ON COMPONENT GROUPS OF $J_0(N)$
AND DEGENERACY MAPS

SAN LING

(Communicated by David E. Rohrlich)

ABSTRACT. For an integer $M > 1$ and a prime $p \geq 5$ not dividing $M$, we study the kernel of the degeneracy map $\Phi_{Mp,p} \rightarrow \Phi_{Mp',p'}$, where $\Phi_{Mp,p}$ and $\Phi_{Mp',p'}$ are the component groups of $J_0(Mp)$ and $J_0(Mp')$, respectively. This is then used to determine the kernel of the degeneracy map $J_0(Mp)^2 \rightarrow J_0(Mp^2)$ when $J_0(M) = 0$. We also compute the group structure of $\Phi_{Mp^2,p}$ in some cases.

Let $N \geq 1$ be a positive integer, let $X_0(N)$ be the classical modular curve defined over $\mathbb{Q}$, and let $J_0(N)$ denote its Jacobian variety, also defined over $\mathbb{Q}$.

For a prime number $p$, $X_0(N)$ and $J_0(N)$ are also defined over $\mathbb{Q}_p$. When $\gcd(p, N) = 1$, $J_0(N)$ has good reduction at $p$. When $p$ divides $N$, the special fibre $J_0(N)_{\mathbb{F}_p}$ in the Néron model of $J_0(N)$ over $\mathbb{Z}_p$ is the extension of a finite étale group scheme $\Phi_{N,p}$ by the connected component of identity $J_0(N)^{\circ \varepsilon}_{\mathbb{F}_p}$. The finite group $\Phi_{N,p}$ is called the group of components of the special fibre of the Néron model of $J_0(N)$ over $\mathbb{Z}_p$. It has been computed for certain values of $N$ with $p \geq 5$ (cf. [11], [2], [10]). When $p^2$ does not divide $N$, then $\Phi_{N,p}$ contains a canonical cyclic subgroup $\Phi_{N,p}'$ (see §1 for discussion) such that $\Phi_{N,p}/\Phi_{N,p}'$ has exponent dividing 6.

If $N'$ is a positive divisor of $N$ and $D$ is a positive divisor of $N/N'$, let $\nu_D : X_0(N) \rightarrow X_0(N')$ be the degeneracy map induced by $\tau \mapsto D\tau$. This map induces $\nu_D' : J_0(N') \rightarrow J_0(N)$ and $(\nu_D)_* : J_0(N) \rightarrow J_0(N')$ on the Jacobian varieties. We also use the same notation for the maps they induce on the component groups.

The kernel of $\eta = \prod_{D|N/N'} \nu_D'$ is useful in the study of congruence relations between cusp forms of different levels (cf. [13], [6] and [7]). However, even when this kernel is finite, its determination can be difficult. An understanding of the kernel $K$ of the map $\eta$ induces on the component groups enables one to have a better control over the kernel of $\eta$ (cf. loc. cit. as well as Theorem 1 and Proposition 1 below).

The kernel $K$ of $\eta$ on the component groups is known in some cases. For example, when $N = Mpq$ and $N' = Mp$, where $M$ is a positive integer, $p \geq 5$ is a prime not dividing $M$ and $q$ is a prime such that $\gcd(q, Mp) = 1$, $K$ contains...
\[
\left\{ \left( \frac{x}{x} \right) \in \Phi^2_{M,p,p} \quad \forall \, x \in \Phi_{M,p,p} \right\} \quad ([14], [15]) .
\]

When \( N = p^r \) and \( N' = p \), where \( p \geq 5 \) is a prime, \( K = \left\{ \left( \frac{x_1}{x_r} \right) \in \Phi^r_{p,p} \mid \sum x_i = 0 \right\} \) ([8]). In this paper, we prove

**Theorem 1.** Let \( M > 1 \) be a positive integer with prime power decomposition \( M = \prod \ell^n_i \) and let \( p \geq 5 \) be a prime not dividing \( M \). Let \( Q = \text{deg}(X_0(M)/X_0(1)) = \prod (\ell + 1)^{n_i-1} \) and let \( \nu \) be the number of primes, distinct from 2 and 3, dividing \( M \). Let \( \sigma_q \) (resp. \( \sigma_p \)) denote the number of points \( x \) of \( X_0(M)(\overline{\mathbb{F}}_p) \) with \( |\text{Aut}(x)| = 4 \) (resp. 6). Let \( g \) be the canonical generator of \( \Phi'_{M,p,p} \) (see §1.1). Then the kernel \( K' \) of the induced map

\[
\eta' = v_1^* \times v_p^* : \Phi'_{M,p,p} \times \Phi_{M,p,p} \longrightarrow \Phi_{M,p,p}
\]

is given in Table 1. In particular, \( v_1^*, v_p^* : \Phi'_{M,p,p} \longrightarrow \Phi_{M,p,p} \) are injective.

For a finite group \( G \) and an integer \( n \), let \( G^{(n)} \) denote the prime-to-\( n \) part of \( G \). In view of the fact that \( \Phi_{M,p,p} / \Phi'_{M,p,p} \) has exponent dividing 6, we have

**Corollary 1.** We have the equality \( K^{(6)} = K'^{(6)} \). In particular, \( K^{(6)} \) is isomorphic to the prime-to-six part of \( \mathbb{Z}/(p - 1)\mathbb{Z} \).

**Corollary 2.** For \( X_0(M) \) such that \( \sigma_4 = \sigma_6 = 0 \), we have \( K = K' \).

**Proof.** This follows from the fact that \( \Phi_{M,p,p} = \Phi'_{M,p,p} \) in these cases (cf. [12], [2]). \( \square \)

**Remark.** When \( N = Mpq \) and \( N' = Mp \), where \( M, p \) are as in Theorem 1 and \( q \) is a prime such that \( \text{g.c.d.}(q, Mp) = 1 \), it can be shown that \( v_1^*, v_q^* : \Phi^{(6)}_{M,p,p} \longrightarrow \Phi_{Mpq,p} \) are injective, so \( K^{(6)} = \left\{ \left( \frac{x}{x} \right) \mid x \in \Phi^{(6)}_{M,p,p} \right\} \).

Let \( M \geq 1 \) be a positive integer and let \( p \geq 5 \) be a prime not dividing \( M \). Let \( \Sigma(Mp) \) be the Shimura subgroup of \( J_0(Mp) \) (so \( \Sigma(Mp)_{Q_p} \) is the corresponding subgroup scheme of \( J_0(Mp)_{Q_p} \)). Then \( \Sigma(Mp)_{Q_p} \) extends (by the Zariski closure) to a finite subgroup scheme of the Néron model of \( J_0(Mp) \) over \( \mathbb{Z}_p \) (see §2.1, Lemma 1). We denote the special fibre of this latter group scheme by \( \Sigma(Mp)_{\mathbb{F}_p} \). Proposition 11.9 of [11] shows that, for \( M = 1 \), the scheme-theoretic intersection \( \Sigma(p)_{\mathbb{F}_p} \cap J_0(p)^{\delta(p)}_{\mathbb{F}_p} \) is the trivial group scheme over \( \mathbb{F}_p \).

We generalise Proposition 11.9 of [11] by showing:

**Theorem 2.** Let \( M > 1 \) be a positive integer and let \( p \geq 5 \) be a prime not dividing \( M \). The kernel of the homomorphism \( \Sigma(Mp)^{(6p)}_{\mathbb{F}_p} \longrightarrow \Phi_{M,p,p} \) is isomorphic to \( \Sigma(M)^{(6p)}_{\mathbb{F}_p} \). Equivalently, the scheme-theoretic intersection \( \Sigma(Mp)^{(6p)}_{\mathbb{F}_p} \cap J_0(Mp)^{\delta(p)}_{\mathbb{F}_p} \) is isomorphic to \( \Sigma(M)^{(6p)}_{\mathbb{F}_p} \).

Let \( \tilde{\Phi}_{M,p,p} \) denote the image of \( \Sigma(Mp)^{(6p)}_{\mathbb{F}_p} \) in Theorem 2. When \( N = Mp^r \) (\( r \geq 2 \)) and \( N' = Mp \), the map \( \eta \) induces another map \( \eta : \tilde{\Phi}_{M,p,p} \longrightarrow \Phi_{M',p} \) on the group of components, with kernel \( K \). Theorem 2 leads easily to the following theorem, which is a somewhat weaker generalisation of Theorem 2 of [8].
Table 1. The kernel $K'$

| Case | $\sigma_4$ | $\sigma_6$ | $p \mod 12$ | $K'$ | $|K'|$ |
|------|------------|------------|-------------|------|------|
| (I)  | 0          | 0          | 1, 5, 7, 11 | \(\begin{cases} \{ \frac{x}{y} \} & x \in \left\langle \frac{Q}{12} \mathbb{g} \right\rangle \text{ (if } M \neq 4) \\ \{ \frac{x}{y} \} & x \in \Phi'_{Mp,p} \text{ (if } M = 4) \end{cases}\) | \(p - 1\) |
| (II) | 0          | 2\(^r\)    | 5, 11       | \(\begin{cases} \{ \frac{x}{y} \} & x \in \left\langle \frac{Q}{4} \mathbb{g} \right\rangle \end{cases}\) | \(p - 1\) |
| (III)| 2\(^r\)    | 0          | 7, 11       | \(\begin{cases} \{ \frac{x}{y} \} & x \in \Phi'_{Mp,p} \text{ (if } M = 2) \\ \{ \frac{x}{y} \} & x \in \left\langle \frac{Q}{6} \mathbb{g} \right\rangle \text{ (if } M = q^r \text{ or } 2q^r, \text{ where } q \equiv 1 \text{ mod 4 is prime)} \\ \{ \frac{x}{y} \} & x \in \left\langle \frac{Q}{12} \mathbb{g} \right\rangle \text{ (if } M \neq 2) \end{cases}\) | \(2(p - 1)\) |
| (IV) | 2\(^r\)    | 2\(^r\)    | 1           | \(\begin{cases} \frac{x}{y} \in \left\langle \frac{Q}{4} \mathbb{g} \right\rangle \end{cases}\) | \(p - 1\) |

**Theorem 3.** If $M > 1$ is a positive integer and $p \geq 5$ is a prime not dividing $M$, then, for $N = Mp^r$ ($r \geq 3$) and $N' = Mp$, the kernel $K$ contains

\[
\left\{ \begin{array}{c} x_1 \\ \vdots \\ x_r \end{array} \right\} \in \Phi'_{Mp,p} \mid x_i \in \tilde{\Phi}_{Mp,p} \text{ for all } i, \sum x_i = 0 .
\]

**Remark.** The case $r = 2$ is dealt with in Theorem 1, with a stronger conclusion.

The organisation of this paper is as follows. We prove Theorem 1 in §1. Theorems 2 and 3 are dealt with in §2. Finally in §3, we discuss some consequences and examples.
1. PROOF OF THEOREM 1

We begin with some remarks on the component group $\Phi_{M,p,p'}$ (where $p \geq 5$ is a prime not dividing $M$) and the canonical cyclic subgroup $\Phi_{M,p,p'}^{C}$ alluded to in the introduction.

1.1. The component group. Let $M \geq 1$ be a positive integer and let $p \geq 5$ be a prime not dividing $M$. Consider the modular curve $X_0(Mp)$ over $\mathbb{Q}_p$. The model of the reduction mod $p$ of $X_0(Mp)$ studied by Deligne-Rapoport [1] consists of two irreducible components $C_0$ and $C_1$, each a copy of the modular curve $X_0(Mp)$, glued together at the supersingular points. For each singular point $x$ with $e(x) > 1$ by a chain of $e(x) - 1$ copies of the projective line $\mathbb{P}^1$. Label these additional components by $C_2, \ldots, C_n$.

Let $L \overset{\text{def}}{=} \bigoplus_{i=0}^{n} \mathbb{Z}[C_i]$ be the free abelian group generated by these components. Let $\iota : L \to L$ be the map defined by $\iota([C_i]) \overset{\text{def}}{=} \sum_{j=0}^{n} (C_i \cdot C_j)[C_j]$. Let $\deg : L \to \mathbb{Z}$ be the obvious degree map. Then $\Phi_{M,p,p}$ contains a canonical cyclic subgroup $\Phi_{M,p,p}^{C}$ generated by the image of $\Phi_{M,p,p}$ of $C_0 - C_1 \in L$. We regard this image of $C_0 - C_1$ as the canonical generator $g$ of $\Phi_{M,p,p}^{C}$. The quotient $\Phi_{M,p,p}/\Phi_{M,p,p}^{C}$ has exponent dividing the lowest common multiple of the $e(x)$'s. In particular, it has exponent dividing 6.

Next consider the modular curve $X_0(Mp^{r})$. The minimal resolution of $X_0(Mp^{r})$ has been constructed by Edixhoven [3]. Let the irreducible components of the minimal resolution be denoted by $C_0', C_1', \ldots, C_n'$ (where $C_0', \ldots, C_n'$ are copies of $X_0(Mp)$ and the remaining ones are copies of $\mathbb{P}^1$) and let $L' = \bigoplus \mathbb{Z}[C_i']$ be the analogue of $L$. Similarly, one can define $\iota' : L' \to L'$ and $\deg' : L' \to \mathbb{Z}$ to be the analogues of $\iota$ and $\deg$, respectively. Let $\pi : X_0(Mp^{r}) \to X_0(Mp)$ be a morphism. Then the discussion in [2] shows that there is a commutative diagram

\[
\begin{array}{ccc}
L & \xrightarrow{\iota} & L \\
\downarrow \pi^*_{\text{div}} & & \downarrow \pi^*_{\text{deg}} \\
L' & \xrightarrow{\iota'} & L' \\
\end{array}
\]

where

\[
\pi^*_{\text{div}}([C]) = \pi^{-1}C(\text{divisor on } X_0(Mp^r)), \quad \pi^*_{\text{deg}}([C]) = \sum_{C' \sim C} \deg(\pi|_{C'})(C').
\]

1.2. The intersection matrix. The map $\iota' : L' \to L'$ can be represented as a square matrix once an ordered basis is chosen for $L'$. This is called the intersection matrix of $J_0(Mp^{r})$. When $r = 2$, the model of reduction mod $p$ of $X_0(Mp^2)$ studied by Katz-Mazur consists of three irreducible components, each a copy of $X_0(Mp)$, glued together at the supersingular points. We let these three components be $C_0', C_1', C_2'$, where $C_0'$ and $C_1'$ both have multiplicity 1 and $C_2'$ has multiplicity $p - 1$. Let $C_3', \ldots, C_n'$ be the additional components, if any, introduced to form the minimal resolution. Using the ordered basis $\{C_0', C_1', C_2', \ldots\}$ for $L'$, the intersection matrix of $J_0(Mp^2)$ is given as follows (according to the cases listed out in Table 1):
Table 2. Values of $\alpha$, $\beta$ and $\delta$.

<table>
<thead>
<tr>
<th>Case</th>
<th>(II)</th>
<th>(III)</th>
<th>(IV)</th>
</tr>
</thead>
<tbody>
<tr>
<td>$p \mod 12$</td>
<td>$1, 7, 5, 11$</td>
<td>$1, 5, 7, 11$</td>
<td>$1, 5, 7, 11$</td>
</tr>
<tr>
<td>$\alpha$</td>
<td>$0 \cdot 2^\nu$</td>
<td>$0 \cdot 2^\nu$</td>
<td>$0 \cdot 2^\nu$</td>
</tr>
<tr>
<td>$\beta$</td>
<td>$-3$</td>
<td>$-3$</td>
<td>$-2$</td>
</tr>
<tr>
<td>$\delta$</td>
<td>$0$</td>
<td>$1$</td>
<td>$1$</td>
</tr>
</tbody>
</table>

(I) It is the $3 \times 3$ matrix

$$
\begin{pmatrix}
-\frac{Q(p-1)}{12} & \frac{Q(p-1)}{12} & \frac{Q(p-1)}{12} \\
-\frac{Q(p-1)}{12} & -\frac{Q(p-1)}{12} & \frac{Q(p-1)}{12} \\
\frac{Q(p-1)}{12} & \frac{Q(p-1)}{12} & -\frac{Q(p-1)}{12}
\end{pmatrix}
$$

(II), (III) It is the $(3 + 2^\nu) \times (3 + 2^\nu)$ matrix (with $\alpha$, $\beta$, $\delta$ given in Table 2)

$$
\begin{pmatrix}
-\frac{Q(p-1)+\alpha}{12} & \frac{Q(p-1)-\alpha}{12} & \frac{Q(p-1)-\alpha}{12} \\
\frac{Q(p-1)-\alpha}{12} & -\frac{Q(p-1)+\alpha}{12} & \frac{Q(p-1)-\alpha}{12} \\
\frac{Q(p-1)-\alpha}{12} & \frac{Q(p-1)-\alpha}{12} & -\frac{Q(p-1)-\alpha}{12}
\end{pmatrix}
$$

(IV) It is the $(3 + 2 \cdot 2^\nu) \times (3 + 2 \cdot 2^\nu)$ matrix (with $\alpha$, $\beta$, $\delta$ given in Table 2)

$$
\begin{pmatrix}
-\frac{Q(p-1)+\alpha}{12} & \frac{Q(p-1)-\alpha}{12} & \frac{Q(p-1)-\alpha}{12} \\
\frac{Q(p-1)-\alpha}{12} & -\frac{Q(p-1)+\alpha}{12} & \frac{Q(p-1)-\alpha}{12} \\
\frac{Q(p-1)-\alpha}{12} & \frac{Q(p-1)-\alpha}{12} & -\frac{Q(p-1)-\alpha}{12}
\end{pmatrix}
$$

1.3. The kernel of $\eta'$. Consider (1) with $r = 2$ and $\pi$ as the two degeneracy maps $v_1, v_p$. To determine which $(\lambda g, -\mu g) \in \Phi_{M,p} \times \Phi_{M,p}$ actually belongs to the kernel of $\eta'$, we consider $\eta'((\lambda(C_0 - C_1), -\mu(C_0 - C_1))$ (which belongs to ker(deg')). In fact, $(\lambda g, -\mu g) \in \ker \eta'$ if and only if $\eta'((\lambda(C_0 - C_1), -\mu(C_0 - C_1)) \in \im(i')$.

Since $v_1^*(C_0) = pC_0'$, $v_1^*(C_1) = C_1' + C_2'$, $v_p^*(C_0) = C_0' + C_2'$ and $v_p^*(C_1) = pC_1'$ (cf. (2)), we have

$$(v_1^* \times v_p^*)(\lambda(C_0 - C_1), -\mu(C_0 - C_1)) = (p\lambda - \mu)C_0' + (p\mu - \lambda)C_1' - (\lambda + \mu)C_2'.
$$

It follows that $(\lambda g, -\mu g) \in \ker \eta'$ if and only if

$$
v = (p\lambda - \mu, p\mu - \lambda, -(\lambda + \mu), 0, \ldots, 0)^T
$$

is a $\mathbb{Z}$-linear combination of the columns of the intersection matrix in §1.2.
Let \( c_i \) denote the \( i \)th column of the intersection matrix. Let \( m \) be the number of columns in the intersection matrix. Let \( \lambda_i \) (\( 1 \leq i \leq m \)) be integers and suppose

\[
\nu = \lambda_1 c_1 + \cdots + \lambda_m c_m.
\]

By simple row operations, it is easy to show that the following identities hold:

\[
\mu = \frac{Q}{12} \left( \lambda_3 - \lambda_2(p - 1) \right)
\]

and

\[
\mu - \lambda = \frac{Q(p - 1)}{12}(\lambda_1 - \lambda_2).
\]

Now we prove Theorem 1 case by case.

(I) In this case, the order of \( \Phi'_{M,p,p} \) is \( \frac{Q(p-1)}{12} \). Suppose that \( M \neq 4 \). Then 12 divides \( Q \). From (4), \( \mu \in \frac{Q}{12}\mathbb{Z} \). From (5), \( \mu \equiv \lambda \mod \frac{Q(p-1)}{12} \). Therefore the kernel \( K' \) is contained in \( \left\{ \left( \frac{x}{Q} \right) \mid x \in \langle \frac{Q}{12}g \rangle \right\} \). Taking \( \lambda_1 = 1, \lambda_2 = 0 \) and \( \lambda_3 = 1 \) in (3), we obtain \( \mu = \frac{Q}{12} \) and \( \lambda = \frac{Q}{12} - \frac{Q(p-1)}{12} \), so \( K' = \left\{ \left( \frac{x}{Q} \right) \mid x \in \langle \frac{Q}{12}g \rangle \right\} \).

When \( M = 4 \), then \( Q = 6 \) and \( \Phi'_{M,p,p} \) has order \( \frac{p-1}{2} \). The identity (5) implies \( \mu \equiv \lambda \mod \frac{p-1}{2} \), so \( K' \subseteq \left\{ \left( \frac{x}{p} \right) \mid x \in \Phi'_{M,p,p} \right\} \). Taking \( \lambda_3 = 2, \lambda_2 = 0 = \lambda_1 \), we get \( \mu = \lambda = 1 \), so \( K' = \left\{ \left( \frac{x}{p} \right) \mid x \in \Phi'_{M,p,p} \right\} \).

(II) When \( p \equiv 5 \) or 11 \( \mod 12 \), the order of \( \Phi'_{M,p,p} \) is \( \frac{Q(p-1)}{4} \). We have the additional identities

\[
\lambda_1 + \lambda_2 + \lambda_3 - 3\lambda_i = 0 \quad (4 \leq i \leq 3 + 2^\nu).
\]

In particular, all \( \lambda_i \) (\( 4 \leq i \leq 3 + 2^\nu \)) are equal. Substituting (6) into (4), we obtain, for example, \( \mu = \frac{Q}{12} \left[ 3\lambda_1 - \lambda_2(p + 1) - (\lambda_1 - \lambda_2) \right] \).

Since \( \text{g.c.d.}(Q,12) = 4 \) in this case and \( \mu \in \mathbb{Z} \), it follows that \( \lambda_1 - \lambda_2 \in 3\mathbb{Z} \). Putting this into (5), we get \( \mu \equiv \lambda \mod \frac{Q(p-1)}{4} \). Mimicking the method in (I) with \( \lambda_1 = \lambda_2 = 0, \lambda_3 = 3 \) and \( \lambda_i = 1 \) (\( i \geq 4 \)), Theorem 1 follows in this case.

When \( p \equiv 1 \) or 7 \( \mod 12 \), the order of \( \Phi'_{M,p,p} \) is \( \frac{Q(p-1)}{12} \). In this case, \( \text{g.c.d.}(Q,12) = 4 \) too. Instead of (6), we have the additional identities

\[
\lambda_3 - 3\lambda_i = 0 \quad (4 \leq i \leq 3 + 2^\nu).
\]

Substituting into (4) gives \( \mu = \frac{Q}{4} \left[ \lambda_1 - \lambda_2 \left( \frac{p-1}{4} \right) \right] \in \frac{Q}{4}\mathbb{Z} \). Trying with \( \lambda_1 = \lambda_2 = 0, \lambda_3 = 3 \) and \( \lambda_i = 1 \) (\( i \geq 4 \)) shows that \( K' = \left\{ \left( \frac{x}{Q} \right) \mid x \in \langle \frac{Q}{4}g \rangle \right\} \).

(III) This case is very similar to (II), so we simply give a sketch of the argument used.

When \( p \equiv 7, 11 \mod 12 \), the order of \( \Phi'_{M,p,p} \) is \( \frac{Q(p-1)}{6} \). Instead of (6), we have

\[
\lambda_1 + \lambda_2 + \lambda_3 - 2\lambda_i = 0 \quad (4 \leq i \leq 3 + 2^\nu).
\]

Then we split into three cases:

(i) if \( M = 2 \), then \( Q = 3 \) and \( \text{g.c.d.}(Q,12) = 3 \);
(ii) if \( M = q^r \) or \( 2q^r \) (\( q \equiv 1 \mod 4 \) is a prime), then \( \text{g.c.d.}(Q,12) = 6 \);
(iii) if \( M \) has at least two odd prime divisors, then \( \text{g.c.d.}(Q,12) = 12 \).
Mimicking (II) gives the desired answer, except for a slight complication in the case (iii).

If $\lambda_1 - \lambda_2 \not\in 2\mathbb{Z}$, then $\mu \equiv \lambda \mod \frac{Q(p-1)}{6}$ and $\mu \in \mathbb{Z}$. If $\lambda_1 - \lambda_2 \in 2\mathbb{Z}$, then $\mu \equiv \lambda + \frac{Q(p-1)}{12} \mod \frac{Q(p-1)}{6}$. This case can indeed occur. For example, take $\lambda_1 = 1$, $\lambda_2 = 0$, $\lambda_3 = 1$, $\lambda_i = 1$ ($i \geq 4$).

When $p \equiv 1, 5 \mod 12$, the order of $\Phi^\#_{M, p}$ is $\frac{Q(p-1)}{12}$. Instead of (7), we have

\[\lambda_3 - 2\lambda_i = 0 \quad (4 \leq i \leq 3 + 2^r).\]

We only need to consider two cases: when $M = 2$ and when $M \neq 2$.

(IV) Again, except for some details, the strategy of proof in this case is similar to that above. Information that differs from above is given in the following table:

<table>
<thead>
<tr>
<th>$p \mod 12$</th>
<th>$\frac{Q(p-1)}{12}$</th>
<th>Additional Identities</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>$\frac{Q(p-1)}{12}$</td>
<td>$\lambda_3 = 2\lambda_i$ (4 ≤ $i \leq 3 + 2^r$) &lt;br&gt; (so $\lambda_i = 3z, \lambda_j = 2z$ for some $z \in \mathbb{Z}$)</td>
</tr>
<tr>
<td>5</td>
<td>$\frac{Q(p-1)}{4}$</td>
<td>$\lambda_3 = 2\lambda_i$ (4 ≤ $i \leq 3 + 2^r$) &lt;br&gt; $\lambda_1 + \lambda_2 + \lambda_3 = 3\lambda_j$ (4 ≤ $i \leq 3 + 2^r$)</td>
</tr>
<tr>
<td>7</td>
<td>$\frac{Q(p-1)}{6}$</td>
<td>$\lambda_1 + \lambda_2 + \lambda_3 = 2\lambda_i$ (4 ≤ $i \leq 3 + 2^r$) &lt;br&gt; $\lambda_3 = 3\lambda_j$ (4 + $2^r$ ≤ $j \leq 3 + 2^r$)</td>
</tr>
<tr>
<td>11</td>
<td>$\frac{Q(p-1)}{2}$</td>
<td>$\lambda_1 + \lambda_2 + \lambda_3 = 2\lambda_i = 3\lambda_j$ (4 ≤ $i \leq 3 + 2^r$ &lt; $j \leq 3 + 2^r$) &lt;br&gt; (so $\lambda_i = 3z, \lambda_j = 2z$ for some $z \in \mathbb{Z}$)</td>
</tr>
</tbody>
</table>

When $M = q^r$ ($q \equiv 1 \mod 12$ is a prime), $\text{g.c.d.}(Q, 12) = 2$. Otherwise, $\text{g.c.d.}(Q, 12) = 4$.

This completes the proof of Theorem 1.

2. THE PART OF THE SHIMURA SUBGROUP ON THE CONNECTED COMPONENT

We continue to let $M > 1$ be an integer and let $p \geq 5$ be a prime not dividing $M$. In this §, we prove Theorem 2. This result is then used to find a lower bound for $K$.

2.1. Extension of the Shimura subgroup to the Néron model. The content of this § is due to Bas Edixhoven.

**Lemma 1.** Let $M > 1$ be an integer and let $p \geq 5$ be a prime not dividing $M$. The Shimura subgroup $\Sigma(Mp)_{\mathbb{Q}_p}$ extends (by the Zariski closure) to a finite subgroup scheme of the Néron model of $J_0(Mp)$ over $\mathbb{Z}_p$.

**Proof.** Since $p \geq 5$, there is at most one extension of $\Sigma(Mp)_{\mathbb{Q}_p}$ to $\mathbb{Z}_p$. There is indeed one such extension, and it is multiplicative, since $\Sigma(Mp)_{\mathbb{Q}_p}$ is the Cartier dual of a constant group scheme. Denote the extension by $\Sigma(Mp)$.

The prime-to-$p$ part of $\Sigma(Mp)_{\mathbb{Q}_p}$ is constant over the maximal unramified extension of $\mathbb{Q}_p$, so it is étale, and hence has finite Zariski closure in $J_0(Mp)$.

Since $\Sigma(Mp)_{\mathbb{Q}_p}$ is of multiplicative type and that $p \geq 5$, its $p$-part has no nontrivial unramified quotient. Since $J_0(Mp)_{\mathbb{Q}_p}$ has semistable reduction and the action of $\text{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ on $J_0(Mp)_{\mathbb{Q}_p}[p]/J_0(Mp)(\mathbb{Z}_p)[p]$ is unramified, an argument analogous to the one in the proof of Lemma 6.2 of [14] shows that the Zariski closure of the $p$-part in $J_0(Mp)$ is finite. \[\square\]
Remark. Let \( N \geq 5 \) be a prime, let \( S = \text{Spec}(\mathbb{Z}) \) and \( S' = \text{Spec}(\mathbb{Z}[\frac{1}{N}]) \). Let \( n = \frac{N-1}{\text{c.c.}(N)} \). As in [11] page 99, let \( X_1(N)_{S'} \to X_0(N)_{S'} \) be the maximal étale extension intermediate to \( X_1(N) \to X_0(N) \), and let \( U \) be the covering group of this étale subcovering. First we note that the definition of the Cartier dual of \( X \).

2.2. Proof of Theorem 2. Let \( \mathbb{Q}_p^{unr} \) denote the maximal unramified extension of \( \mathbb{Q}_p \). The points of the prime-to-\( p \) part of the Shimura subgroup \( \Sigma(Mp)(\mathbb{Q}_p) \) are defined over \( \mathbb{Q}_p^{unr} \). The “reduction mod \( p \)” yields an isomorphism \( \Sigma(Mp)(\mathbb{Q}_p^{unr})(\mathbb{Q}_p) \cong \Sigma(Mp)(\mathbb{Q}_p)(\mathbb{Q}_p) \) (cf. [4], Appendix). Similarly, we have isomorphisms \( \Sigma(M)(\mathbb{Q}_p^{unr})(\mathbb{Q}_p) \cong \Sigma(M)(\mathbb{Q}_p)(\mathbb{Q}_p) \) and \( \Sigma(p)(\mathbb{Q}_p^{unr}) \cong \Sigma(p)(\mathbb{Q}_p) \).

We recall from a special case of Theorem 10 of [7] that there is an isomorphism

\[ \Sigma(M)(\mathbb{Q})^{(6p)} \times \Sigma(p)(\mathbb{Q})^{(6p)} \cong \Sigma(M)(\mathbb{Q})^{(6p)}, \]

obtained from the degeneracy maps. This isomorphism is invariant under the action of \( \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \). Working over extensions of \( \mathbb{Q}_p \), we get

\[ \Sigma(M)(\mathbb{Q}_p^{unr})^{(6p)} \times \Sigma(p)(\mathbb{Q}_p^{unr})^{(6p)} \cong \Sigma(M)(\mathbb{Q}_p^{unr})^{(6p)}, \]

and hence

\[ \Sigma(M)(\mathbb{F}_p)^{(6p)} \times \Sigma(p)(\mathbb{F}_p)^{(6p)} \cong \Sigma(M)(\mathbb{F}_p)^{(6p)} \]

Since \( J_0(M) \) has good reduction mod \( p \), we have a commutative diagram

\[
\begin{array}{c}
\Sigma(M)(\mathbb{F}_p)^{(6p)} \times \Sigma(p)(\mathbb{F}_p)^{(6p)} \\
\downarrow \\
\Phi_{M,p} \times \Phi_{M,p}
\end{array}
\]

(11)

Theorem 2 follows upon combining Theorem 1, (10), (11) and Proposition 11.9 of [11].

2.3. Proof of Theorem 3. The degeneracy maps \( v_1^*, \ldots, v_{p-1}^* : J_0(Mp) \to J_0(Mp') \) are injective and they coincide with one another on \( \Sigma(Mp) \) ([9], Remark after Theorem 5). By the discussion in §2.2, these degeneracy maps induce injections \( v_1^*/\mathbb{F}_p, \ldots, v_{p-1}^*/\mathbb{F}_p : \Sigma(Mp)(\mathbb{F}_p)^{(6p)} \to J_0(Mp')(\mathbb{F}_p) \) and these induced maps are identical. Then there is a commutative diagram

\[
\begin{array}{c}
\Sigma(Mp)(\mathbb{F}_p)^{(6p)} \times \cdots \times \Sigma(Mp)(\mathbb{F}_p)^{(6p)} \\
\downarrow \\
\Phi_{M,p} \times \cdots \times \Phi_{M,p}
\end{array}
\]

(12)

The vertical maps come from the projection of the special fibre of the Néron model onto the group of components.

Theorem 3 now follows from Theorem 2 and the fact that \( v_1^*/\mathbb{F}_p, \ldots, v_{p-1}^*/\mathbb{F}_p \) are identical on \( \Sigma(Mp)(\mathbb{F}_p)^{(6p)} \).

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
3. Applications

We give two examples of applications of the results proved above.

Example 1. Theorem 1 can be used to generalise Theorem 2 of [7].

Proposition 2. Let \( M \) be a positive integer such that \( J_0(M) = 0 \) and let \( p \geq 5 \) be a prime not dividing \( M \). Let \( K_\eta \) be the kernel of \( \eta = v_1^* \times v_2^* : J_0(Mp) \to J_0(Mp^2) \), and let \( K_0 \) be the \( \eta \)-group.

1. For \( M \in \{1, 2, 3, 4, 5, 6, 8, 9, 12, 16, 18\} \), we have \( K_\eta = K_0 \) (cf. [7], Theorem 2).
2. If \( M = 10 \) or 25, then \( K_0 \subseteq K_\eta \) and \( K_0, K_\eta \) are equal up to a 2-group.
3. If \( M = 7 \), then \( K_0 \subseteq K_\eta \) and \( K_0, K_\eta \) are equal up to a 3-group.
4. If \( M = 13 \), then \( K_0 \subseteq K_\eta \) and their prime-to-six parts are equal.

Proof of Proposition 1. An argument similar to the one used in [7] may be repeated here. Since \( K_0 \subseteq K_\eta \) and there is a natural inclusion of \( K_\eta \) into \( K \), it suffices to compare the orders of \( K_0 \) and \( K \). The former is given in [9] while the latter is given by Theorem 1.

Remark. As in [7], Proposition 1 implies the existence of congruence relations between certain weight-2 cusp forms.

Example 2. Using the intersection matrix given in \S 1.2, one can in theory compute the component group \( \Phi_{Mp^2, p} \). We give the example of \( \Phi_{Mp^2, p} \) in the case (I).

It is routine to check that \( \Phi_{Mp^2, p} \) is generated by the images of \( C_0'' - pC_1' + C_2' \) and \( (p - 1)C_1' - C_2' \). Furthermore, it is easy to verify that the \( \mathbb{Z} \)-span of the columns of the intersection matrix of \( J_0(Mp^2) \) in case (I) has a \( \mathbb{Z} \)-basis consisting of \( \left\{ \begin{pmatrix} \frac{Q(p-1)}{Q(p+1)} \\ \frac{Q(p-1)}{Q(p+1)} - \frac{Q(p+1)}{12} \end{pmatrix}, \begin{pmatrix} 0 \\ \frac{Q(p-1)}{Q(p+1)} - \frac{Q(p+1)}{12} \end{pmatrix} \right\} \). It then follows immediately that

Proposition 2. Let \( M, p, Q, \ell \) and \( n_\ell \) be as in Theorem 1. Suppose that both of the following conditions hold:

(i) either \( n_2 > 1 \) or there exists \( \ell \equiv -1 \mod 4 \) that divides \( M \);
(ii) either \( n_3 > 1 \) or there exists \( \ell \equiv -1 \mod 3 \) that divides \( M \).

Then the component group \( \Phi_{Mp^2, p} \) is isomorphic to \( \mathbb{Z}/\frac{Q(p-1)}{12}\mathbb{Z} \oplus \mathbb{Z}/\frac{Q(p+1)}{12}\mathbb{Z} \).

References


Department of Mathematics, National University of Singapore, Singapore 119260, Republic of Singapore.

E-mail address: matlings@nus.edu.sg