mu_m)$, where $m = (d, N/d)$ ([10], Section 1). The Galois group $\mathrm{Gal}(\mathbf{Q}(\mu_m)/\mathbf{Q})$ permutes all the cusps of level d. Let (P_d) denote the divisor on $X_0(N)$ defined as the sum of all the cusps of level d (each with multiplicity one). Clearly (P_d) is invariant under $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$.

It is easy to see that the $\mathbf{Q}$-rational cuspidal subgroup $C(N)$ of $J_0(N)$ is generated by divisor classes coming from divisors of the kind

$$\phi((d, N/d))P_1 - (P_d)$$

as d runs through the positive divisors of N. Here ϕ is the Euler totient function.

For divisors δ and d of N, let

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

Let $\mathbf{r} = (r_\delta)$ be a family of integers satisfying the conditions in Proposition 1. Then the divisor of $g_{\mathbf{r}}$ is supported at the cusps, and ([3], Proposition 3.2.8)

$$(g_{\mathbf{r}}) = \sum_{d|N} b_{\mathbf{r}}(d) \cdot (P_d),$$

where

$$b_{\mathbf{r}}(d) = \frac{1}{24} \sum_{\delta|N} a_N(d, \delta) \cdot r_\delta. \tag{3}$$

Note also that

$$\deg((g_{\mathbf{r}})) = \sum_{d|N} b_{\mathbf{r}}(d) \cdot \phi((d, N/d)) = 0.$$

Conversely, if $D = \sum_{d|N} m_d(P_d)$ is a cuspidal divisor of degree 0, then there exists a modular function $g_{\mathbf{r}}$ of the type described in Proposition 1 such that the divisor $(g_{\mathbf{r}})$ is an integral multiple of D (*loc. cit.*, Proposition 3.2.10).

The above discussion and *loc. cit.*, Propositions 3.2.8 and 3.2.10, show that we have a map Λ from the set

$$S_1 = \left\{ \prod_{\delta|N} \eta_\delta^{r_\delta} \;\middle|\; r_\delta \in \mathbf{Q} \text{ and } \sum_{\delta|N} r_\delta = 0 \right\}$$

to the set

$$S_2 = \left\{ \sum_{d|N} m_d(P_d) \;\middle|\; m_d \in \mathbf{Q} \text{ and } \sum_{d|N} m_d \phi((d, N/d)) = 0 \right\}.$$

This map is defined by

$$\Lambda\left(\prod_{\delta|N} \eta_\delta^{r_\delta} \right) = \sum_{d|N} b_{\mathbf{r}}(d) \cdot (P_d), \qquad r_\delta \in \mathbf{Q}, \quad b_{\mathbf{r}}(d) \in \mathbf{Q},$$

with $\sum_{\delta|N} r_\delta = 0$ and $b_{\mathbf{r}}(d)$ as in (3).

PROPOSITION 2: *The map Λ is bijective.*

Proof: Let t denote the number of positive divisors of N, and let $1 = \delta_1 < \delta_2 < \cdots < \delta_t = N$ be all the positive divisors of N. Then S_1 may be identified with

$$\left\{ \begin{pmatrix} r_{\delta_1} \\ \vdots \\ r_{\delta_t} \end{pmatrix} \in \mathbf{Q}^t \colon \sum_{i=1}^{t} r_{\delta_i} = 0 \right\}. \tag{4}$$

Similarly, S_2 has the natural identification with

$$\left\{ \begin{pmatrix} m_{\delta_1} \\ \vdots \\ m_{\delta_t} \end{pmatrix} \in \mathbf{Q}^t \colon \sum_{i=1}^{t} m_{\delta_i} \phi((\delta_i, N/\delta_i)) = 0 \right\}. \tag{5}$$

With these identifications, Λ may be written as a $t \times t$ matrix such that

$$\Lambda_{ij} = \frac{1}{24} a_N(\delta_i, \delta_j).$$

Indeed, given any $\begin{pmatrix} m_{\delta_1} \\ \vdots \\ m_{\delta_t} \end{pmatrix} \in S_2$, there exists an integer e such that $em_{\delta_i} \in \mathbf{Z}$ for all $i = 1, \ldots, t$. Then there exists $g_{\mathbf{r}} = \begin{pmatrix} r_{\delta_1} \\ \vdots \\ r_{\delta_t} \end{pmatrix} \in S_1$ of the type described in Proposition 1 such that

$$\Lambda \begin{pmatrix} r_{\delta_1} \\ \vdots \\ r_{\delta_t} \end{pmatrix} = ke \begin{pmatrix} m_{\delta_1} \\ \vdots \\ m_{\delta_t} \end{pmatrix}, \quad \text{for some } k \in \mathbf{Z}.$$

Therefore,

$$\Lambda \begin{pmatrix} r_{\delta_1}/ke \\ \vdots \\ r_{\delta_t}/ke \end{pmatrix} = \begin{pmatrix} m_{\delta_1} \\ \vdots \\ m_{\delta_t} \end{pmatrix}.$$

This shows that Λ is surjective. Injectivity of Λ follows since S_1 and S_2 are $\mathbf{Q}$-vector spaces of the same dimension. ∎

2.2 THE GENERAL STRATEGY. For a general level N and a divisor δ_i of N (notation as in above subsection), let

$$C_{i-1} = \phi((\delta_i, N/\delta_i))P_1 - (P_{\delta_i}).$$

Then it is clear that the divisor classes $\overline{C}_i$ $(1 \leq i \leq t-1)$ generate $C(N)$.

To compute $C(N)$, we first find the order of each $\overline{C}_i$. To do this, we first compute $\Lambda^{-1}C_i \in S_1$, then find the smallest positive integer k such that the entries of $k\Lambda^{-1}C_i$ satisfy all the conditions of Proposition 1. This k is then the order of $\overline{C}_i$ (cf. [11], Section 4).

Next we establish relations among the generators $\overline{C}_i$ of $C(N)$. We note that a relation $\sum \lambda_i \overline{C}_i = 0$ exists if and only if $\Lambda^{-1}(\sum \lambda_i C_i)$ satisfies the conditions of Proposition 1. In principle, relations can be established for any given N. However, in general, it can be difficult to determine whether all the possible relations have been found. This is precisely the problem that hindered us from determining $C(2^r)$ completely. In this paper, we find all the possible relations among the generators of $C(N)$ for all $N = p^r$, where $p \geq 5$ is a prime.

Having found all the generators of $C(N)$ and all the possible relations among the generators, the group $C(N)$ is practically found.

2.3 THE CASE $N = p^r$. We specialise now to the case $N = p^r$, where p is a prime. Then we may write $\delta_i = p^{i-1}$, $1 \leq i \leq r+1$, and $\delta_j = p^{j-1}$, $1 \leq j \leq r+1$. Consequently,

$$\begin{aligned}\Lambda_{ij} &= \frac{1}{24} a_N(p^{i-1}, p^{j-1}) \\ &= \frac{1}{24} \frac{p^r}{(p^{i-1}, p^{r-i+1})} \frac{(p^{i-1}, p^{j-1})^2}{p^{i+j-2}} \\ &= \frac{1}{24} \frac{1}{(p^{2(i-1)}, p^r)} (p^{i-1}, p^{j-1})^2 p^{r-j+1}.\end{aligned}$$

LEMMA 1: *Let $M = (m_{ij})$ be the $(r+1) \times (r+1)$ matrix with $m_{ij} = (p^{i-1}, p^{j-1})^2$. Then we have*

$$M = BCD,$$

where $b_{ij} = \begin{cases} 1 & \text{if } j \leq i, \\ 0 & \text{otherwise,} \end{cases}$ $c_{ij} = \begin{cases} 1 & \text{if } i = j = 1, \\ p^{2(i-1)} - p^{2(i-2)} & \text{if } i = j \geq 2, \\ 0 & \text{otherwise,} \end{cases}$ *and*

$d_{ij} = \begin{cases} 1 & \text{if } j \geq i, \\ 0 & \text{otherwise.} \end{cases}$

The verification of the lemma is straight-forward, so we leave it to the reader.

Now let $A = (a_{ij})$ be the matrix

$$a_{ij} = \begin{cases} \frac{1}{(p^{2(i-1)}, p^r)} & \text{if } i = j, \\ 0 & \text{otherwise,} \end{cases}$$

and let $E = (e_{ij})$ be the matrix

$$e_{ij} = \begin{cases} p^{r-i+1} & \text{if } i = j, \\ 0 & \text{otherwise.} \end{cases}$$

Then we have

$$\Lambda = \frac{1}{24} ABCDE.$$

Consequently,

$$\Lambda^{-1} = 24 E^{-1} D^{-1} C^{-1} B^{-1} A^{-1}.$$

Writing $A^{-1} = (a'_{ij})$, $B^{-1} = (b'_{ij})$ etc., we have

$$a'_{ij} = \begin{cases} (p^{2(i-1)}, p^r) & \text{if } i = j, \\ 0 & \text{otherwise,} \end{cases} \qquad b'_{ij} = \begin{cases} 1 & \text{if } i = j, \\ -1 & \text{if } i = j+1, \\ 0 & \text{otherwise,} \end{cases}$$

$$c'_{ij} = \begin{cases} 1 & \text{if } i = j = 1, \\ \frac{1}{p^{2(i-1)} - p^{2(i-2)}} & \text{if } i = j \geq 2, \\ 0 & \text{otherwise,} \end{cases} \qquad d'_{ij} = \begin{cases} 1 & \text{if } i = j, \\ -1 & \text{if } j = i+1, \\ 0 & \text{otherwise,} \end{cases}$$

$$e'_{ij} = \begin{cases} p^{i-1-r} & \text{if } i = j, \\ 0 & \text{otherwise.} \end{cases}$$

PROPOSITION 3: *The matrix $\Lambda^{-1} = (\lambda'_{ij})$ is given by*

$$\lambda'_{ij} = \frac{24}{p^r(p^2-1)} (p^{j-1}, p^{r+1-j}) \cdot \kappa_{ij},$$

where

$$\kappa_{ij} = \begin{cases} p^2 & \text{if } i = j = 1 \text{ or } r+1, \\ p^2+1 & \text{if } 2 \leq i = j \leq r, \\ -p & \text{if } |i-j| = 1, \\ 0 & \text{if } |i-j| \geq 2. \end{cases}$$

From our discussion in subsection 2.1, it follows that a rational cuspidal divisor P of degree 0 (with coefficients in $\mathbf{Z}$) actually comes from a modular function on $X_0(p^r)$ precisely when the entries of $\Lambda^{-1}P$ (with P identified with a column vector through (5)) satisfy the conditions of Proposition 1. For this reason, the order of the class of a rational cuspidal divisor P is the smallest positive integer k such that the entries of $k(\Lambda^{-1}P)$ satisfy the conditions of Proposition 1.

3. Proof of Theorem 1(ii)

3.1 THE CASE $r = 2$. From this section, we assume further that $p \geq 5$.

When $r = 2$, the matrix Λ^{-1} is

$$\Lambda^{-1} = \frac{24}{p^2(p^2-1)} \begin{pmatrix} p^2 & -p^2 & 0 \\ -p & p(p^2+1) & -p \\ 0 & -p^2 & p^2 \end{pmatrix} = \frac{24}{p(p^2-1)} \begin{pmatrix} p & -p & 0 \\ -1 & p^2+1 & -1 \\ 0 & -p & p \end{pmatrix}.$$

The $\mathbf{Q}$-rational cuspidal subgroup $C(p^2)$ is clearly generated by divisor classes of the following divisors:

$$C_1 \stackrel{\text{def}}{=} (p-1)P_1 - (P_p),$$
$$C_2 \stackrel{\text{def}}{=} P_1 - P_{p^2}.$$

To completely describe the group structure of $C(p^2)$, it suffices to determine the orders of the divisor classes $\overline{C}_1$ and $\overline{C}_2$ of C_1 and C_2, and find all the relations between them.

To determine the orders of $\overline{C}_1$ and $\overline{C}_2$, we first compute

$$\Lambda^{-1}C_1 = \frac{24}{p(p^2-1)} \begin{pmatrix} p & -p & 0 \\ -1 & p^2+1 & -1 \\ 0 & -p & p \end{pmatrix} \begin{pmatrix} p-1 \\ -1 \\ 0 \end{pmatrix} = \frac{24}{p^2-1} \begin{pmatrix} p \\ -(p+1) \\ 1 \end{pmatrix}, \tag{6}$$

and

$$\Lambda^{-1}C_2 = \frac{24}{p(p^2-1)} \begin{pmatrix} p & -p & 0 \\ -1 & p^2+1 & -1 \\ 0 & -p & p \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix} = \frac{24}{p^2-1} \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix}. \tag{7}$$

Using the criteria in Proposition 1, it is easy to see that the smallest power of $\Lambda^{-1}C_1$ that is a modular function on $X_0(p^2)$ is $\left(\Lambda^{-1}C_1\right)^{(p^2-1)/24}$. Therefore the order of $\overline{C}_1$ is $(p^2-1)/24$. Similarly, we can show that the order of $\overline{C}_2$ is also $(p^2-1)/24$.

Let ℓ denote a prime divisor of $(p^2-1)/24 = ab$. We may write $(p^2-1)/24 = \ell^{r_\ell}\tilde{\ell}$, where $\ell \nmid \tilde{\ell}$. For $i = 1, 2$, let $C_{i,\ell} = \tilde{\ell}C_i$. Then $C(p^2)$ is generated by $\overline{C}_{1,\ell}$ and

$\overline{C}_{2,\ell}$, where ℓ runs through all the prime divisors of $(p^2-1)/24$. Furthermore, for each ℓ, $\overline{C}_{i,\ell}$ $(i=1,2)$ has order ℓ^{r_ℓ}.

To determine the relations between the generators $\overline{C}_1$ and $\overline{C}_2$ of $C(p^2)$, it suffices to find the relations (if any) between $\overline{C}_{1,\ell}$ and $\overline{C}_{2,\ell}$, for each prime ℓ. Suppose that $\lambda_\ell \overline{C}_{1,\ell} + \mu_\ell \overline{C}_{2,\ell} = 0$, where λ_ℓ, μ_ℓ are integers such that $0 \le \lambda_\ell, \mu_\ell \le \ell^{r_\ell} - 1$. This is true if and only if $\Lambda^{-1}(\lambda_\ell C_{1,\ell} + \mu_\ell C_{2,\ell})$ is a modular function on $X_0(p^2)$. From (6) and (7), we have

$$\Lambda^{-1}(\lambda_\ell C_{1,\ell} + \mu_\ell C_{2,\ell}) = \frac{1}{\ell^{r_\ell}} \begin{pmatrix} \lambda_\ell p + \mu_\ell \\ -\lambda_\ell(p+1) \\ \lambda_\ell - \mu_\ell \end{pmatrix}. \tag{8}$$

For (8) to represent a modular function on $X_0(p^2)$, the conditions in Proposition 1 need to be satisfied. Let $v_\ell(x)$ denote the valuation of x at ℓ, i.e., $\ell^{v_\ell(x)}$ is the exact power of ℓ dividing x.

Condition (0) of Proposition 1 applied to the exponent of η_{p^2} implies that

$$v_\ell(\lambda_\ell - \mu_\ell) \ge r_\ell, \quad \text{i.e., } \lambda_\ell = \mu_\ell.$$

If $\ell \ne 2$ divides a, then $(\ell, p+1) = 1$, and applying condition (0) to the exponent of η_p yields

$$v_\ell(\lambda_\ell(p+1)) \ge r_\ell, \quad \text{i.e., } \lambda_\ell = 0.$$

If $\ell = 2$ divides a, then ℓ exactly divides $p+1$. Condition (4) implies that

$$v_2(\lambda_\ell(p+1)) \ge r_2 + 1,$$

thus giving

$$v_2(\lambda_\ell) \ge r_2, \quad \text{i.e., } \lambda_\ell = 0.$$

Summarising the above, we conclude that there is no relation between $\overline{C}_{1,\ell}$ and $\overline{C}_{2,\ell}$ if ℓ is a prime divisor of a.

If ℓ divides b, then $v_\ell(p+1) \ge r_\ell$. Applying condition (0) of Proposition 1 to the exponent of η gives

$$v_\ell(\lambda_\ell p + \mu_\ell) \ge r_\ell,$$

which gives

$$v_\ell(-\lambda_\ell + \mu_\ell) \ge r_\ell, \quad \text{i.e., } \lambda_\ell = \mu_\ell.$$

It is easy to see that conditions (1) through (4) are then automatically satisfied. Therefore, when ℓ is a prime divisor of b, we have $\overline{C}_{1,\ell} + \overline{C}_{2,\ell} = 0$.

Considering all the generators and relations in $C(p^2)$, we obtain

$$C(p^2) \simeq (\mathbf{Z}/a\mathbf{Z})^2 \times \mathbf{Z}/b\mathbf{Z}.$$

3.2 THE CASE $r \geq 3$. For $r \geq 3$, let C_i $(1 \leq i \leq r)$ denote the rational cuspidal divisors (of degree 0)

$$C_i \stackrel{\text{def}}{=} \phi((p^i, p^{r-i}))P_1 - (P_{p^i}).$$

Clearly, $C(p^r)$ is generated by the divisor classes $\overline{C}_i$ of C_i, for $1 \leq i \leq r$.

We first determine the orders of the classes $\overline{C}_i$. Taking Λ^{-1} as in Proposition 3, it is easy to verify the following computations:

$$\Lambda^{-1}C_1 = \frac{24}{p^r(p^2-1)} \begin{pmatrix} p^3 \\ -p^2(p+1) \\ p^2 \\ 0 \\ \vdots \\ 0 \end{pmatrix},$$

$$\Lambda^{-1}C_2 = \frac{24}{p^r(p^2-1)} \begin{pmatrix} p^3(p-1) \\ p^2 \\ -p^2(p^2+1) \\ p^3 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \quad (r \geq 4) \quad \text{or}$$

$$\frac{24}{p^3(p^2-1)} \begin{pmatrix} p^2(p-1) \\ p \\ -p(p^2+1) \\ p^2 \end{pmatrix} (r = 3),$$

$$\Lambda^{-1}C_i = \frac{24}{p^r(p^2-1)} \begin{pmatrix} p^{t(i)+1}(p-1) \\ -p^{t(i)}(p-1) \\ 0 \\ \vdots \\ 0 \\ p^{t(i)+1} \\ -p^{t(i)}(p^2+1) \\ p^{t(i)+1} \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \quad 2 < i < r, \quad t(i) = \min(i, r-i),$$

$$\Lambda^{-1}C_r = \frac{24}{p^r(p^2-1)} \begin{pmatrix} p^2 \\ -p \\ 0 \\ \vdots \\ 0 \\ p \\ -p^2 \end{pmatrix}.$$

Using Proposition 1, we may check that

- the order of $\overline{C}_1$ is $p^{r-2}ab$,
- the order of $\overline{C}_2$ is $p^{r-2}ab$ $(r \geq 4)$, or p^2ab $(r = 3)$,
- the order of $\overline{C}_i$ is $p^{r-t(i)}ab$ $(2 < i < r)$,
- the order of $\overline{C}_r$ is $p^{r-1}ab$.

As an example, we compute the order of $\overline{C}_i$ $(2 < i < r)$. Let the order of $\overline{C}_i$ be denoted by d. Then d is the smallest positive integer such that the entries of $d\Lambda^{-1}C_i = \Lambda^{-1}(dC_i)$ satisfy the conditions (0) through (4) of Proposition 1.

Condition (0) shows that

$$\frac{d}{p^{r-t(i)}ab} \in \mathbf{Z}, \quad \text{i.e., } d \in p^{r-t(i)}ab\mathbf{Z}. \tag{9}$$

It is easy to see that, for any $d \in \mathbf{Z}$, conditions (1), (2) and (3) are satisfied.

Condition (4) is equivalent to

$$\begin{aligned} &\frac{d}{p^{r-t(i)}ab}[-(p-1) - i(p^2+1)] \in 2\mathbf{Z} \quad \text{if } r \text{ is odd,} \\ &\frac{d}{p^{r-t(i)}ab}[-(p-1) + 2ip] \in 2\mathbf{Z} \quad \text{if } r \text{ is even.} \end{aligned} \tag{10}$$

Clearly, since $p \geq 5$ is odd, (10) is true whenever (9) is satisfied.

It follows therefore that the order of $\overline{C}_i$ $(2 < i < r)$ is $p^{r-t(i)}ab$.

Next we determine the relations among the generators $\overline{C}_i$ of $C(p^r)$. Mimicking subsection 3.1, for each prime divisor ℓ of $(p^2-1)/24 = ab$, we write $(p^2-1)/24 = \ell^{r_\ell}\tilde{\ell}$ $(\ell \nmid \tilde{\ell})$, and set

$$\begin{aligned} C_{1,\ell} &= p^{r-2}\tilde{\ell}C_1, \\ C_{2,\ell} &= p^{r-2}\tilde{\ell}C_2 \ (r \geq 4), \text{ or } p^2\tilde{\ell}C_2 \ (r = 3), \\ C_{i,\ell} &= p^{r-t(i)}\tilde{\ell}C_i \ (2 < i < r), \\ C_{r,\ell} &= p^{r-1}\tilde{\ell}C_r. \end{aligned}$$

Similarly, we set

$$C_{i,p} = abC_i \quad (1 \leq i \leq r).$$

We will establish the relations among the generators $\overline{C}_i$ of $C(p^r)$ at each prime, and then combine the information thus obtained. First, we determine the relations among the $\overline{C}_{i,p}$ $(1 \leq i \leq r)$.

Let $v_1(p^{h+1}), v_p(p^{h+1})$: $X_0(p^{h+1}) \to X_0(p^h)$ be the two degeneracy maps from $X_0(p^{h+1})$ to $X_0(p^h)$. Recall that the points on $Y_0(p^{h+1})(\mathbf{C})$ are parametrised by isomorphism classes $[E, G]$, where E is an elliptic curve over $\mathbf{C}$ and G is a cyclic subgroup of order p^{h+1}. Then, on $Y_0(p^{h+1})(\mathbf{C})$, we have the following modular interpretation:

$$\begin{aligned} v_1(p^{h+1})([E, G]) &= [E, G_{p^h}], \\ v_p(p^{h+1})([E, G]) &= [E/G_p, G/G_p], \end{aligned}$$

where G_p and G_{p^h} denote the unique subgroups of G of orders p and p^h respectively.

For $0 \leq i \leq h+1$, and x such that $(x, p) = 1$ and x taken modulo (p^i, p^{h+1-i}), we recall that (with $\left(\begin{smallmatrix} x \\ p^i \end{smallmatrix}\right)$ representing the cusps on $X_0(p^{h+1})$)

$$v_1(p^{h+1})\begin{pmatrix} x \\ p^i \end{pmatrix} = \begin{cases} \begin{pmatrix} x \\ p^i \end{pmatrix} & 0 \leq i \leq h/2. \text{ This point is ramified.} \\ \begin{pmatrix} x \bmod p^{h-i} \\ p^i \end{pmatrix} & h/2 < i \leq h \\ \begin{pmatrix} 1 \\ p^h \end{pmatrix} & i = h+1. \end{cases} \tag{11}$$

$$(12)\quad v_p(p^{h+1})\begin{pmatrix} x \\ p^i \end{pmatrix} = \begin{cases} \begin{pmatrix} 0 \\ 1 \end{pmatrix} & i = 0 \\ \begin{pmatrix} x \bmod p^{i-1} \\ p^{i-1} \end{pmatrix} & 1 \le i < \frac{h}{2} + 1 \\ \begin{pmatrix} x \\ p^{i-1} \end{pmatrix} & \frac{h}{2} + 1 \le i \le h+1. \\ & \text{This point is ramified.} \end{cases}$$

The degeneracy maps $v_1, v_p, \ldots, v_{p^{r-h}}\colon X_0(p^r) \to X_0(p^h)$ in the introduction may be described by

$$\begin{aligned} v_1 &= v_1(p^{h+1}) \circ \cdots \circ v_1(p^{r-1}) \circ v_1(p^r), \\ v_{p^i} &= v_1(p^{h+1}) \circ \cdots \circ v_1(p^{r-i}) \circ v_p(p^{r-i+1}) \circ \cdots \circ v_p(p^r), \quad 0 < i < r-h, \\ v_{p^{r-h}} &= v_p(p^{h+1}) \circ \cdots \circ v_p(p^{r-1}) \circ v_p(p^r). \end{aligned}$$

With $h = 2$, the map $v_1\colon X_0(p^r) \to X_0(p^2)$ induces, via Pic functoriality, a map $v_1^*\colon J_0(p^2) \to J_0(p^r)$ on the Jacobian varieties. Using (11) and (12), we can show that

$$v_1^*(\overline{P_1 - P_{p^2}}) = \sum_{i=2}^{[\frac{r}{2}]} p^{r-2i}\overline{C}_i + \sum_{i=[\frac{r}{2}]+1}^{r-2} \overline{C}_i + \overline{C}_{r-1} + \overline{C}_r,$$

where $[x]$ denotes the greatest integer less than or equal to x.

Observing that $ab(\overline{P_1 - P_{p^2}}) = 0$ in $J_0(p^2)$ (subsection 2.1), we obtain

$$(13)\qquad 0 = \sum_{i=2}^{[\frac{r}{2}]} p^{r-2i}\overline{C}_{i,p} + \sum_{i=[\frac{r}{2}]+1}^{r-2} \overline{C}_{i,p} + \overline{C}_{r-1,p} + \overline{C}_{r,p}.$$

This shows that $\overline{C}_{r,p}$ is a $\mathbf{Z}$-linear combination of $\overline{C}_{i,p}$ $(2 \le i \le r-1)$.

Let $w = w_{p^r}$ be the Atkin–Lehner involution on $X_0(p^r)$. Recall that the restriction of w to $Y_0(p^r)(\mathbf{C})$ has the following modular interpretation:

$$w([E, G]) = [E/G, (E[p^r] + G)/G],$$

where E is an elliptic curve over $\mathbf{C}$, G is a cyclic subgroup of E of order p^r, and $E[p^r]$ is the group of p^r-torsion points in E.

We also recall that, if $\binom{x}{p^i}$ is a cusp on $X_0(p^r)$ (where $(x,p) = 1$ and x is taken modulo (p^i, p^{r-i})), then

$$w\begin{pmatrix} x \\ p^i \end{pmatrix} = \begin{pmatrix} -x \\ p^{r-i} \end{pmatrix}.$$

Applying w to (13), we obtain

$$0 = \sum_{i=2}^{[\frac{r}{2}]} \overline{C}_{i,p} + \sum_{i=[\frac{r}{2}]+1}^{r-2} p^{2i-r}\overline{C}_{i,p} + \overline{C}_{1,p} - p^{r-2}\overline{C}_{r,p}.$$

This is shows that $\overline{C}_{1,p}$ is a $\mathbf{Z}$-linear combination of $\overline{C}_{i,p}$ for $2 \leq i \leq r-2$ and $i = r$. Together with the conclusion after (13), we have shown that the p-primary part $C(p^r)_p$ of $C(p^r)$ is generated by $\overline{C}_{i,p}$ $(2 \leq i \leq r-1)$.

If $r = 3$, then $C(p^3)_p$ is generated by $\overline{C}_{2,p}$, hence

$$C(p^3)_p \simeq \mathbf{Z}/p^2\mathbf{Z}. \tag{14}$$

For $r \geq 4$, the generators $\overline{C}_{i,p}$ $(2 \leq i \leq r-1)$ may be subject to some relations.

To find the relations among all the $\overline{C}_{i,p}$ $(2 \leq i \leq r-1)$, we suppose that

$$\lambda_2\overline{C}_{2,p} + \cdots + \lambda_{r-1}\overline{C}_{r-1,p} = 0, \tag{15}$$

where $0 \leq \lambda_2 \leq p^{r-2} - 1$ and $0 \leq \lambda_i \leq p^{r-t(i)} - 1$ $(3 \leq i \leq r-1)$.

Let $\alpha \geq 3$ be the largest integer such that $\lambda_\alpha \neq 0$ in (15).

Considering the $(\alpha+2)$nd row in the vector representing

$$\Lambda^{-1}(\lambda_2 C_{2,p} + \cdots + \lambda_\alpha C_{\alpha,p}),$$

and applying Proposition 1, we see that (15) implies

$$v_p(\lambda_\alpha) \geq r - t(\alpha) - 1.$$

Since the order of $\overline{C}_{\alpha,p}$ is $p^{r-t(\alpha)}$, we have

$$v_p(\lambda_\alpha) = r - t(\alpha) - 1.$$

Considering next the $(\alpha+1)$st row in the same vector, and again using Proposition 1, we get

$$v_p(\lambda_{\alpha-1}p^{t(\alpha-1)+1} - \lambda_\alpha p^{t(\alpha)}(p^2+1)) \geq r.$$

Since $v_p(\lambda_\alpha p^{t(\alpha)}(p^2+1)) = r-1$, it follows that

$$v_p(\lambda_{\alpha-1}p^{t(\alpha-1)+1}) = r-1,$$

which is equivalent to

$$v_p(\lambda_{\alpha-1}) = \begin{cases} 2(\alpha-1) - \alpha - 1 & \text{if } \alpha - 1 \geq \frac{r}{2}, \\ r - \alpha - 1 & \text{if } \alpha - 1 \leq \frac{r}{2}. \end{cases}$$

Continuing this process by next considering the αth row in the vector $\Lambda^{-1}(\lambda_2 C_{2,p} + \cdots + \lambda_\alpha C_{\alpha,p})$, and so on till the 4th row, we may deduce that, for $2 \leq i \leq \alpha$,

$$v_p(\lambda_i) = \begin{cases} 2i - \alpha - 1 & \text{if } i \geq \frac{r}{2}, \\ r - \alpha - 1 & \text{if } i \leq \frac{r}{2}. \end{cases}$$

Now consider the 3rd row of the vector $\Lambda^{-1}(\lambda_2 C_{2,p} + \cdots + \lambda_\alpha C_{\alpha,p})$. The entry is

$$\frac{1}{p^r}[-\lambda_2 p^2(p^2+1) + \lambda_3 p^{t(3)+1}].$$

It is straight-forward to verify that

$$v_p(\lambda_3 p^{t(3)+1}) = r - \alpha + 3,$$

and

$$v_p(\lambda_2 p^2(p^2+1)) = r - \alpha + 1.$$

Therefore,

$$v_p(-\lambda_2 p^2(p^2+1) + \lambda_3 p^{t(3)+1}) < r,$$

which contradicts condition (0) of Proposition 1.

We therefore conclude that $\lambda_2 = \cdots = \lambda_{r-1} = 0$ in (15), which means that the generators $\overline{C}_{i,p}$ $(2 \leq i \leq r-1)$ are independent of one another. Consequently,

$$C(p^r)_p \simeq \mathbf{Z}/p^{r-2}\mathbf{Z} \times \prod_{2<i<r} \mathbf{Z}/p^{r-t(i)}\mathbf{Z}, \qquad \text{for } r \geq 4. \tag{16}$$

Remark. We observe that for $p \neq 2$ a prime, it is clear that

$$C(p^r)_p = C(p^r)_p^+ \times C(p^r)_p^-,$$

with $C(p^r)_p^+$ and $C(p^r)_p^-$ as defined in the introduction. Therefore, the group structure of $C(p^r)_p$ will become evident once the group structures of $C(p^r)_p^+$ and $C(p^r)_p^-$ are determined (in Section 4).

Now we compute the ℓ-primary part $C(p^r)_\ell$ of $C(p^r)$, for ℓ dividing $(p^2-1)/24 = ab$. Clearly, $C(p^r)_\ell$ is generated by $\overline{C}_{i,\ell}$ $(1 \leq i \leq r)$. Suppose that

$$\mu_1 \overline{C}_{1,\ell} + \cdots + \mu_r \overline{C}_{r,\ell} = 0. \tag{17}$$

Note that each μ_i is unique up to modulo ℓ^{r_ℓ}.

By considering the $(r+1)$st row in the vector $\Lambda^{-1}(\mu_1 C_{1,\ell} + \cdots + \mu_r C_{r,\ell})$, and applying Proposition 1, we get

$$v_\ell(\mu_{r-1}p^2 - \mu_r p^2) \geq r_\ell, \quad \text{i.e., } \mu_{r-1} \equiv \mu_r \bmod \ell^{r_\ell}.$$

Subsequently, considering the rth row, $(r-1)$st row, etc., of the same vector, shows that

$$\begin{array}{lll} \mu_i \equiv \mu_r & \bmod \ell^{r_\ell} & \text{if } i \geq \frac{r}{2}, \\ \mu_{\frac{r-1}{2}} \equiv \mu_{\frac{r+1}{2}} p & \bmod \ell^{r_\ell} & \text{if } r \text{ is odd}, \\ \mu_i \equiv \mu_{i+1} p^2 & \bmod \ell^{r_\ell} & \text{if } i+1 \leq \frac{r}{2}. \end{array}$$

If $\ell \neq 2$ divides a, then $(\ell, p+1) = 1$, and consideration of the first (or second) row of $\Lambda^{-1}(\mu_1 C_{1,\ell} + \cdots + \mu_r C_{r,\ell})$ shows that

$$\begin{aligned} r_\ell \leq & v_\ell(\mu_1 p^3 + \mu_2 p^3(p-1) + \cdots + \mu_i p^{t(i)+1}(p-1) + \cdots + \mu_r p^2) \\ = & v_\ell(\mu_1 p^3 + \mu_2 p^4) = v_\ell(\mu_1 p^3 + \mu_1 p^2) \\ = & v_\ell(\mu_1 p^2(p+1)) = v_\ell(\mu_1), \end{aligned}$$

i.e., $\mu_1 \equiv 0 \bmod \ell^{r_\ell}$.

Hence,

$$\mu_1 \equiv \mu_2 \equiv \cdots \equiv \mu_r \equiv 0 \bmod \ell^{r_\ell}.$$

If $\ell = 2$ and ℓ divides a, then $v_2(p+1) = 1$. To fix ideas, we may choose $\mu_1, \ldots, \mu_r$ such that

$$\begin{array}{ll} \mu_i = \mu_r & \text{if } i \geq \frac{r}{2}, \\ \mu_{\frac{r-1}{2}} = \mu_{\frac{r+1}{2}} p & \text{if } r \text{ is odd}, \\ \mu_i = \mu_{i+1} p^2 & \text{if } i+1 \leq \frac{r}{2}. \end{array}$$

Then it is easy to check that the third to $(r+1)$st rows of the vector $\Lambda^{-1}(\mu_1 C_{1,\ell} + \cdots + \mu_r C_{r,\ell})$ are all equal to 0. Condition (4) of Proposition 1 then implies that the second row of $\Lambda^{-1}(\mu_1 C_{1,\ell} + \cdots + \mu_r C_{r,\ell})$ must be even. This in turn implies that

$$v_2(\mu_1 p^2(p+1)) \geq r_2 + 1, \quad \text{i.e., } v_2(\mu_1) \geq r_2, \quad \text{i.e., } \mu_1 \equiv 0 \bmod 2^{r_2}.$$

Hence,

$$\mu_1 \equiv \mu_2 \equiv \cdots \equiv \mu_r \equiv 0 \bmod 2^{r_2}.$$

In other words, there is no relation among the $\overline{C}_{i,\ell}$ if ℓ is a prime divisor of a.

If $\ell \neq 2$ is a prime divisor of b, then $v_\ell(p+1) \geq r_\ell$. We verify readily that all the conditions in Proposition 1 are satisfied.

If $\ell = 2$ divides b, then $v_2(p+1) = r_2 + 2$, so the conditions of Proposition 1 are again satisfied.

Therefore, if ℓ is a prime divisor of b, then relations among the $\overline{C}_{i,\ell}$ exist if and only if

$$\begin{aligned} &\mu_1 \equiv \mu_2 \equiv \cdots \equiv \mu_r \bmod \ell^{r_\ell} && \text{if } r \text{ is even,} \\ &\mu_1 \equiv \mu_2 \equiv \cdots \equiv \mu_{\frac{r-1}{2}} \equiv -\mu_{\frac{r+1}{2}} \equiv \cdots \equiv -\mu_r \bmod \ell^{r_\ell} && \text{if } r \text{ is odd.} \end{aligned}$$

Equivalently, we have the relations

$$\begin{aligned} &\overline{C}_{1,\ell} + \cdots + \overline{C}_{r,\ell} = 0 && \text{if } r \text{ is even,} \\ &\overline{C}_{1,\ell} + \cdots + \overline{C}_{\frac{r-1}{2},\ell} - \overline{C}_{\frac{r+1}{2},\ell} - \cdots - \overline{C}_{r,\ell} = 0 && \text{if } r \text{ is odd.} \end{aligned}$$

We conclude therefore that the prime-to-p part $C(p^r)^{(p)}$ of $C(p^r)$ has the group structure

$$C(p^r)^{(p)} \simeq (\mathbf{Z}/a\mathbf{Z})^r \times (\mathbf{Z}/b\mathbf{Z})^{r-1}, \qquad r \geq 3. \tag{18}$$

This completes the proof of Theorem 1(ii).

4. Action of Atkin–Lehner involution

Let $w = w_{p^r}$ be the Atkin–Lehner involution on $J_0(p^r)$. Let $C(p^r)_p^+$ and $C(p^r)_p^-$ be as defined just before Theorem 1. We prove Theorem 1(i) in this section.

Since $C_i = \phi((p^i, p^{r-i}))P_1 - (P_{p^i})$ $(1 \leq i \leq r)$, we have

$$wC_i = \phi((p^i, p^{r-i}))P_{p^r} - (P_{p^{r-i}}).$$

When $r = 3$, we proved in subsection 3.2 that $C(p^3)_p$ is generated by $\overline{C}_{2,p}$. It is straight-forward to verify that

$$(w+1)\overline{C}_{2,p} = 0$$

using Proposition 1. It follows therefore that

$$C(p^3)_p = C(p^3)_p^- \simeq \mathbf{Z}/p^2\mathbf{Z}.$$

Now we assume $r \geq 4$.

LEMMA 2: *For $p \geq 5$ a prime and $r \geq 4$, we have*

$$C(p^r)_p^+ = \langle \overline{C}_{i,p} + w\overline{C}_{i,p} \ (2 \leq i \leq [\tfrac{r}{2}]) \rangle,$$
$$C(p^r)_p^- = \langle \overline{C}_{r,p}, \overline{C}_{i,p} - w\overline{C}_{i,p} \ (2 \leq i \leq [\tfrac{r-1}{2}]) \rangle.$$

Proof: Since $C(p^r)_p^+$ is the image of $(w+1)$ on $C(p^r)_p$ and $C(p^r)_p$ is generated by $\overline{C}_{i,p}$ $(2 \leq i \leq r-1)$, we have

$$C(p^r)_p^+ = \langle \overline{C}_{i,p} + w\overline{C}_{i,p} \ (2 \leq i \leq r-1) \rangle. \tag{19}$$

However, $C_i + wC_i = C_{r-i} + wC_{r-i}$ clearly, so

$$\overline{C}_{i,p} + w\overline{C}_{i,p} = \overline{C}_{r-i,p} + w\overline{C}_{r-i,p}. \tag{20}$$

Since $C_r = P_1 - P_{p^r}$, it follows immediately that $C_r + wC_r = 0$, i.e., $\overline{C}_{r,p} \in C(p^r)_p^-$. Using this fact, we deduce from (13) that

$$\overline{C}_{r-1,p} + w\overline{C}_{r-1,p} \in \langle \overline{C}_{i,p} + w\overline{C}_{i,p} \ (2 \leq i \leq r-2) \rangle. \tag{21}$$

Combining (19), (20) and (21), we conclude that

$$C(p^r)_p^+ = \langle \overline{C}_{i,p} + w\overline{C}_{i,p} \ (2 \leq i \leq \left[\frac{r}{2}\right]) \rangle.$$

Similarly, we obtain

$$C(p^r)_p^- = \langle \overline{C}_{i,p} - w\overline{C}_{i,p} \ (2 \leq i \leq r-1) \rangle.$$

We note that

$$C_{r-i} - wC_{r-i} = -(C_i - wC_i) + 2\phi((p^i, p^{r-i}))C_r.$$

It also follows from (13) that

$$\overline{C}_{r-1,p} - w\overline{C}_{r-1,p} \in \langle \overline{C}_{r,p}, \overline{C}_{i,p} - w\overline{C}_{i,p} \ (2 \leq i \leq r-2) \rangle.$$

Therefore,

$$C(p^r)_p^- = \langle \overline{C}_{r,p}, \overline{C}_{i,p} - w\overline{C}_{i,p} \ (2 \leq i \leq \left[\frac{r}{2}\right]) \rangle.$$

However, note that when r is even, we have

$$C_{\frac{r}{2}} - wC_{\frac{r}{2}} = \phi(p^{\frac{r}{2}})C_r.$$

Hence we conclude that

$$C(p^r)_p^- = \langle \overline{C}_{r,p}, \overline{C}_{i,p} - w\overline{C}_{i,p} \ (2 \leq i \leq \left[\frac{r-1}{2}\right]) \rangle. \qquad \blacksquare$$

It is routine to check the following:

- the order of $\overline{C}_{i,p} + w\overline{C}_{i,p}$ $(2 \le i \le \left[\frac{r}{2}\right])$ is p^{r-i},
- the order of $\overline{C}_{i,p} - w\overline{C}_{i,p}$ $(2 \le i \le \left[\frac{r-1}{2}\right])$ is p^{r-i},
- there is no non-trivial relation among $\overline{C}_{i,p} + w\overline{C}_{i,p}$ $(2 \le i \le \left[\frac{r}{2}\right])$,
- there is no non-trivial relation among $\overline{C}_{i,p} - w\overline{C}_{i,p}$ $(2 \le i \le \left[\frac{r-1}{2}\right])$.

It then follows that

$$C(p^r)_p^+ \simeq \mathbf{Z}/p^{r-[\frac{r}{2}]}\mathbf{Z} \times \cdots \times \mathbf{Z}/p^{r-3}\mathbf{Z} \times \mathbf{Z}/p^{r-2}\mathbf{Z},$$
$$C(p^r)_p^- \simeq \mathbf{Z}/p^{r-[\frac{r-1}{2}]}\mathbf{Z} \times \cdots \times \mathbf{Z}/p^{r-2}\mathbf{Z} \times \mathbf{Z}/p^{r-1}\mathbf{Z}.$$

This completes the proof of Theorem 1(i).

5. Kernels of degeneracy maps

An important ingredient in our proof of Theorem 3 is Theorem 5, which we state and prove below.

For $1 \le h \le r-1$, let $v_1, v_p, \ldots, v_{p^{r-h}}\colon X_0(p^r) \to X_0(p^h)$ be the degeneracy maps from $X_0(p^r)$ to $X_0(p^h)$ defined in subsection 3.2. They induce, via Pic functoriality, the maps $v_1^*, \ldots, v_{p^{r-h}}^*\colon J_0(p^h) \to J_0(p^r)$. Let $\gamma_{h,r}$ denote the map

$$\gamma_{h,r} \stackrel{\text{def}}{=} v_1^* \times \cdots \times v_{p^{r-h}}^*\colon J_0(p^h)^{r-h+1} \longrightarrow J_0(p^r).$$

By passing to characteristic p, $\gamma_{h,r}$ induces naturally a map on the component groups, which we also call $\gamma_{h,r}$:

$$\gamma_{h,r}\colon (\Phi_{p^h})^{r-h+1} \longrightarrow \Phi_{p^r}.$$

THEOREM 5: *Let $p \ge 5$ be a prime. Let $\gamma_{1,r}$ be the map*

$$\gamma_{1,r} = v_1^* \times \cdots \times v_{p^{r-1}}^*\colon \Phi_p^r \longrightarrow \Phi_{p^r}.$$

Then the kernel of $\gamma_{1,r}$ is

$$\left\{ \begin{pmatrix} x_1 \\ \vdots \\ x_r \end{pmatrix} \in \Phi_p^r \;\middle|\; \sum x_i = 0 \right\}.$$

Proof: Let $\Sigma(p)$ denote the Shimura subgroup in $J_0(p)$, and let $U(p)$ denote the covering group of the maximal étale subcover of the covering $X_1(p) \to X_0(p)$. It is well known that $\Sigma(p)$ may be regarded as the Cartier dual of $U(p)$ ([9], II.11).

Let $\Sigma(\mathbf{F}_p)$ be defined by

$$\Sigma(\mathbf{F}_p) \stackrel{\text{def}}{=} \mathrm{Hom}(U(p), \mu_a(\mathbf{F}_p)),$$

where $\mu_a(\mathbf{F}_p)$ denotes the group of ath roots of unity in $\mathbf{F}_p$. It is known (cf. [9], [6]) that $\Sigma(p)$ is of order $a = \frac{p-1}{(p-1,12)}$. Hence, $U(p)$ and $\Sigma(\mathbf{F}_p)$ are also of order a.

Recall that, when restricted to the prime-to-p torsion, the canonical reduction map

$$\pi_h \colon J_0(p^h)(\mathbf{Q}_p) \longrightarrow \mathcal{J}_0(p^h)_s(\mathbf{F}_p) \tag{22}$$

is injective.

The degeneracy maps $v_1^*, \ldots, v_{p^{r-1}}^* \colon J_0(p) \to J_0(p^r)$ are injective, and they coincide with one another on $\Sigma(p)$ ([6], Remark after Theorem 5). Together with (22), we see that these degeneracy maps induce *injections* $v_{1/\mathbf{F}_p}^*, \ldots, v_{p^{r-1}/\mathbf{F}_p}^* \colon \Sigma(\mathbf{F}_p) \to \mathcal{J}_0(p^r)_s(\mathbf{F}_p)$, and these induced maps are identical. We therefore obtain the commutative diagram

$$\begin{array}{ccc} \Sigma(\mathbf{F}_p) \times \cdots \times \Sigma(\mathbf{F}_p) & \xrightarrow{\gamma_{1,r}} & \mathcal{J}_0(p^r)_s(\mathbf{F}_p) \\ \downarrow u & & \downarrow \\ \Phi_p \times \cdots \times \Phi_p & \xrightarrow{\gamma_{1,r}} & \Phi_{p^r}. \end{array} \tag{23}$$

The horizontal maps are the obvious maps induced from (22), and the vertical maps come from the projection of the special fibre of the Néron model onto the group of components.

From [9], II Proposition 11.9, we know that u is an isomorphism.

Since

$$\gamma_{1,r} = v_{1/\mathbf{F}_p}^* \times \cdots \times v_{p^{r-1}/\mathbf{F}_p}^* \colon \Sigma(\mathbf{F}_p)^r \to \mathcal{J}_0(p^r)_s(\mathbf{F}_p),$$

and $v_{1/\mathbf{F}_p}^*, \ldots, v_{p^{r-1}/\mathbf{F}_p}^*$ are identical on $\Sigma(\mathbf{F}_p)$, together with (23) it follows that the kernel of $\gamma_{1,r} \colon \Phi_p^r \to \Phi_{p^r}$ contains

$$\left\{ \begin{pmatrix} x_1 \\ \vdots \\ x_r \end{pmatrix} \in \Phi_p^r \;\middle|\; \sum x_i = 0 \right\}.$$

On the other hand, $v_1^*\colon \Phi_p \to \Phi_{p^r}$ is injective (cf. [5], §2.1 or [7], Lemma 4.1), so the image of Φ_p^r under $\gamma_{1,r}$ contains a subgroup of order a.

By considering the cardinalities, it follows immediately that the kernel of $\gamma_{1,r}\colon \Phi_p^r \to \Phi_{p^r}$ is precisely

$$\left\{ \begin{pmatrix} x_1 \\ \vdots \\ x_r \end{pmatrix} \in \Phi_p^r \;\middle|\; \sum x_i = 0 \right\}.$$

This completes the proof of Theorem 5. ∎

6. Computation of Φ_{p^r}

We shall prove Theorem 3 in this section.

For $p \geq 5$ a prime, we recall that, if $\ell \neq 2, 3$ is a prime, then the canonical reduction map

$$\pi_h\colon C(p^h)_\ell \longrightarrow (\Phi_{p^h})_\ell$$

is surjective ([7], Theorem 2.3).

If $(\ell, pab) = 1$, then $C(p^r)_\ell$ is trivial according to Theorem 1. Since π_r is surjective, we conclude that

$$(\Phi_{p^r})_\ell \text{ is trivial if } (\ell, pab) = 1. \tag{24}$$

If ℓ divides b (and $(\ell, 6) = 1$), then $C(p^r)_\ell \simeq (\mathbf{Z}/\ell^{v_\ell(b)}\mathbf{Z})^{r-1}$. Since Φ_{p^r} contains a copy of $(\mathbf{Z}/b\mathbf{Z})^{r-1}$ ([7], Theorems 1.1(i) and 4.3), surjectivity of π_r and cardinality consideration show that

$$(\Phi_{p^r})_\ell \simeq (\mathbf{Z}/\ell^{v_\ell(b)}\mathbf{Z})^{r-1} \quad \text{if } (\ell, 6) = 1, \quad \ell \text{ divides } b. \tag{25}$$

If ℓ divides a (and $(\ell, 6) = 1$), then $C(p^r)_\ell \simeq (\mathbf{Z}/\ell^{v_\ell(a)}\mathbf{Z})^r$ by Theorem 1.

Consider the following commutative diagram:

$$\begin{array}{ccc} C(p)_\ell^r & \xrightarrow{\gamma_{1,r}} & C(p^r)_\ell \\ \downarrow{\scriptstyle \pi_1^r} & & \downarrow{\scriptstyle \pi_r} \\ (\Phi_p)_\ell^r & \xrightarrow{\gamma_{1,r}} & (\Phi_{p^r})_\ell. \end{array} \tag{26}$$

Recall that ([5], Theorem 2) the kernel of the map $\gamma_{1,r}\colon J_0(p)^r \to J_0(p^r)$ is the group

$$K = \left\{ \begin{pmatrix} x_1 \\ \vdots \\ x_r \end{pmatrix} \in \Sigma(p)^r \;\middle|\; \sum x_i = 0 \right\}.$$

Since $\Sigma(p) \cap C(p) = C(p)[2] \stackrel{\text{def}}{=} \{x \in C(p)\colon 2x = 0\}$ ([9], II Proposition 11.11), and $\ell \neq 2$, the restriction $\gamma_{1,r}\colon C(p)_\ell^r \to C(p^r)_\ell$ is therefore injective. Comparing cardinalities, we obtain the isomorphism

$$\gamma_{1,r}\colon C(p)_\ell^r \xrightarrow{\simeq} C(p^r)_\ell. \tag{27}$$

Surjectivity of π_r and π_1^r, commutativity of (26), as well as the isomorphism (27), combine to show that any element of $(\Phi_{p^r})_\ell$ lies in the image of $(\Phi_p)_\ell^r$ under $\gamma_{1,r}$. By Theorem 5,

$$|(\Phi_{p^r})_\ell| \leq |\gamma_{1,r}((\Phi_p)_\ell)| = \ell^{v_\ell(a)}.$$

On the other hand, $(\Phi_{p^r})_\ell$ contains a subgroup of order $\ell^{v_\ell(a)}$ (cf. [5], subsection 2.1, or [7], Lemma 4.1). Therefore we have

$$(\Phi_{p^r})_\ell \simeq \mathbf{Z}/\ell^{v_\ell(a)}\mathbf{Z} \quad \text{if } (\ell, 6) = 1, \quad \ell \text{ divides } a. \tag{28}$$

Putting (24), (25) and (28) together, we obtain Theorem 3(i).

Finally, we take $\ell = p$. If $p \equiv 11 \bmod 12$, the surjectivity of π_r yields an upper bound for $|(\Phi_{p^r})_p|$:

$$|(\Phi_{p^r})_p| \leq \begin{cases} p^{r-2} \prod_{2<i<r} p^{r-t(i)}, & r \geq 4, \\ p^2, & r = 3, \\ 1, & r = 2. \end{cases}$$

These are equivalent to the bounds in the statement of Theorem 3(ii).

This completes the proof of Theorem 3.

7. More on kernels of degeneracy maps

In this section, as a corollary of Theorem 3, we prove

THEOREM 6: *Let $p \geq 5$ be a prime, and let $\ell \neq 2, 3$ be a prime divisor of a. Then, for $1 \leq h \leq r-1$, the kernel of the map*

$$\gamma_{h,r} = v_1^* \times \cdots \times v_{p^{r-h}}^*\colon (\Phi_{p^h})_\ell^{r-h+1} \longrightarrow (\Phi_{p^r})_\ell$$

is given by

$$\left\{ \begin{pmatrix} x_1 \\ \vdots \\ x_{r-h+1} \end{pmatrix} \in (\Phi_{p^h})_\ell^{r-h+1} \;\middle|\; \sum x_i = 0 \right\}.$$

Remarks: (1) When $h = 1$ or 2, Theorem 6 holds also for $\ell = 2, 3$. This follows immediately from Theorem 5 and the isomorphism $(\Phi_p)_\ell \simeq (\Phi_{p^2})_\ell$.

(2) When $p \not\equiv 11 \bmod 12$, the same conclusion again holds for $\ell = 2, 3$ (cf. [7], Theorem 1.1(ii)).

COROLLARY : *Let $p \geq 5$ be a prime. The kernel of the map*

$$\gamma_{2,r} = v_1^* \times \cdots \times v_{p^{r-2}}^* \colon \Phi_{p^2}^{r-1} \longrightarrow \Phi_{p^r}$$

is

$$\left\{ \begin{pmatrix} bx_1 \\ \vdots \\ bx_{r-1} \end{pmatrix} \in \Phi_{p^2}^{r-1} \;\middle|\; x_i \in \Phi_{p^2} \text{ for all } i, \sum bx_i = 0 \right\}.$$

Proof: This follows immediately from Theorem 6, the first remark after Theorem 6, the injectivity of $\gamma_{2,r}$ when restricted to the b-part of $\Phi_{p^2}^{r-1}$ ([7], Theorem 4.3), and the fact that $\Phi_{p^2} \simeq \mathbf{Z}/ab\mathbf{Z}$. ∎

Proof of Theorem 6: Let $\ell \neq 2, 3$ be a prime dividing a. The degeneracy map $v_1^* \colon J_0(p) \to J_0(p^h)$ induces an isomorphism

$$v_1^* \colon (\Phi_p)_\ell \xrightarrow{\simeq} (\Phi_{p^h})_\ell.$$

Therefore, in order to determine the kernel of

$$\gamma_{h,r} \colon (\Phi_{p^h})_\ell^{r-h+1} \longrightarrow (\Phi_{p^r})_\ell,$$

we consider the following commutative diagram:

$$\begin{array}{ccc} (\Phi_p)_\ell^{r-h+1} & = & (\Phi_p)_\ell^{r-h+1} \\ {\scriptstyle (v_1^*)^{r-h+1}}\downarrow & & \downarrow{\scriptstyle v_1^* \times \cdots \times v_{p^{r-h}}^*} \\ (\Phi_{p^h})_\ell^{r-h+1} & \xrightarrow{\gamma_{h,r}} & (\Phi_{p^r})_\ell. \end{array}$$

Since the vertical map $(v_1^*)^{r-h+1}$ is an isomorphism, and the maps $v_1^*, \ldots, v_{p^{r-h}}^* \colon (\Phi_p)_\ell \to (\Phi_{p^r})_\ell$ all coincide (cf. Section 4), it follows immediately that the kernel

of $\gamma_{h,r}\colon (\Phi_{p^h})_\ell^{r-h+1} \to (\Phi_{p^r})_\ell$ is

$$\left\{ \begin{pmatrix} x_1 \\ \vdots \\ x_{r-h+1} \end{pmatrix} \in (\Phi_{p^h})_\ell^{r-h+1} \;\middle|\; \sum x_i = 0 \right\}. \quad \blacksquare$$

References

[1] S. Edixhoven, *Minimal resolution and stable reduction of $X_0(N)$*, Annales de l'Institut Fourier **40** (1990), 31–67.

[2] S. Edixhoven, *L'action de l'algèbre de Hecke sur les groupes de composantes des jacobiennes des courbes modulaires est "Eisenstein"*, Astérisque **196–197** (1991), 159–170.

[3] G. Ligozat, *Courbes modulaires de genre 1*, Bulletin de la Société Mathématique de France, Mémoire **43** (1975).

[4] S. Ling, *The old subvariety of $J_0(pq)$ and the Eisenstein kernel in Jacobians*, Israel Journal of Mathematics **84** (1993), 365–384.

[5] S. Ling, *Congruences between cusp forms and the geometry of Jacobians of modular curves*, Mathematische Annalen **295** (1993), 111–133.

[6] S. Ling and J. Oesterlé, *The Shimura subgroup of $J_0(N)$*, Astérisque **196–197** (1991), 171–203.

[7] D. Lorenzini, *Torsion points on the modular Jacobian $J_0(N)$*, Compositio Mathematica **96** (1995), 149–172.

[8] Ju. Manin, *Parabolic points and zeta functions of modular curves*, Izvestiya Akademii Nauk SSSR **6** (1972); AMS Translation 19–64.

[9] B. Mazur, *Modular curves and the Eisenstein ideal*, Publications Mathématiques de l'Institut des Hautes Études Scientifiques **47** (1978), 33–186.

[10] A. Ogg, *Rational points on certain elliptic curves*, Proceedings of Symposia in Pure Mathematics **24** (1973), 221–231.

[11] A. Ogg, *Hyperelliptic modular curves*, Bulletin de la Société Mathématique de France **102** (1974), 449–462.