PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 126, Number 11, November 1998, Pages 3201–3210
S 0002-9939(98)04592-4

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 $\Phi_{Mp,p}^r \to \Phi_{Mp^r,p}$, where $\Phi_{Mp,p}$ and $\Phi_{Mp^r,p}$ are the component groups of $J_0(Mp)$ and $J_0(Mp^r)$, respectively. This is then used to determine the kernel of the degeneracy map $J_0(Mp)^2 \to J_0(Mp^2)$ 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 $\mathbf{Q}$, and let $J_0(N)$ denote its Jacobian variety, also defined over $\mathbf{Q}$.

For a prime number p, $X_0(N)$ and $J_0(N)$ are also defined over $\mathbf{Q}_p$. When g.c.d.$(p, N) = 1$, $J_0(N)$ has good reduction at p. When p divides N, the special fibre $J_0(N)_{\mathbf{F}_p}$ in the Néron model of $J_0(N)$ over $\mathbf{Z}_p$ is the extension of a finite étale group scheme $\Phi_{N,p}$ by the connected component of identity $J_0(N)^o_{\mathbf{F}_p}$. 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 $\mathbf{Z}_p$. 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 $v_D : X_0(N) \to X_0(N')$ be the degeneracy map induced by $\tau \mapsto D\tau$. This map induces $v_D^* : J_0(N') \to J_0(N)$ and $(v_D)_* : J_0(N) \to J_0(N')$ on the Jacobian varieties. We also use the same notation for the maps they induce on the component groups.

The kernel of $\eta = \prod_{D|N/N'} v_D^*$ 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 η induces on the component groups enables one to have a better control over the kernel of η (cf. *loc. cit.* as well as Theorem 1 and Proposition 1 below).

The kernel K of η 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 g.c.d.$(q, Mp) = 1$, K contains

Received by the editors April 7, 1997.
1991 *Mathematics Subject Classification.* Primary 11G18, 14H40.
Key words and phrases. Modular curves, Jacobians, component groups, degeneracy maps.
It is a pleasure to thank Bas Edixhoven for patiently correcting the author's initial erroneous understanding of some concepts and for the content of §2.1.

$\left\{ \binom{x}{-x} \in \Phi^2_{Mp,p},\ \forall\, x \in \Phi_{Mp,p} \right\}$ ([14], [15]). When $N = p^r$ and $N' = p$, where $p \geq 5$ is a prime, $K = \left\{ \left(\begin{array}{c} x_1 \\ \vdots \\ x_r \end{array} \right) \in \Phi^r_{p,p} \middle| \sum x_i = 0 \right\}$ ([8]). In this paper, we prove

Theorem 1. *Let $M > 1$ be a positive integer with prime power decomposition $M = \prod \ell^{n_\ell}$ and let $p \geq 5$ be a prime not dividing M. Let $Q = \deg(X_0(M)/X_0(1)) = \prod(\ell+1)\ell^{n_\ell - 1}$ and let ν be the number of primes, distinct from 2 and 3, dividing M. Let σ_4 (resp. σ_6) denote the number of points x of $X_0(M)(\overline{\mathbf{F}}_p)$ with $|\mathrm{Aut}(x)| = 4$ (resp. 6). Let $\mathbf{g}$ be the canonical generator of $\Phi'_{Mp,p}$ (see §1.1). Then the kernel K' of the induced map*

$$\eta' = v_1^* \times v_p^* : \Phi'_{Mp,p} \times \Phi'_{Mp,p} \longrightarrow \Phi_{Mp^2,p}.$$

is given in Table 1. In particular, $v_1^*, v_p^* : \Phi'_{Mp,p} \to \Phi_{Mp^2,p}$ 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 $\Phi_{Mp,p}/\Phi'_{Mp,p}$ 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 $\mathbf{Z}/(p-1)\mathbf{Z}$.*

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

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

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

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 $\Sigma(Mp)_{\mathbf{Q}_p}$ is the corresponding subgroup scheme of $J_0(Mp)_{\mathbf{Q}_p}$). Then $\Sigma(Mp)_{\mathbf{Q}_p}$ extends (by the Zariski closure) to a finite subgroup scheme of the Néron model of $J_0(Mp)$ over $\mathbf{Z}_p$ (see §2.1, Lemma 1). We denote the special fibre of this latter group scheme by $\Sigma(Mp)_{\mathbf{F}_p}$. Proposition 11.9 of [11] shows that, for $M = 1$, the scheme-theoretic intersection $\Sigma(p)_{\mathbf{F}_p} \cap J_0(p)^o_{\mathbf{F}_p}$ is the trivial group scheme over $\mathbf{F}_p$.

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 $\Sigma(Mp)^{(6p)}_{\mathbf{F}_p} \to \Phi_{Mp,p}$ is isomorphic to $\Sigma(M)^{(6p)}_{\mathbf{F}_p}$. Equivalently, the scheme-theoretic intersection $\Sigma(Mp)^{(6p)}_{\mathbf{F}_p} \cap J_0(Mp)^o_{\mathbf{F}_p}$ is isomorphic to $\Sigma(M)^{(6p)}_{\mathbf{F}_p}$.*

Let $\tilde{\Phi}_{Mp,p}$ denote the image of $\Sigma(Mp)^{(6p)}_{\mathbf{F}_p}$ in Theorem 2. When $N = Mp^r$ $(r \geq 2)$ and $N' = Mp$, the map η induces another map $\eta : \Phi^r_{Mp,p} \longrightarrow \Phi_{Mp^r,p}$ 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	σ_4	σ_6	p mod 12	K'	$\lvert K'\rvert$
(I)	0	0	$1, 5, 7, 11$	$\left\{\begin{pmatrix} x \\ -x \end{pmatrix} \mid x \in \langle \frac{Q}{12}\mathbf{g}\rangle\right\}$ (if $M \neq 4$)	$p-1$
				$\left\{\begin{pmatrix} x \\ -x \end{pmatrix} \mid x \in \Phi'_{Mp,p}\right\}$ (if $M = 4$)	$\frac{p-1}{2}$
(II)	0	2^ν	$5, 11$	$\left\{\begin{pmatrix} x \\ -x \end{pmatrix} \mid x \in \langle \frac{Q}{4}\mathbf{g}\rangle\right\}$	$p-1$
			$1, 7$	$\left\{\begin{pmatrix} x \\ -x \end{pmatrix} \mid x \in \langle \frac{Q}{4}\mathbf{g}\rangle\right\}$	$\frac{p-1}{3}$
(III)	2^ν	0	$7, 11$	$\left\{\begin{pmatrix} x \\ -x \end{pmatrix} \mid x \in \Phi'_{Mp,p}\right\}$ (if $M = 2$)	$\frac{p-1}{2}$
				$\left\{\begin{pmatrix} x \\ -x \end{pmatrix} \mid x \in \langle \frac{Q}{6}\mathbf{g}\rangle\right\}$ (if $M = q^r$ or $2q^r$, where $q \equiv 1 \bmod 4$ is prime)	$p-1$
				$\left\{\begin{pmatrix} x \\ -x+\frac{Q(p-1)}{12}\mathbf{g} \end{pmatrix} \mid x \in \langle \frac{Q}{12}\mathbf{g}\rangle - \langle \frac{Q}{6}\mathbf{g}\rangle\right\}$ $\cup \left\{\begin{pmatrix} x \\ -x \end{pmatrix} \mid x \in \langle \frac{Q}{6}\mathbf{g}\rangle\right\}$ (otherwise)	$2(p-1)$
			$1, 5$	$\left\{\begin{pmatrix} x \\ -x \end{pmatrix} \mid x \in \Phi'_{Mp,p}\right\}$ (if $M = 2$)	$\frac{p-1}{4}$
				$\left\{\begin{pmatrix} x \\ -x \end{pmatrix} \mid x \in \langle \frac{Q}{6}\mathbf{g}\rangle\right\}$ (if $M \neq 2$)	$\frac{p-1}{2}$
(IV)	2^ν	2^ν	1	$\left\{\begin{pmatrix} x \\ -x \end{pmatrix} \mid x \in \langle \frac{Q}{2}\mathbf{g}\rangle\right\}$	$\frac{p-1}{6}$
			5	$\left\{\begin{pmatrix} x \\ -x \end{pmatrix} \mid x \in \langle \frac{Q}{2}\mathbf{g}\rangle\right\}$ (if $M = q^r$, where $q \equiv 1 \bmod 12$ is prime)	$\frac{p-1}{2}$
				$\left\{\begin{pmatrix} x \\ -x \end{pmatrix} \mid x \in \langle \frac{Q}{4}\mathbf{g}\rangle\right\}$ (otherwise)	$p-1$
			7	$\left\{\begin{pmatrix} x \\ -x \end{pmatrix} \mid x \in \langle \frac{Q}{2}\mathbf{g}\rangle\right\}$ (if $M = q^r$, where $q \equiv 1 \bmod 12$ is prime)	$\frac{p-1}{3}$
				$\left\{\begin{pmatrix} x \\ -x+\frac{Q(p-1)}{12}\mathbf{g} \end{pmatrix} \mid x \in \langle \frac{Q}{4}\mathbf{g}\rangle - \langle \frac{Q}{2}\mathbf{g}\rangle\right\}$ $\cup \left\{\begin{pmatrix} x \\ -x \end{pmatrix} \mid x \in \langle \frac{Q}{2}\mathbf{g}\rangle\right\}$ (otherwise)	$\frac{2(p-1)}{3}$
			11	$\left\{\begin{pmatrix} x \\ -x \end{pmatrix} \mid x \in \langle \frac{Q}{2}\mathbf{g}\rangle\right\}$ (if $M = q^r$, where $q \equiv 1 \bmod 12$ is prime)	$p-1$
				$\left\{\begin{pmatrix} x \\ -x+\frac{Q(p-1)}{4}\mathbf{g} \end{pmatrix} \mid x \in \langle \frac{Q}{4}\mathbf{g}\rangle - \langle \frac{Q}{2}\mathbf{g}\rangle\right\}$ $\cup \left\{\begin{pmatrix} x \\ -x \end{pmatrix} \mid x \in \langle \frac{Q}{2}\mathbf{g}\rangle\right\}$ (otherwise)	$2(p-1)$

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*

$$\left\{ \begin{pmatrix} x_1 \\ \vdots \\ x_r \end{pmatrix} \in \Phi^r_{Mp,p} \;\middle|\; x_i \in \tilde{\Phi}_{Mp,p} \text{ for all } i, \ \sum x_i = 0 \right\}.$$

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 $\Phi_{Mp,p}$ (where $p \geq 5$ is a prime not dividing M) and the canonical cyclic subgroup $\Phi'_{Mp,p}$ 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 $\mathbf{Q}_p$. 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 $X_0(M)_{\mathbf{F}_p}$, glued together at the supersingular points. For each singular point x, let $e(x) \overset{\text{def}}{=} \frac{1}{2}|\mathrm{Aut}(x)|$. A regular minimal model of $X_0(Mp)$ may be obtained by replacing each singular point x with $e(x) > 1$ by a chain of $e(x) - 1$ copies of the projective line $\mathbf{P}^1$. Label these additional components by $C_2, \ldots, C_n$.

Let $L \overset{\text{def}}{=} \oplus_{i=0}^{n} \mathbf{Z}[C_i]$ 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 $\deg : L \to \mathbf{Z}$ be the obvious degree map. Then $\Phi_{Mp,p} = \ker(\deg)/\mathrm{im}(\iota)$.

According to [12] and [14] Theorem 2.4, $\Phi_{Mp,p}$ contains a canonical cyclic subgroup $\Phi'_{Mp,p}$, generated by the image in $\Phi_{Mp,p}$ of $C_0 - C_1 \in L$. We regard this image of $C_0 - C_1$ as the canonical generator $\mathbf{g}$ of $\Phi'_{Mp,p}$. The quotient $\Phi_{Mp,p}/\Phi'_{Mp,p}$ 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 $C'_0, C'_1, \ldots$ (where $C'_0, \ldots, C'_r$ are copies of $X_0(M)_{\mathbf{F}_p}$ and the remaining ones are copies of $\mathbf{P}^1$) and let $L' = \oplus \mathbf{Z}[C'_i]$ be the analogue of L. Similarly, one can define $\iota' : L' \to L'$ and $\deg' : L' \to \mathbf{Z}$ to be the analogues of ι 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

$$\begin{array}{ccccc} L & \xrightarrow{\iota} & L & \xrightarrow{\deg} & \mathbf{Z} \\ \downarrow \pi^*_{\mathrm{div}} & & \downarrow \pi^*_{\deg} & & \downarrow \deg(\pi) \\ L' & \xrightarrow{\iota'} & L' & \xrightarrow{\deg'} & \mathbf{Z}, \end{array} \tag{1}$$

where

(2)

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

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 $X_0(M)_{\mathbf{F}_p}$, 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 $C'_3, \ldots$ 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 α, β and δ.

Case	(II)		(III)		(IV)			
p mod 12	1, 7	5, 11	1, 5	7, 11	1	5	7	11
α	0	$4\cdot 2^\nu$	0	$6\cdot 2^\nu$	0	$4\cdot 2^\nu$	$6\cdot 2^\nu$	$10\cdot 2^\nu$
β	-3	-3	-2	-2	0	0	1	1
δ	0	1	0	1	0	1	0	1

(I) It is the 3×3 matrix

$$\begin{pmatrix} -\frac{Qp(p-1)}{12} & \frac{Q(p-1)}{12} & \frac{Q(p-1)}{12} \\ \frac{Q(p-1)}{12} & -\frac{Qp(p-1)}{12} & \frac{Q(p-1)}{12} \\ \frac{Q(p-1)}{12} & \frac{Q(p-1)}{12} & -\frac{Q}{6} \end{pmatrix}.$$

(II), (III) It is the $(3+2^\nu)\times(3+2^\nu)$ matrix (with α, β, δ given in Table 2)

$$\begin{pmatrix} -\frac{Qp(p-1)+\alpha}{12} & \frac{Q(p-1)-\alpha}{12} & \frac{Q(p-1)-\alpha}{12} & \delta & \cdots & \delta \\ \frac{Q(p-1)-\alpha}{12} & -\frac{Qp(p-1)+\alpha}{12} & \frac{Q(p-1)-\alpha}{12} & \delta & \cdots & \delta \\ \frac{Q(p-1)-\alpha}{12} & \frac{Q(p-1)-\alpha}{12} & -\frac{Q}{6}+\frac{2^\nu}{\beta} & 1 & \cdots & 1 \\ \delta & \delta & 1 & \beta & 0\cdots & 0 \\ \vdots & \vdots & \vdots & 0 & \ddots & \vdots \\ \delta & \delta & 1 & 0 & \cdots & \beta \end{pmatrix}.$$

(IV) It is the $(3+2\cdot 2^\nu)\times(3+2\cdot 2^\nu)$ matrix (with α, β, δ given in Table 2)

$$\begin{pmatrix} -\frac{Qp(p-1)+\alpha}{12} & \frac{Q(p-1)-\alpha}{12} & \frac{Q(p-1)-\alpha}{12} & \beta & \cdots & \beta & \delta & \cdots & \delta \\ \frac{Q(p-1)-\alpha}{12} & -\frac{Qp(p-1)+\alpha}{12} & \frac{Q(p-1)-\alpha}{12} & \beta & \cdots & \beta & \delta & \cdots & \delta \\ \frac{Q(p-1)-\alpha}{12} & \frac{Q(p-1)-\alpha}{12} & -\frac{Q+5\cdot 2^\nu}{6} & 1 & \cdots & 1 & 1 & \cdots & 1 \\ \beta & \beta & 1 & -2 & 0\cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & 0 & \ddots & 0 & \vdots & \vdots & \vdots \\ \beta & \beta & 1 & 0 & \cdots & -2 & 0 & \cdots & 0 \\ \delta & \delta & 1 & 0 & \cdots & 0 & -3 & 0\cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ \delta & \delta & 1 & 0 & \cdots & 0 & 0 & \cdots & -3 \end{pmatrix}.$$

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

$$\mathbf{v} = (p\lambda-\mu, p\mu-\lambda, -(\lambda+\mu), 0, \cdots, 0)^{\mathbf{T}}$$

is a $\mathbf{Z}$-linear combination of the columns of the intersection matrix in §1.2.

Let $\mathbf{c}_i$ denote the i^{th} column of the intersection matrix. Let m be the number of columns in the intersection matrix. Let λ_i $(1 \le i \le m)$ be integers and suppose

$$\mathbf{v} = \lambda_1 \mathbf{c}_1 + \cdots + \lambda_m \mathbf{c}_m. \tag{3}$$

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

$$\mu = \frac{Q}{12}\left[\lambda_3 - \lambda_2(p-1)\right] \tag{4}$$

and

$$\mu - \lambda = \frac{Q(p-1)}{12}(\lambda_1 - \lambda_2). \tag{5}$$

Now we prove Theorem 1 case by case.

(I) In this case, the order of $\Phi'_{Mp,p}$ is $\frac{Q(p-1)}{12}$. Suppose that $M \neq 4$. Then 12 divides Q. From (4), $\mu \in \frac{Q}{12}\mathbf{Z}$. From (5), $\mu \equiv \lambda \bmod \frac{Q(p-1)}{12}$. Therefore the kernel K' is contained in $\left\{ \binom{x}{-x} \mid x \in \langle \frac{Q}{12}\mathbf{g} \rangle \right\}$. 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 $K' = \left\{ \binom{x}{-x} \mid x \in \langle \frac{Q}{12}\mathbf{g} \rangle \right\}$.

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

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

$$\lambda_1 + \lambda_2 + \lambda_3 - 3\lambda_i = 0 \qquad (4 \le i \le 3 + 2^{\nu}). \tag{6}$$

In particular, all λ_i $(4 \le i \le 3 + 2^{\nu})$ are equal. Substituting (6) into (4), we obtain, for example, $\mu = \frac{Q}{12}\left[3\lambda_4 - \lambda_2(p+1) - (\lambda_1 - \lambda_2)\right]$.

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

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

$$\lambda_3 - 3\lambda_i = 0 \qquad (4 \le i \le 3 + 2^{\nu}). \tag{7}$$

Substituting into (4) gives $\mu = \frac{Q}{4}\left[\lambda_4 - \lambda_2\left(\frac{p-1}{3}\right)\right] \in \frac{Q}{4}\mathbf{Z}$. Trying with $\lambda_1 = \lambda_2 = 0$, $\lambda_3 = 3$ and $\lambda_i = 1$ $(i \ge 4)$ shows that $K' = \left\{ \binom{x}{-x} \mid x \in \langle \frac{Q}{4}\mathbf{g} \rangle \right\}$.

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

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

$$\lambda_1 + \lambda_2 + \lambda_3 - 2\lambda_i = 0 \qquad (4 \le i \le 3 + 2^{\nu}). \tag{8}$$

Then we split into three cases:

(i) if $M = 2$, then $Q = 3$ and g.c.d.$(Q, 12) = 3$;
(ii) if $M = q^r$ or $2q^r$ ($q \equiv 1 \bmod 4$ is a prime), then g.c.d.$(Q, 12) = 6$;
(iii) if M has at least two odd prime divisors, then g.c.d.$(Q, 12) = 12$.

Mimicking (II) gives the desired answer, except for a slight complication in the case (iii).

If $\lambda_1 - \lambda_2 \in 2\mathbf{Z}$, then $\mu \equiv \lambda \bmod \frac{Q(p-1)}{6}$ and $\mu \in \mathbf{Z}$. If $\lambda_1 - \lambda_2 \notin 2\mathbf{Z}$, then $\mu \equiv \lambda + \frac{Q(p-1)}{12} \bmod \frac{Q(p-1)}{6}$. This case can indeed occur. For example, take $\lambda_1 = 1$, $\lambda_2 = 0$, $\lambda_3 = 1$, $\lambda_i = 1$ $(i \geq 4)$.

When $p \equiv 1, 5 \bmod 12$, the order of $\Phi'_{Mp,p}$ is $\frac{Q(p-1)}{12}$. Instead of (7), we have

$$\lambda_3 - 2\lambda_i = 0 \qquad (4 \leq i \leq 3 + 2^\nu). \tag{9}$$

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:

p mod 12	$\lvert\Phi'_{Mp,p}\rvert$	Additional Identities
1	$\frac{Q(p-1)}{12}$	$\lambda_3 = 2\lambda_i = 3\lambda_j \quad (4 \leq i \leq 3 + 2^\nu < j \leq 3 + 2 \cdot 2^\nu)$ (so $\lambda_i = 3z$, $\lambda_j = 2z$ for some $z \in \mathbf{Z}$)
5	$\frac{Q(p-1)}{4}$	$\lambda_3 = 2\lambda_i \quad (4 \leq i \leq 3 + 2^\nu)$ $\lambda_1 + \lambda_2 + \lambda_3 = 3\lambda_j \quad (4 + 2^\nu \leq j \leq 3 + 2 \cdot 2^\nu)$
7	$\frac{Q(p-1)}{6}$	$\lambda_1 + \lambda_2 + \lambda_3 = 2\lambda_i \quad (4 \leq i \leq 3 + 2^\nu)$ $\lambda_3 = 3\lambda_j \quad (4 + 2^\nu \leq j \leq 3 + 2 \cdot 2^\nu)$
11	$\frac{Q(p-1)}{2}$	$\lambda_1 + \lambda_2 + \lambda_3 = 2\lambda_i = 3\lambda_j \quad (4 \leq i \leq 3 + 2^\nu < j \leq 3 + 2 \cdot 2^\nu)$ (so $\lambda_i = 3z$, $\lambda_j = 2z$ for some $z \in \mathbf{Z}$)

When $M = q^r$ ($q \equiv 1 \bmod 12$ is a prime), g.c.d.$(Q, 12) = 2$. Otherwise, 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 $\Sigma(Mp)_{\mathbf{Q}_p}$ extends (by the Zariski closure) to a finite subgroup scheme of the Néron model of $J_0(Mp)$ over $\mathbf{Z}_p$.*

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

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

Since $\Sigma(Mp)_{\mathbf{Q}_p}$ is of multiplicative type and that $p \geq 5$, its p-part has no nontrivial unramified quotient. Since $J_0(Mp)_{\mathbf{Q}_p}$ has semistable reduction and the action of $\mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$ on $J_0(Mp)(\overline{\mathbf{Q}}_p)[p]/J_0(Mp)(\overline{\mathbf{Z}}_p)[p]$ 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. □

Remark. Let $N \geq 5$ be a prime, let $S = \operatorname{Spec}(\mathbf{Z})$ and $S' = \operatorname{Spec}\left(\mathbf{Z}\left[\frac{1}{N}\right]\right)$. Let $n = \frac{N-1}{\text{g.c.d.}(N-1,12)}$. As in [11] page 99, let $X_2(N)_{S'} \to X_0(N)_{S'}$ 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 U in *loc. cit.* should be $U_S^* = Hom_S(U, \mu_n)$, not $Hom_S(U, \mu_N)$, as U is cyclic of order n. It follows immediately that U^* is *not* étale over S' as it is not étale at primes dividing n, contrary to what is claimed in the proof of Proposition 11.6 of [11].

However, the conclusion of Proposition 11.6 of [11] is still true. Over S', U acts freely on $X_1(N)_{S'}$, so we have an isomorphism between $U_{S'}^*$ and the kernel of $J_0(N)_{S'} \to J_1(N)_{S'}$. At N, U^* is étale, so the Néron property of $J_0(N)_S$ (as claimed in the proof given in [11]) works.

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

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

$$\Sigma(M)(\overline{\mathbf{Q}})^{(6p)} \times \Sigma(p)(\overline{\mathbf{Q}})^{(6p)} \simeq \Sigma(Mp)(\overline{\mathbf{Q}})^{(6p)},$$

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

$$\Sigma(M)(\mathbf{Q}_p^{unr})^{(6p)} \times \Sigma(p)(\mathbf{Q}_p^{unr})^{(6p)} \simeq \Sigma(Mp)(\mathbf{Q}_p^{unr})^{(6p)},$$

and hence

$$\Sigma(M)(\overline{\mathbf{F}}_p)^{(6p)} \times \Sigma(p)(\overline{\mathbf{F}}_p)^{(6p)} \simeq \Sigma(Mp)(\overline{\mathbf{F}}_p)^{(6p)}. \tag{10}$$

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

$$\begin{array}{ccc} \Sigma(M)(\overline{\mathbf{F}}_p)^{(6p)} \times \Sigma(p)(\overline{\mathbf{F}}_p)^{(6p)} & \longrightarrow & \Sigma(Mp)(\overline{\mathbf{F}}_p)^{(6p)} \\ \downarrow & & \downarrow \\ 0 \times \Phi'_{p,p} & \longrightarrow & \Phi_{Mp,p}. \end{array} \tag{11}$$

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

2.3. **Proof of Theorem 3.** The degeneracy maps $v_1^*, \ldots, v_{p^{r-1}}^* : J_0(Mp) \to J_0(Mp^r)$ 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 $v_{1/\mathbf{F}_p}^*, \ldots, v_{p^{r-1}/\mathbf{F}_p}^* : \Sigma(Mp)(\overline{\mathbf{F}}_p)^{(6p)} \to J_0(Mp^r)(\overline{\mathbf{F}}_p)$ and these induced maps are identical. Then there is a commutative diagram

$$\begin{array}{ccc} \Sigma(Mp)(\overline{\mathbf{F}}_p)^{(6p)} \times \cdots \times \Sigma(Mp)(\overline{\mathbf{F}}_p)^{(6p)} & \xrightarrow{\eta} & J_0(Mp^r)(\overline{\mathbf{F}}_p) \\ \downarrow & & \downarrow \\ \Phi_{Mp,p} \times \cdots \times \Phi_{Mp,p} & \xrightarrow{\eta} & \Phi_{Mp^r,p}. \end{array}$$

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 $v_{1/\mathbf{F}_p}^*, \ldots, v_{p^{r-1}/\mathbf{F}_p}^*$ are identical on $\Sigma(Mp)(\overline{\mathbf{F}}_p)^{(6p)}$.

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 1. *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_η be the kernel of $\eta = v_1^* \times v_p^* : J_0(Mp)^2 \longrightarrow J_0(Mp^2)$, and let $K_0 \stackrel{\text{def}}{=} \left\{ \binom{x}{-x} \mid x \in \Sigma(Mp) \right\}$. Then*

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_η are equal up to a 2-group.

3. If $M = 7$, then $K_0 \subseteq K_\eta$ and K_0, K_η 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_η 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 §1.2, one can in theory compute the component group $\Phi_{Mp^r,p}$. 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 $\mathbf{Z}$-span of the columns of the intersection matrix of $J_0(Mp^2)$ in case (I) has a $\mathbf{Z}$-basis consisting of $\left\{ \begin{pmatrix} \frac{Q(p-1)}{12} \\ -\frac{Qp(p-1)}{12} \\ \frac{Q(p-1)}{12} \end{pmatrix}, \begin{pmatrix} 0 \\ \frac{(p+1)Q(p-1)}{12} \\ -\frac{Q(p+1)}{12} \end{pmatrix} \right\}$. It then follows immediately that

Proposition 2. *Let M, p, Q, ℓ and n_ℓ be as in Theorem 1. Suppose that both of the following conditions hold:*

(i) either $n_2 > 1$ or there exists $\ell \equiv -1 \bmod 4$ that divides M;

(ii) either $n_3 > 1$ or there exists $\ell \equiv -1 \bmod 3$ that divides M.

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

References

1. P. Deligne, M. Rapoport, Les schémas de modules de courbes elliptiques, *in* "Modular Functions of One Variable II", Lecture Notes in Math. **349**, 1973, pp. 143–316. MR **49:**2762
2. B. 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. MR **92k:**11059
3. B. Edixhoven, Minimal resolution and stable reduction of $X_0(N)$. *Ann. Inst. Fourier* **40** (1990), 31–67. MR **92f:**11080
4. N. Katz, Galois properties of torsion points on abelian varieties. *Invent. Math.* **62** (1981), 481–502. MR **82d:**14025
5. N. Katz, B. Mazur, "Arithmetic Moduli of Elliptic Curves". Annals of Mathematics Studies, Study 108, 1985. MR **86i:**11024
6. S. Ling, Congruences between cusp forms and the geometry of Jacobians of modular curves. *Math. Ann.* **295** (1993), 111–133. MR **94a:**11063
7. S. Ling, Shimura subgroups and degeneracy maps. *J. Number Theory* **54** (1995), 39–59. MR **96h:**11058

8. S. Ling, On the **Q**-rational cuspidal subgroup and the component group of $J_0(p^r)$. *Israel J. Math.* **99** (1997), 29–54. CMP 97:11
9. S. Ling, J. Oesterlé, The Shimura subgroup of $J_0(N)$. *Astérisque* **196-197** (1991), 171–203. MR **93b:**14038
10. D.J. Lorenzini, Torsion points on the modular Jacobian $J_0(N)$. *Comp. Math.* **96** (1995), 149–172. MR **96b:**11076
11. B. Mazur, Modular curves and the Eisenstein ideal. *Publ. Math. I.H.E.S.* **47** (1978), 33–186. MR **80c:**14015
12. M. Raynaud, Jacobienne des courbes modulaires et opérateurs de Hecke. *Astérisque* **196–197** (1991), 9–25. MR **93b:**11077
13. K. Ribet, Congruence relations between modular forms, *in* "Proceedings, International Congress of Mathematicians,", pp. 503–514, PWN, Warsaw, 1984. MR **87c:**11045
14. K. Ribet, On modular representations of Gal($\overline{\mathbf{Q}}/\mathbf{Q}$) arising from modular forms. *Invent. Math.* **100** (1990), 431–476. MR **91g:**11066
15. K. Ribet, On the component groups and the Shimura subgroup of $J_0(N)$, *in* "Séminaire de théorie des nombres de Bordeaux," 1987–88, exposé 6. MR **91b:**11070

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

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