RELATIONS BETWEEN JACOBIANS OF MODULAR CURVES OF LEVEL p^2

IMIN CHEN, BART DE SMIT, AND MARTIN GRABITZ

Abstract. We derive a relation between induced representations on the group $\mathrm{GL}_2(\mathbb{Z}/p^2\mathbb{Z})$ which implies a relation between the jacobians of certain modular curves of level p^2. The motivation for the construction of this relation is the determination of the applicability of Mazur's method to the modular curve associated to the normalizer of a non-split Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}/p^2\mathbb{Z})$.

Nous établissons une relation entre les représentations induites sur le groupe $\mathrm{GL}_2(\mathbb{Z}/p^2\mathbb{Z})$ qui implique une relation entre les jacobiennes des certaines courbes modulaires de niveaux p^2. La motivation de la construction de cette relation est la détermination de l'applicabilité de la méthode de Mazur à la courbe modulaire associée au normalisateur d'un subgroupe Cartan non-deployé de $\mathrm{GL}_2(\mathbb{Z}/p^2\mathbb{Z})$.

1. Introduction

Let $X(p^n)$ denote the compactified modular curve classifying elliptic curves with full level p^n structure where p is an odd prime. This modular curve is defined over $\mathbb{Q}$ and has a right group action of $\mathrm{GL}_2(\mathbb{Z}/p^n\mathbb{Z})$ which is also defined over $\mathbb{Q}$.

Consider the following subgroups of $\mathrm{GL}_2(\mathbb{Z}/p^n\mathbb{Z})$, which we refer to as a non-split Cartan subgroup, and the normalizer of a non-split Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}/p^n\mathbb{Z})$, respectively, where $\epsilon \in (\mathbb{Z}/p^n\mathbb{Z})^\times$ is a non-square.

$$T' = T'(p^n) = \left\{ \begin{pmatrix} a & b\epsilon \\ b & a \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}/p^n\mathbb{Z}) \right\}$$
$$N' = N'(p^n) = \left\{ \begin{pmatrix} a & b\epsilon \\ b & a \end{pmatrix}, \begin{pmatrix} a & b\epsilon \\ -b & -a \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}/p^n\mathbb{Z}) \right\}$$

Let $X_{N'}(p^n) = X(p^n)/N'$ be the quotient of $X(p^n)$ by the subgroup N'. This modular curve is defined over $\mathbb{Q}$ and classifies pairs $(E, [\phi])$ where $E|K$ is an elliptic curve defined over K together with an N'-equivalence class of isomorphisms $\phi : \mathbb{Z}/p^n\mathbb{Z} \times \mathbb{Z}/p^n\mathbb{Z} \to E[p^n](\overline{K})$ defined over K. In particular, a K-rational point on $X_{N'}(p^n)$ corresponds to an $E|K$ (up to $\overline{K}$ isomorphism) whose mod p^n representation with respect to the basis ϕ has image lying in N' ([3], Chapter 7).

A long standing question of Serre [9] asks whether the mod p representations of non-CM elliptic curves over $\mathbb{Q}$ are surjective if $p > c_{\mathbb{Q}}$ is greater than some constant $c_{\mathbb{Q}}$ (e.g. $c_{\mathbb{Q}} = 37$?). This can be translated into the question whether the $\mathbb{Q}$-rational points of certain modular curves all arise from CM elliptic curves and cusps if $p > c_{\mathbb{Q}}$.

Date: 25 September 2002.

Research partially supported by NSERC and PRG grants.

One of the modular curves involved in Serre's question is $X_{N'}(p)$. Unfortunately, the method used by Mazur [5] to determine the $\mathbb{Q}$-rational points on more conventional modular curves do not seem to apply directly to $X_{N'}(p)$ as its jacobian conjecturally does not have any non-trivial rank 0 quotients, a vital starting condition for the method. One might therefore ask if the jacobians of the modular curves $X_{N'}(p^n)$ have non-trivial rank 0 quotients for some $n > 1$, for instance $n = 2$.

In this note, we derive a relation of jacobians (see Theorem 3.1) which relates the jacobian of $X_{N'}(p^2)$ to that of more conventional modular curves using the representation theory of $\mathrm{GL}_2(\mathbb{Z}/p^2\mathbb{Z})$. This should make it possible to determine whether $J_{N'}$ has any non-trivial rank 0 quotients [1].

2. Relations between induced representations

Let p be an odd prime. Consider the local ring $R = \mathbb{Z}/p^2\mathbb{Z}$ with maximal ideal $\mathfrak{m} = p\mathbb{Z}/p^2\mathbb{Z}$. In what follows, conjugation by h of an element g will mean hgh^{-1}.

Lemma 2.1. *Let $g \in \mathrm{GL}_2(R)$ and suppose ϵ is a fixed non-square in $R^\times$. Then g is conjugate to one of the following types of matrices below. Moreover, the matrices as enumerated below represent distinct conjugacy classes in $\mathrm{GL}_2(R)$ (if H is a quotient of $R^\times$, we write $\beta \in H$ to mean the β are chosen from a complete set of inequivalent representatives in $R^\times$ for H).*

$$\begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix} \text{ for } \alpha \in R^\times \qquad (\textit{Type I})$$

$$\begin{pmatrix} \alpha & \epsilon\beta \\ \beta & \alpha \end{pmatrix} \text{ for } \alpha \in R, \beta \in R^\times / \{\pm 1\} \qquad (\textit{Type } T')$$

$$\begin{pmatrix} \alpha & 1 \\ 0 & \alpha \end{pmatrix} \text{ for } \alpha \in R^\times \qquad (\textit{Type B})$$

$$\begin{pmatrix} \alpha & 0 \\ 0 & \delta \end{pmatrix} \text{ for } \{\alpha, \delta\} \subset R^\times \text{ and } \alpha \not\equiv \delta \pmod{\mathfrak{m}} \qquad (\textit{Type T})$$

$$\begin{pmatrix} \alpha & p\epsilon\beta \\ \beta & \alpha \end{pmatrix} \text{ for } \alpha \in R^\times, \beta \in (R/\mathfrak{m})^\times / \{\pm 1\} \qquad (\textit{Type } RT')$$

$$\begin{pmatrix} \alpha & p\beta \\ \beta & \alpha \end{pmatrix} \text{ for } \alpha \in R^\times, \beta \in (R/\mathfrak{m})^\times / \{\pm 1\} \qquad (\textit{Type RT})$$

$$\begin{pmatrix} \alpha & p\epsilon\beta^2 \\ p & \alpha \end{pmatrix} \text{ for } \alpha \in R^\times, \beta \in (R/\mathfrak{m})^\times / \{\pm 1\} \qquad (\textit{Type } RI')$$

$$\begin{pmatrix} \alpha & 0 \\ p & \alpha \end{pmatrix} \text{ for } \alpha \in R^\times \qquad (\textit{Type RB})$$

$$\begin{pmatrix} \alpha & p\beta^2 \\ p & \alpha \end{pmatrix} \text{ for } \alpha \in R^\times, \beta \in (R/\mathfrak{m})^\times / \{\pm 1\} \qquad (\textit{Type RI})$$

Proof. We give an explicit recipe for determining the conjugacy type of a general element in $\mathrm{GL}_2(R)$. Note that one can verify the list above is complete by counting elements (see Table 1). The general framework for this calculation can be described as follows. Let

$$g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(R)$$

be given and let

$$P_g(X) = \det(XI - A) = X^2 - tX + n$$

be the characteristic polynomial of g, where t and n are the trace and determinant of g, respectively. Suppose R is a subring of S and $P_g(\lambda) = 0$ for $\lambda \in S$. Then $gv = \lambda v$ where

$$v = \begin{pmatrix} \lambda - d \\ c \end{pmatrix},$$

that is, v is an eigenvector for g with eigenvalue λ. Now, the roots of $P_g(X)$ are formally given by the expression

$$\lambda = \frac{t \pm \sqrt{\Delta}}{2}$$

where $\Delta = t^2 - 4n$.

Suppose $\Delta = u^2$ where $u \in R^\times$. Then λ is one of $\lambda_1 = \frac{t+u}{2}, \lambda_2 = \frac{t-u}{2}$. Since $n = \lambda_1\lambda_2$, it follows that $\lambda_1, \lambda_2 \in R^\times$. Note that $\lambda_1 \not\equiv \lambda_2 \in R/\mathfrak{m}$ are distinct modulo $\mathfrak{m}$ (we are assuming p is odd). It is not possible for the reduction $\bar{g}$ modulo $\mathfrak{m}$ to be a scalar in $\mathrm{GL}_2(R/\mathfrak{m})$ for then Δ would not be a unit. Thus, either one of $b, c \in R^\times$ or both $b, c \equiv 0 \pmod{\mathfrak{m}}$ but $a \not\equiv d \pmod{\mathfrak{m}}$. In the latter case, conjugation by the matrix

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

gives a matrix with one of $b, c \in R^\times$. Conjugating by the matrix

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

if necessary, we may assume that $c \in R^\times$. The vectors

$$v_1 = \begin{pmatrix} \lambda_1 - d \\ c \end{pmatrix}, v_2 = \begin{pmatrix} \lambda_2 - d \\ c \end{pmatrix}$$

are eigenvectors of g with eigenvalue λ_1, λ_2, respectively. It follows that g is conjugate to the matrix

$$\begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$$

by the matrix

$$P = \begin{pmatrix} v_1 \mid v_2 \end{pmatrix}^{-1}$$

which lies in $GL_2(R)$ since its determinant is $c(\lambda_1 - \lambda_2) \in R^\times$.

Suppose that $\Delta = \delta u^2$ where δ is one of ϵ, p, or $p\epsilon$, and $u \in R^\times$. First note that one of $b, c \in R^\times$, for if both are not, then Δ would be a non-zero square modulo $\mathfrak{m}$ or the reduction $\bar{g}$ modulo $\mathfrak{m}$ would be a scalar. In the latter case, go to case (2) of next paragraph. In the former case, conjugation by the matrix

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

allows us to assume that $c \not\equiv 0 \pmod{\mathfrak{m}}$. Then λ is one of $\lambda_1 = \frac{t+u\sqrt{\delta}}{2}, \lambda_2 = \frac{t-u\sqrt{\delta}}{2}$ lying in the ring $R[\sqrt{\delta}] = R[X]/(X^2-\delta) = R \cdot 1 \oplus R \cdot X$. The vectors

$$v_1 = \begin{pmatrix} \lambda_1 - d \\ c \end{pmatrix}, v_2 = \begin{pmatrix} \lambda_2 - d \\ c \end{pmatrix}$$

are eigenvectors of g with eigenvalue λ_1, λ_2, respectively. Conjugating g by the matrix

$$\begin{pmatrix} c & d - t/2 \\ 0 & u/2 \end{pmatrix}$$

gives us a matrix g' for which

$$v_1' = \begin{pmatrix} \sqrt{\delta} \\ 1 \end{pmatrix}, v_2' = \begin{pmatrix} -\sqrt{\delta} \\ 1 \end{pmatrix}$$

are eigenvectors with eigenvalues λ_1, λ_2, respectively. By solving the equation

$$g' v_i' = \lambda_i v_i'$$

we see the resulting matrix must therefore be

$$\begin{pmatrix} t/2 & \delta u/2 \\ u/2 & t/2 \end{pmatrix}$$

which is of the form

$$\begin{pmatrix} \alpha & \delta\beta \\ \beta & \alpha \end{pmatrix}$$

where $\alpha \in R, \beta \in R^\times$.

Suppose that $\Delta = 0$. The reduction $\bar{g}$ modulo $\mathfrak{m}$ is therefore conjugate to one of

$$\begin{pmatrix} t/2 & 1 \\ 0 & t/2 \end{pmatrix}, \begin{pmatrix} t/2 & 0 \\ 0 & t/2 \end{pmatrix}$$

in $\mathrm{GL}_2(R/\mathfrak{m})$. Thus, we may assume without loss of generality that one of the following holds:

(1) $a \equiv d \pmod{\mathfrak{m}}, c \equiv 0 \pmod{\mathfrak{m}}, b \equiv 1 \pmod{\mathfrak{m}}$
(2) $a \equiv d \pmod{\mathfrak{m}}, b \equiv c \equiv 0 \pmod{\mathfrak{m}}$

In case (1), we see that $\Delta = (a+d)^2 - 4(ad-bc) = (a-d)^2 + 4bc$. Since $\Delta = 0$ in R, and $b \in R^\times$, it follows that in fact $c = 0$ in R. Thus,

$$g = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}.$$

Conjugating by

$$\begin{pmatrix} 1 & 0 \\ 0 & b \end{pmatrix},$$

we may assume

$$g = \begin{pmatrix} a & 1 \\ 0 & d \end{pmatrix}.$$

Finally, conjugating by

$$\begin{pmatrix} 1 & 1 \\ \frac{a-d}{2} & \frac{a-d}{2}+1 \end{pmatrix}$$

shows that g is conjugate to

$$\begin{pmatrix} \frac{a+d}{2} & 1+d-a \\ 0 & \frac{a+d}{2} \end{pmatrix}$$

which conjugate to a matrix of the form

$$\begin{pmatrix} \alpha & 1 \\ 0 & \alpha \end{pmatrix}$$

where $\alpha \in R^{\times}$.

In case (2), we either have $b = c = 0$ in R or one of $b, c \neq 0$ in R. In the former subcase, g is a scalar in $\mathrm{GL}_2(R)$ or g is of the form

$$\begin{pmatrix} a+p\beta & 0 \\ 0 & a-p\beta \end{pmatrix}$$

which is conjugate to

$$\begin{pmatrix} a & p\beta^2 \\ p & a \end{pmatrix}$$

by the matrix

$$\begin{pmatrix} 1 & 1 \\ \beta^{-1} & -\beta^{-1} \end{pmatrix}.$$

In the latter subcase, write $c = pc', b = pb'$. Without loss of generality, $c' \in R^{\times}$. Conjugating by

$$\begin{pmatrix} 1 & 0 \\ 0 & {c'}^{-1} \end{pmatrix},$$

we may now assume

$$g = \begin{pmatrix} a & pb'' \\ p & d \end{pmatrix}$$

where $b'' = b'c'$. Since $d = a + px$ for some $x \in R$, conjugation by

$$\begin{pmatrix} 1 & x/2 \\ 0 & 1 \end{pmatrix}$$

shows that g is conjugate to

$$\begin{pmatrix} \frac{a+d}{2} & pb_0 \\ p & \frac{a+d}{2} \end{pmatrix}$$

where $b_0 = (b'c' + x^2/4)$ which is of the form

$$\begin{pmatrix} \alpha & p\beta \\ p & \alpha \end{pmatrix}$$

where $\alpha \in R^\times, \beta \in R$.

We have thus shown every $g \in \mathrm{GL}_2(R)$ is conjugate to one of the listed types of matrices. Matrices of type I, B, RI', RB, RI have discriminant $0 \in R$, while matrices of type T', T, RT', RT, have discriminant $\epsilon\beta^2$, $(\alpha-\delta)^2$, $p\epsilon\beta^2$, $p\beta^2$, respectively. Thus, matrices of different types are not conjugate, except possibly for matrices from the former group. Matrices of type I, B, RI', RB, RI are mutually non-conjugate because the centralizers of matrices of each of these types have differing orders (see next Lemma 2.2). Finally, matrices within each type as enumerated are not conjugate by consideration of trace and determinant, except for the types RI', RB, RI, which are mutually non-conjugate by a matrix calculation. □

Lemma 2.2. *With notation as in Lemma 2.1, the order of the centralizer in $G = \mathrm{GL}_2(R)$ of an element of g only depends on the type of conjugacy class $I, T', B, T, RT', RT, RI', RB, RI$. For the representatives given in Lemma 2.1, the centralizers are given explicitly as follows.*

$$\begin{aligned}
C_G(I) &= \mathrm{GL}_2(R) \\
C_G(T') &= \left\{ \begin{pmatrix} a & b\epsilon \\ b & a \end{pmatrix} \mid (a,b) \not\equiv (0,0) \pmod{\mathfrak{m}} \right\} \\
C_G(B) &= \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \mid a \in R^\times, b \in R \right\} \\
C_G(T) &= \left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \mid a, d \in R^\times \right\} \\
C_G(RT') &= \left\{ \begin{pmatrix} a & bp\epsilon \\ b & a \end{pmatrix} \mid a \in R^\times, b \in R \right\} \\
C_G(RT) &= \left\{ \begin{pmatrix} a & bp \\ b & a \end{pmatrix} \mid a \in R^\times, b \in R \right\} \\
C_G(RI') &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a \equiv d \pmod{\mathfrak{m}}, b \equiv c\epsilon\beta^2 \pmod{\mathfrak{m}}, a^2 - c^2\epsilon\beta^2 \not\equiv 0 \pmod{\mathfrak{m}} \right\} \\
C_G(RB) &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, d \in R^\times, b \in R, a \equiv d \pmod{\mathfrak{m}}, b \equiv 0 \pmod{\mathfrak{m}} \right\} \\
C_G(RI) &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a \equiv d \pmod{\mathfrak{m}}, b \equiv c\beta^2 \pmod{\mathfrak{m}}, a^2 - c^2\beta^2 \not\equiv 0 \pmod{\mathfrak{m}} \right\}
\end{aligned}$$

Proof. This can be verified by a direct matrix calculation. □

The information contained in the following Table 1 is a useful summary of conjugacy information for later computational purposes.

Table 1. Conjugacy information

conjugacy type	number of this type	size of centralizer	size of conjugacy class
I	$p(p-1)$	$p^4 \cdot (p^2-1)(p^2-p)$	1
T'	$p^2 \cdot (p^2-p)/2$	$p^2 \cdot (p^2-1)$	$p^2(p^2-p)$
B	$p(p-1)$	$p(p-1) \cdot p^2$	$p^2(p^2-1)$
T	$p^2 \cdot (p-1)(p-2)/2$	$p^2(p-1)^2$	$p^2(p^2+p)$
RT'	$p(p-1) \cdot (p-1)/2$	$p(p-1) \cdot p^2$	$p^2(p^2-1)$
RT	$p(p-1) \cdot (p-1)/2$	$p(p-1) \cdot p^2$	$p^2(p^2-1)$
RI'	$p(p-1) \cdot (p-1)/2$	$p^4 \cdot (p^2-1)$	p^2-p
RB	$p(p-1)$	$p^4 \cdot (p-1)p$	p^2-1
RI	$p(p-1) \cdot (p-1)/2$	$p^4 \cdot (p-1)^2$	p^2+p

Let $\pi : \mathrm{GL}_2(R) \to \mathrm{GL}_2(R/\mathfrak{m})$ be the reduction mod $\mathfrak{m}$ map. Let $T'(p)$ be a non-split Cartan subgroup of $\mathrm{GL}_2(R/\mathfrak{m})$. Let $T(p)$ be a split Cartan subgroup of $\mathrm{GL}_2(R/\mathfrak{m})$. Let $B(p)$ be a Borel subgroup of $\mathrm{GL}_2(R/\mathfrak{m})$. Consider the following subgroups of $\mathrm{GL}_2(R)$:

$$
\begin{aligned}
B' &= \left\{ \begin{pmatrix} a & bp \\ 0 & d \end{pmatrix} : a, d \in R^\times, b \in R \right\} \\
\overline{B} &= \pi^{-1}(B(p)) \\
T' &= \left\{ \begin{pmatrix} a & b\epsilon \\ b & a \end{pmatrix} \mid (a,b) \not\equiv (0,0) \pmod{\mathfrak{m}} \right\} \\
\overline{T}' &= \pi^{-1}(T'(p)) \\
T &= \left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \mid a, d \in R^\times \right\} \\
\overline{T} &= \pi^{-1}(T(p)) \\
N' &= \left\{ \begin{pmatrix} a & b\epsilon \\ b & a \end{pmatrix}, \begin{pmatrix} a & b\epsilon \\ -b & -a \end{pmatrix} \mid a, b \in R, (a,b) \not\equiv (0,0) \pmod{\mathfrak{m}} \right\} \\
N &= \left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}, \begin{pmatrix} 0 & a \\ d & 0 \end{pmatrix} \mid a, d \in R^\times \right\} \\
RI' &= \left\{ \begin{pmatrix} a & bp\epsilon \\ bp & a \end{pmatrix} \mid a \in R^\times, b \in R \right\} \\
RI &= \left\{ \begin{pmatrix} a & bp \\ bp & a \end{pmatrix} \mid a \in R^\times, b \in R \right\}.
\end{aligned}
$$

Lemma 2.3. *Let H be a subgroup of a group G. Let χ be the character $\mathrm{Ind}_H^G 1$ of G. Let $S_g = \{s \in G \mid s^{-1}gs \in H\}$. Then $\chi(g) = \#S_g/H$.*

Proof. Note that $gsH = sH$ if and only if $s^{-1}gs \in H$. $\square$

Lemma 2.4. *Let $[g]$ be the conjugacy class of g. With the notation in Lemma 2.3, we have $\#S_g = \#C_G(g) \cdot \#H \cap [g]$.*

Proof. The orbit of g under conjugation is bijective with $G/C_G(g)$. $\square$

Using the above two lemmas and the derivation in Lemma 2.1, one can compute the characters $G = \mathrm{GL}_2(R)$ induced by the trivial character on a subgroup in the list above. These values are summarized in Tables 2 and 3. For example, let $\chi = \mathrm{Ind}_T^G 1$. Let us compute $\chi(g)$ for

$$g = \begin{pmatrix} \alpha & p\beta^2 \\ p & \alpha \end{pmatrix}$$

of type RI. First, we count the number of elements

$$h = \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \in T$$

which are conjugate to g. By consideration of discriminants, it must be the case that $a \equiv d \pmod{\mathfrak{m}}$ so write $d = a + px$. Using the derivation in Lemma 2.1, h is conjugate to

$$\begin{pmatrix} a & px^2 \\ p & a \end{pmatrix}$$

where $x \not\equiv 0 \pmod{\mathfrak{m}}$. Thus, there are 2 elements in T which are conjugate to g. Alternatively, it would be possible to count this by using centralizers, trace, and determinant to distinguish conjugacy classes. Applying the lemmas above, we see that $\chi(g) = 2p^2$.

TABLE 2. Characters of some induced representations of $G = \mathrm{GL}_2(R)$

$[g]$	$\mathrm{Ind}_{T'}^G 1$	$\mathrm{Ind}_{T'}^G 1$	$\mathrm{Ind}_{RI}^G 1$	$\mathrm{Ind}_{RI'}^G 1$	$\mathrm{Ind}_T^G 1$	$\mathrm{Ind}_T^G 1$
I	$(p^2-p)p^2$	p^2-p	$p^3(p^2-1)$	$p^3(p^2-1)$	$(p^2+p)p^2$	(p^2+p)
$T'(t=0)$	2	2	0	0	0	0
$T'(t \neq 0)$	2	2	0	0	0	0
B	0	0	0	0	0	0
$T(t=0)$	0	0	0	0	2	2
$T(t \neq 0)$	0	0	0	0	2	2
RT'	0	0	0	0	0	0
RT	0	0	0	0	0	0
RI'	$2p^2$	p^2-p	0	$2(p+1)p^2$	0	p^2+p
RB	0	p^2-p	0	0	0	p^2+p
RI	0	p^2-p	$2(p-1)p^2$	0	$2p^2$	p^2+p

TABLE 3. Characters of some induced representations of $G = \mathrm{GL}_2(R)$

$[g]$	$\mathrm{Ind}_{B'}^{G} 1$	$\mathrm{Ind}_{\overline{B}}^{G} 1$	$\mathrm{Ind}_{N'}^{G} 1$	$\mathrm{Ind}_{N}^{G} 1$	$\mathrm{Ind}_{\overline{T}}^{G} 1$	$\mathrm{Ind}_{G}^{G} 1$
I	$p^2(p+1)$	$p+1$	$\frac{p^2(p^2-p)}{2}$	$\frac{p^2(p^2+p)}{2}$	p^2+p	1
$T'(t=0)$	0	0	$\frac{p^2+p}{2}+1$	$\frac{p^2+p}{2}$	0	1
$T'(t\neq 0)$	0	0	1	0	0	1
B	0	1	0	0	0	1
$T(t=0)$	2	2	$\frac{p^2-p}{2}$	$\frac{p^2-p}{2}+1$	2	1
$T(t\neq 0)$	2	2	0	1	2	1
RT'	0	1	0	0	0	1
RT	0	1	0	0	0	1
RI'	0	$p+1$	p^2	0	p^2+p	1
RB	p^2	$p+1$	0	0	p^2+p	1
RI	$2p^2$	$p+1$	0	p^2	p^2+p	1

In Tables 2 and 3, t denotes the trace of the conjugacy class in question. From these tables, we deduce the following relations between characters.

Theorem 2.5. *We have the following character relations:*

$$\begin{aligned}(p+1)(\mathrm{Ind}_{T'}^{G} 1 - \mathrm{Ind}_{\overline{T}'}^{G} 1) + (\mathrm{Ind}_{RI}^{G} 1 - \mathrm{Ind}_{RI'}^{G} 1) &= (p-1)(\mathrm{Ind}_{T}^{G} 1 - \mathrm{Ind}_{\overline{T}}^{G} 1),\\ 2(\mathrm{Ind}_{N'}^{G} 1 - \mathrm{Ind}_{N}^{G} 1) &= (\mathrm{Ind}_{T'}^{G} 1 - \mathrm{Ind}_{T}^{G} 1),\\ \mathrm{Ind}_{B'}^{G} 1 + \mathrm{Ind}_{\overline{B}}^{G} 1 + \mathrm{Ind}_{N'}^{G} 1 &= \mathrm{Ind}_{N}^{G} 1 + \mathrm{Ind}_{\overline{T}}^{G} 1 + \mathrm{Ind}_{G}^{G} 1.\end{aligned}$$

Another relation between the characters considered in Theorem 2.5 is given by lifting the first relation in [2] for $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ to $\mathrm{GL}_2(\mathbb{Z}/p^2\mathbb{Z})$:

$$\mathrm{Ind}_{\overline{T}}^{G} 1 - \mathrm{Ind}_{\overline{T}'}^{G} 1 = 2(\mathrm{Ind}_{\overline{B}}^{G} 1 - \mathrm{Ind}_{G}^{G} 1).$$

Together with the three relations in Theorem 2.5 this provides a $\mathbb{Z}$-basis of the lattice of all relations between the 11 characters under consideration.

3. Relations between jacobians of modular curves

Let $H \leq \mathrm{GL}_2(R)$ be a subgroup and let $X_H = X(p^2)/H$ be its quotient by H. Let J_H be the jacobian of X_H defined as its Picard variety. By the results in [7] [8], the Picard variety of X_H exists and is an abelian variety defined over $\mathbb{Q}$. Applying the general methods in [2], the character relation in Theorem 2.5 for instance implies the following relation of jacobians.

Theorem 3.1. *The following $\mathbb{Q}$-isogeny of abelian varieties over $\mathbb{Q}$ holds.*

$$J_{B'} \times J_{\overline{B}} \times J_{N'} \sim_{\mathbb{Q}} J_N \times J_{\overline{T}} \times J_G.$$

Let us briefly recall the principle involved. In [2], arguments for the following theorem are given (strictly speaking, stated only for a specific character relation but the arguments clearly work for the general case).

Theorem 3.2 (de Smit-Edixhoven)**.** *Let G be a finite group and let $\mathcal{C}$ denote an additive $\mathbb{Q}$-linear category. Suppose M is an object of $\mathcal{C}$ with an action of G and which admits invariants by subgroups H_i, K_j of G. If*

$$\sum_{i=1}^{m} \mathrm{Ind}_{H_i}^{G} 1 = \sum_{j=1}^{n} \mathrm{Ind}_{K_j}^{G} 1$$

then we have an isomorphism in $\mathcal{C}$

$$\oplus_{i=1}^{m} M^{H_i} \cong \oplus_{j=1}^{n} M^{K_j}.$$

Note first that the character relation gives the existence of an isomorphism of $\mathbb{Q}[G]$-modules

$$\oplus_{i=1}^{m} \mathbb{Q}[G/H_i] \cong \oplus_{j=1}^{n} \mathbb{Q}[G/K_j].$$

To show Theorem 3.2 one now uses Yoneda's lemma. More specifically, note that $\mathrm{Hom}_{\mathcal{C}}(X,Y)$ is a $\mathbb{Q}$-vector space for any $X, Y \in \mathcal{C}$ as $\mathcal{C}$ is additive $\mathbb{Q}$-linear. Now, for each $X \in \mathcal{C}$, we obtain an isomorphism of $\mathbb{Q}$-vector spaces using Frobenius reciprocity and the defining property of invariants

$$\begin{aligned}\mathrm{Hom}_{\mathcal{C}}(X, \oplus_{i=1}^{m} M^{H_i}) \to \oplus_{i=1}^{m} \mathrm{Hom}_{\mathcal{C}}(X, M)^{H_i} \to \mathrm{Hom}_{\mathbb{Q}[G]}(\oplus_{i=1}^{m} \mathbb{Q}[G/H_i], \mathrm{Hom}_{\mathcal{C}}(X, M)) \to \\ \mathrm{Hom}_{\mathbb{Q}[G]}(\oplus_{j=1}^{n} \mathbb{Q}[G/K_j], \mathrm{Hom}_{\mathcal{C}}(X, M)) \to \mathrm{Hom}_{\mathcal{C}}(X, \oplus_{j=1}^{n} M^{K_j}).\end{aligned}$$

These isomorphisms are functorial in X, so by Yoneda's lemma, we obtain the desired isomorphism of objects in $\mathcal{C}$.

Let $\mathcal{A}$ denote the category of abelian varieties over $\mathbb{Q}$ and $\mathcal{A} \otimes \mathbb{Q}$ the category whose objects are the objects of $\mathcal{A}$ but $\mathrm{Hom}_{\mathcal{A}\otimes\mathbb{Q}}(X,Y) = \mathrm{Hom}_{\mathcal{A}}(X,Y) \otimes \mathbb{Q}$. The category $\mathcal{A} \otimes \mathbb{Q}$ is additive and $\mathbb{Q}$-linear by basic properties of abelian varieties (c.f. [6]). Moreover, $A, B \in \mathcal{A}$ are $\mathbb{Q}$-isogenous if and only if $A, B \in \mathcal{A} \otimes \mathbb{Q}$ are isomorphic.

Let J be the jacobian of $X(p^2)$. The object J has an action α of $G = \mathrm{GL}_2(R)$ by Picard functoriality and H-invariants exists for each subgroup H of G by taking the image of the idempotent $\frac{1}{|H|}\sum_{h\in H} h$. Moreover, $J^H \cong J_H$ in the category $\mathcal{A} \otimes \mathbb{Q}$. Applying Theorem 3.2, we deduce the desired relation of jacobians in Theorem 3.1.

4. Applicability of Mazur's method

¿From [4], Chapter 11, one has that

$$\begin{aligned} X_N &\cong_{\mathbb{Q}} X_0^+(p^4) := X_0(p^4)/\left\langle W_{p^4} \right\rangle \\ X_T &\cong_{\mathbb{Q}} X_0(p^4) \\ X_{\overline{T}} &\cong_{\mathbb{Q}} X_0(p^2) \\ X_{B'} &\cong_{\mathbb{Q}} X_0(p^3) \\ X_{\overline{B}} &\cong_{\mathbb{Q}} X_0(p) \end{aligned}$$

where W_{p^4} denotes the Fricke involution of $X_0(p^4)$. Thus, Theorem 3.1 implies the following

Corollary 4.1.

$$J_0(p^3) \times J_0(p) \times J_{N'} \sim_{\mathbb{Q}} J_0^+(p^4) \times J_0(p^2)$$

where $J_0(p^r)$ is the jacobian of $X_0(p^r)$ and $J_0^+(p^r)$ is the jacobian of $X_0^+(p^r)$. The factors in this relation are all jacobians of conventional modular curves except for $J_{N'}$. This should make it possible to determine whether $J_{N'}$ has any non-trivial rank 0 quotients [1].

5. Aknowledgements

The first author would like to express his thanks to MPIM and MSRI for his visits there in January-August 2000 and October-December 2000 respectively. The second author would like to thank MSRI for its hospitality in the fall of 2000. Thanks are also due to B. Powell for proofreading an earlier version of this paper.

References

[1] I. Chen. Jacobians of a certain class of modular curves of level p^n. In preparation, 2003.
[2] B. de Smit and S. Edixhoven. Sur un résultat d'Imin Chen. *Math. Res. Lett.*, 7(2–3):147–153, 2000.
[3] N. Katz and B. Mazur. *Arithmetic Moduli of Elliptic Curves.* Number 108 in Annals of Mathematics Studies. Princeton University Press, 1985.
[4] N. Katz and B. Mazur. *Arithmetic Moduli of Elliptic Curves.* Number 108 in Annals of Mathematics Studies. Princeton University Press, 1985.
[5] B. Mazur. Rational isogenies of prime degree. *Inventiones mathematicae*, 44:129–162, 1978.
[6] D. Mumford. *Abelian varieties.* Tata Institute of Fundamental Research Studies in Mathemaitcs 5. Oxford University Press, London, 1970.
[7] J.P. Murre. On contravariant functors from the category of preschemes over a field into the category of abelian groups. *Publ. Math. IHES*, 23:5–43, 1964.
[8] F. Oort. Sur le schéma de Picard. *Bull. Soc. Math. Fr.*, 90:1–14, 1962.
[9] J.P. Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Inventiones Mathematicae*, 15:259–331, 1972.

Imin Chen, Department of Mathematics, Simon Fraser University, Burnaby, B.C., Canada, V5A 1S6, ichen@math.sfu.ca

Bart de Smit, Mathematisch Instituut, Universiteit Leiden, Postbus 9512, 2300 RA Leiden, Netherlands, desmit@math.leidenuniv.nl

Martin Grabitz, Mathematisches Institut der Humboldt Universitaet, Rudower Chaussee 25 (Ecke Magnusstrasse), 12489 Berlin House 1, grabitz@mathematik.hu-berlin.de