Available online at www.sciencedirect.com
SCIENCE DIRECT®
ELSEVIER
COMPTES RENDUS MATHEMATIQUE
C. R. Acad. Sci. Paris, Ser. I 339 (2004) 187–192

Algebraic Geometry/Group Theory

Jacobians of modular curves associated to normalizers of Cartan subgroups of level p^n

Imin Chen [1]

Department of Mathematics, Simon Fraser University, Burnaby V5A 1S6, B.C., Canada

Received 24 July 2003; accepted after revision 30 April 2004
Available online 17 June 2004

Presented by Jean-Pierre Serre

Abstract

We derive a relation between induced representations of the group $\mathrm{GL}_2(\mathbb{Z}/p^n\mathbb{Z})$ which implies a relation between the Jacobians of certain modular curves of level p^n. A consequence of this relation is that the Jacobian of the modular curve associated to the normalizer of a non-split Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}/p^n\mathbb{Z})$ does not have any non-zero rank 0 quotient defined over $\mathbb{Q}$ if the Birch and Swinnerton–Dyer conjecture holds for Abelian varieties. ***To cite this article: I. Chen, C. R. Acad. Sci. Paris, Ser. I 339 (2004).***

Résumé

Jacobiennes de courbes modulaires associées aux normalisateurs de sous-groupes de Cartan de niveau p^n. Nous établissons une relation entre des représentations induites du groupe $\mathrm{GL}_2(\mathbb{Z}/p^n\mathbb{Z})$, ce qui implique une relation entre les jacobiennes de certaines courbes modulaires de niveau p^n. Une conséquence de cette relation est que la jacobienne de la courbe modulaire associée au normalisateur d'un sous-groupe Cartan non-déployé de $\mathrm{GL}_2(\mathbb{Z}/p^n\mathbb{Z})$ n'a aucun quotient non-nul de rang 0 défini sur $\mathbb{Q}$ si l'on admet la conjecture de Birch et Swinnerton–Dyer pour les variétés abéliennes. ***Pour citer cet article : I. Chen, C. R. Acad. Sci. Paris, Ser. I 339 (2004).***

Version française abrégée

Pour p un nombre premier impair et $n \in \mathbb{N}$, soit $R = \mathbb{Z}/p^n\mathbb{Z}$ et $G = \mathrm{GL}_2(R)$. Soit $X(p^n)$ la courbe modulaire compactifiée qui classifie les courbes elliptiques avec structure de plein niveau p^n [8]. Cette courbe modulaire a un modèle défini sur $\mathbb{Q}$ qui est géométriquement débranché et qui a un action droite par G aussi définie sur $\mathbb{Q}$. Pour un sous-groupe H de G, soit $X_H(p^n)$ le quotient de $X(p^n)$ par H et $J_H(p^n)$ sa jacobienne. Soit N' l'analogue dans G du normalisateur d'un sous-groupe de Cartan non-deployé (voir le Tableau 1).

E-mail address: ichen@math.sfu.ca (I. Chen).
[1] Research supported by NSERC and PRG grants.

1631-073X/$ – see front matter © 2004 Académie des sciences. Published by Elsevier SAS. All rights reserved.
doi:10.1016/j.crma.2004.04.027

Soit $X_0^+(p^r)$ le quotient de la courbe modulaire $X_0(p^r)$ par son involution Fricke W_{p^r}. Soit $J_0(p^r)$ et $J_0^+(p^r)$ les jacobiennes des courbes modulaires $X_0(p^r)$ et $X_0^+(p^r)$ respectivement. Soit $N_0(p^t)$ et $N_0^+(p^t)$ les quotients nouveaux de $J_0(p^t)$ et $J_0^+(p^t)$ respectivement, définis comme les quotients par les sommes des images des morphismes de dégénérescence provenant des niveaux inférieurs (cf. [10,12]). Si deux variétés abéliennes A_1 et A_2 définies sur $\mathbb{Q}$ sont isogènes sur $\mathbb{Q}$ on écrit $A_1 \sim_{\mathbb{Q}} A_2$. A partir d'une relation parmi les représentations induites du groupe G (Théorème 1.1), on utilise la méthode générale de [6] avec des identités de factorisations pour les jacobiennes des courbes modulaires (Proposition 1.3) afin de prouver le théorème suivant.

Théorème 0.1. *Pour tout $n \in \mathbb{N}$, on a :*

$$J_{N'}\left(p^n\right) \sim_{\mathbb{Q}} \prod_{r=0}^{n} N_0^+\left(p^{2r}\right).$$

On remarque que le cas $n = 1$ et ses variantes avec structure de niveau auxiliaire étaient connus par les spécialistes depuis quelques temps (cf. référence à Ligozat dans [7] et Elkies dans [5]). Des références plus récentes incluent [2,6,14]. On note aussi que le cas spécial $N^+ = 1, N^- = p^{2n}$ du Corollaire 3.3.2 dans [13], dérivé par formule de trace et le théorème d'isogène de Faltings, est une variante du Théorème 0.1 où on considére les sous-groupes de Cartan au lieu des normalisateurs des sous-groupes de Cartan. Le théorème ci-dessus a la conséquence suivante pour l'arithmétique de la courbe modulaire $X_{N'}(p^n)$.

Théorème 0.2. *Admettons la conjecture de Birch et Swinnerton–Dyer pour les variétés abéliennes. Alors, pour chaque $n \in \mathbb{N}$, la variété abélienne $J_{N'}(p^n)$ n'a aucun quotient non-nul de rang 0 défini sur $\mathbb{Q}$.*

On sait déjà depuis quelque temps que la courbe modulaire $X_{N'}(p)$ représente le cas le plus difficile de la question de Serre concernant la surjectivité des représentations galoisiennes associées aux courbes elliptiques [15,9]. Les résultats ci-dessus montrent que cette difficulté subsiste quand le niveau p est replacé par une puissance de p.

1. Introduction

Let p be an odd prime and $n \in \mathbb{N}$. Let $R = \mathbb{Z}/p^n\mathbb{Z}$ and $G = \mathrm{GL}_2(R)$. Consider the subgroups N', B_{s-1}, N, T_r of G described explicitly in Table 1 where by convention we let $T_0 = G$. These subgroups can be described in the following manner. Let G act on $\mathbb{P}^1(S)$ from the left where $S = R[Y]/(Y^2 - \epsilon)$ and ϵ is a non-square in $R^\times$. The subgroups N' and N are stabilizers in G of the subsets $\{Y, -Y\}$ and $\{0, \infty\}$ respectively. Let G act on $\mathbb{P}^1(\mathbb{Z}/p^r\mathbb{Z}) \times \mathbb{P}^1(\mathbb{Z}/p^r\mathbb{Z})$ diagonally and by reduction modulo p^r on each component. The subgroup T_r is the stabilizer in G of $(0, \infty)$. Let G act on $\mathbb{P}^1(\mathbb{Z}/p^{s-1}\mathbb{Z}) \times \mathbb{P}^1(\mathbb{Z}/p^s\mathbb{Z})$ diagonally and by reduction modulo p^{s-1} and modulo p^s respectively. The subgroup B_{s-1} is the stabilizer in G of $(0, \infty)$. In the case $n = 1$, N' and N are the normalizers of non-split and split Cartan subgroups of G respectively, T_1 is a split Cartan subgroup of G, and B_0 is a Borel subgroup of G.

For a subgroup H of G, let $\mathrm{Ind}_H^G 1$ be the induction of the trivial representation of H to G where representations are assumed to act on $\mathbb{Q}$-vector spaces. If two representations ρ_1 and ρ_2 of G are isomorphic over $\mathbb{Q}$ (i.e. their representation spaces are isomorphic as $\mathbb{Q}[G]$-modules), we write $\rho_1 \cong_{\mathbb{Q}} \rho_2$.

Theorem 1.1. *For each $n \in \mathbb{N}$, we have*:

$$\mathrm{Ind}_{N'}^G 1 \oplus \bigoplus_{s=1}^{n} \mathrm{Ind}_{B_{s-1}}^G 1 \cong_{\mathbb{Q}} \mathrm{Ind}_N^G 1 \oplus \bigoplus_{r=0}^{n-1} \mathrm{Ind}_{T_r}^G 1. \tag{1}$$

Table 1
Conventions and definitions

Conventions used in tables
p is an odd prime
$R = \mathbb{Z}/p^n\mathbb{Z}$
$\epsilon \in R^\times$ is a non-square
$m = n - 1$
$1 \leqslant r, s \leqslant n$
$1 \leqslant \mu < \nu \leqslant n - 1$
$[\cdot]$ denotes the value 1 if $\cdot$ is true and 0 otherwise
t denotes the trace of the conjugacy class

Subgroup	Form of elements	Order
N'	$\left\{\begin{pmatrix} a & b\epsilon \\ b & a \end{pmatrix}, \begin{pmatrix} a & b\epsilon \\ -b & -a \end{pmatrix}\right\}$	$2p^{2m} \cdot (p^2 - 1)$
B_{s-1}	$\left\{\begin{pmatrix} a & bp^{s-1} \\ cp^s & d \end{pmatrix}\right\}$	$p^{4n-2s-1} \cdot (p-1)^2$
N	$\left\{\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}, \begin{pmatrix} 0 & b \\ c & 0 \end{pmatrix}\right\}$	$2p^m \cdot (p-1)^2$
T_r	$\left\{\begin{pmatrix} a & bp^r \\ cp^r & d \end{pmatrix}\right\}$	$p^{4n-2r-2} \cdot (p-1)^2$

Table 2
Conjugacy classes of G

Type	Representatives	Parameters	Form of elements in centralizer
I	$\begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix}$	$\alpha \in R^\times$	$\left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right\}$
T'	$\begin{pmatrix} \alpha & \epsilon\beta^2 \\ 1 & \alpha \end{pmatrix}$	$\alpha \in R, \beta \in R^\times$	$\left\{\begin{pmatrix} a & c\epsilon\beta^2 \\ c & a \end{pmatrix}\right\}$
B	$\begin{pmatrix} \alpha & 0 \\ 1 & \alpha \end{pmatrix}$	$\alpha \in R^\times$	$\left\{\begin{pmatrix} a & 0 \\ c & a \end{pmatrix}\right\}$
T	$\begin{pmatrix} \alpha & \beta^2 \\ 1 & \alpha \end{pmatrix}$	$\alpha \in R, \beta \in R^\times$	$\left\{\begin{pmatrix} a & c\beta^2 \\ c & a \end{pmatrix}\right\}$
RT'_ν	$\begin{pmatrix} \alpha & p^\nu\epsilon\beta^2 \\ 1 & \alpha \end{pmatrix}$	$\alpha \in R^\times, \beta \in (R/p^{n-\nu}R)^\times$	$\left\{\begin{pmatrix} a & cp^\nu\epsilon\beta^2 \\ c & a \end{pmatrix}\right\}$
RT_ν	$\begin{pmatrix} \alpha & p^\nu\beta^2 \\ 1 & \alpha \end{pmatrix}$	$\alpha \in R^\times, \beta \in (R/p^{n-\nu}R)^\times$	$\left\{\begin{pmatrix} a & cp^\nu\beta^2 \\ c & a \end{pmatrix}\right\}$
RI'_μ	$\begin{pmatrix} \alpha & p^\mu\epsilon\beta^2 \\ p^\mu & \alpha \end{pmatrix}$	$\alpha \in R^\times, \beta \in (R/p^{n-\mu}R)^\times$	$\left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix}: a \equiv d \pmod{p^{n-\mu}}, b \equiv c\epsilon\beta^2 \pmod{p^{n-\mu}}\right\}$
$RBI'_{\mu,\nu}$	$\begin{pmatrix} \alpha & p^\nu\epsilon\beta^2 \\ p^\mu & \alpha \end{pmatrix}$	$\alpha \in R^\times, \beta \in (R/p^{n-\nu}R)^\times$	$\left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix}: a \equiv d \pmod{p^{n-\mu}}, b \equiv cp^{\nu-\mu}\epsilon\beta^2 \pmod{p^{n-\mu}}\right\}$
RB_μ	$\begin{pmatrix} \alpha & 0 \\ p^\mu & \alpha \end{pmatrix}$	$\alpha \in R^\times$	$\left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix}: a \equiv d \pmod{p^{n-\mu}}, b \equiv 0 \pmod{p^{n-\mu}}\right\}$
$RBI_{\mu,\nu}$	$\begin{pmatrix} \alpha & p^\nu\beta^2 \\ p^\mu & \alpha \end{pmatrix}$	$\alpha \in R^\times, \beta \in (R/p^{n-\nu}R)^\times$	$\left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix}: a \equiv d \pmod{p^{n-\mu}}, b \equiv cp^{\nu-\mu}\beta^2 \pmod{p^{n-\mu}}\right\}$
RI_μ	$\begin{pmatrix} \alpha & p^\mu\beta^2 \\ p^\mu & \alpha \end{pmatrix}$	$\alpha \in R^\times, \beta \in (R/p^{n-\mu}R)^\times$	$\left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix}: a \equiv d \pmod{p^{n-\mu}}, b \equiv c\beta^2 \pmod{p^{n-\mu}}\right\}$

Proof. Tables 2 and 3 describe the conjugacy classes and related information of the group G. This can be used to compute the character values in Table 3 and the first two columns of Table 4. By reduction modulo lower powers of p, we may deduce the last two columns of Table 4. The character values listed in Table 3 and Table 4 allow us to verify that the character of the representation on the left-hand side of (1) is equal to the character of the representation on right-hand side (1), thereby showing the two representations in question are isomorphic over $\mathbb{Q}$. □

Let $X(p^n)$ denote the compactified modular curve classifying elliptic curves with full level p^n structure [8]. By a full level p^n structure of an elliptic curve E over a scheme S, we mean a group homomorphism ϕ from $A = \mathbb{Z}/p^n\mathbb{Z} \times \mathbb{Z}/p^n\mathbb{Z}$ to $E[p^n](S)$ such that $\sum_{a\in A}[\phi(a)]$ is equal to $E[p^n]$ as a Cartier divisor of E over S where $[\phi(a)]$ denotes the Cartier divisor associated to $\phi(a)$. This modular curve has a model over $\mathbb{Q}$ which is

Table 3
Conjugacy information and values of the characters of some induced representations of G

Type	Number of this type	Size of centralizer	Size of conjugacy class	$\mathrm{Ind}_{N'}^G 1$	$\mathrm{Ind}_N^G 1$
I	$p^m(p-1)$	$p^{4m}\cdot(p^2-1)(p^2-p)$	1	$\frac{p^{2m}(p^2-p)}{2}$	$\frac{p^{2m}(p^2+p)}{2}$
$T'(t=0)$	$p^m(p-1)/2$	$p^{2m}\cdot(p^2-1)$	$p^{2m}\cdot(p^2-p)$	$1+\frac{p^m(p+1)}{2}$	$\frac{p^m(p+1)}{2}$
$T'(t\neq 0)$	$(p^n-1)\cdot p^m(p-1)/2$	$p^{2m}\cdot(p^2-1)$	$p^{2m}\cdot(p^2-p)$	1	0
B	$p^m(p-1)$	$p^m(p-1)\cdot p^n$	$p^{2m}\cdot(p^2-1)$	0	0
$T(t=0)$	$p^m(p-1)/2$	$p^{2m}(p-1)^2$	$p^{2m}\cdot(p^2+p)$	$\frac{p^m(p-1)}{2}$	$1+\frac{p^m(p-1)}{2}$
$T(t\neq 0)$	$(p^n-2p^m-1)\cdot p^m(p-1)/2$	$p^{2m}(p-1)^2$	$p^{2m}\cdot(p^2+p)$	0	1
RT'_ν	$p^m(p-1)\cdot p^{m-\nu}(p-1)/2$	$p^m(p-1)\cdot p^n$	$p^{2m}\cdot(p^2-1)$	0	0
RT_ν	$p^m(p-1)\cdot p^{m-\nu}(p-1)/2$	$p^m(p-1)\cdot p^n$	$p^{2m}\cdot(p^2-1)$	0	0
RI'_μ	$p^m(p-1)\cdot p^{m-\mu}(p-1)/2$	$p^{2m+2\mu}\cdot(p^2-1)$	$p^{2m-2\mu}\cdot(p^2-p)$	$p^{2\mu}$	0
$RBI'_{\mu,\nu}$	$p^m(p-1)\cdot p^{m-\nu}(p-1)/2$	$p^{2m+2\mu}\cdot p(p-1)$	$p^{2m-2\mu}\cdot(p^2-1)$	0	0
RB_μ	$p^m(p-1)$	$p^{2m+2\mu}\cdot p(p-1)$	$p^{2m-2\mu}\cdot(p^2-1)$	0	0
$RBI_{\mu,\nu}$	$p^m(p-1)\cdot p^{m-\nu}(p-1)/2$	$p^{2m+2\mu}\cdot p(p-1)$	$p^{2m-2\mu}\cdot(p^2-1)$	0	0
RI_μ	$p^m(p-1)\cdot p^{m-\mu}(p-1)/2$	$p^{2m+2\mu}\cdot(p-1)^2$	$p^{2m-2\mu}\cdot(p^2+p)$	0	$p^{2\mu}$

Table 4
Values of the characters of some induced representations of G

Type	$\mathrm{Ind}_{B_{n-1}}^G 1$	$\mathrm{Ind}_{T_n}^G 1$	$\mathrm{Ind}_{B_{s-1}}^G 1$	$\mathrm{Ind}_{T_r}^G 1$
I	$p^{2m}\cdot(p+1)$	$p^{2m}\cdot p(p+1)$	$p^{2(s-1)}\cdot(p+1)$	$p^{2(r-1)}\cdot p(p+1)$
$T'(t=0)$	0	0	0	0
$T'(t\neq 0)$	0	0	0	0
B	$1\cdot[n=1]$	0	$1\cdot[s=1]$	0
$T(t=0)$	2	2	2	2
$T(t\neq 0)$	2	2	2	2
RT'_ν	0	0	$1\cdot[s=1]$	0
RT_ν	0	0	$1\cdot[s=1]$	0
RI'_μ	0	0	$p^{2(s-1)}\cdot(p+1)\cdot[\mu\geqslant s]$	$p^{2(r-1)}\cdot p(p+1)\cdot[\mu\geqslant r]$
$RBI'_{\mu,\nu}$	0	0	$p^{2(s-1)}\cdot(p+1)\cdot[\mu\geqslant s]+p^{2(s-1)}\cdot[\mu=s-1]$	$p^{2(r-1)}\cdot p(p+1)\cdot[\mu\geqslant r]$
RB_μ	$p^{2m}\cdot[\mu=m]$	0	$p^{2(s-1)}\cdot(p+1)\cdot[\mu\geqslant s]+p^{2(s-1)}\cdot[\mu=s-1]$	$p^{2(r-1)}\cdot p(p+1)\cdot[\mu\geqslant r]$
$RBI_{\mu,\nu}$	0	0	$p^{2(s-1)}\cdot(p+1)\cdot[\mu\geqslant s]+p^{2(s-1)}\cdot[\mu=s-1]$	$p^{2(r-1)}\cdot p(p+1)\cdot[\mu\geqslant r]$
RI_μ	$2p^{2\mu}$	$2p^{2\mu}$	$p^{2(s-1)}\cdot(p+1)\cdot[\mu\geqslant s]+2p^{2\mu}\cdot[\mu<s]$	$p^{2(r-1)}\cdot p(p+1)\cdot[\mu\geqslant r]+2p^{2\mu}\cdot[\mu<r]$

geometrically disconnected and which has a right group action of G also defined over $\mathbb{Q}$. For a subgroup H of G, let $X_H(p^n)$ be the quotient of $X(p^n)$ by H and $J_H(p^n)$ be its Jacobian (taken to be its Picard variety). If two Abelian varieties A_1 and A_2 defined over $\mathbb{Q}$ are isogenous over $\mathbb{Q}$ we write $A_1 \sim_{\mathbb{Q}} A_2$. If they are isomorphic over $\mathbb{Q}$, we write $A_1 \cong_{\mathbb{Q}} A_2$.

Theorem 1.2. *For each $n\in\mathbb{N}$, we have*:

$$J_{N'}\big(p^n\big)\times\prod_{s=1}^{n}J_{B_{s-1}}\big(p^n\big)\sim_{\mathbb{Q}}J_N\big(p^n\big)\times\prod_{r=0}^{n-1}J_{T_r}\big(p^n\big).$$

Proof. Using the general method in [6], we deduce the theorem from the relation between induced representations in Theorem 1.1. This generalizes the case $n = 2$ shown in [4]. □

For a non-negative integer r, let $X_0^+(p^r)$ denote the quotient of the modular curve $X_0(p^r)$ by its Fricke involution W_{p^r} where by convention we let W_{p^r} be the identity and $X_0^+(p^r) = X_0(p^r)$ if $r = 0$. Let $J_0(p^r)$ and $J_0^+(p^r)$ denote the Jacobians of the modular curves $X_0(p^r)$ and $X_0^+(p^r)$ respectively. Let $N_0(p^t)$ and $N_0^+(p^t)$ denote the new quotients of $J_0(p^t)$ and $J_0^+(p^t)$ respectively, defined as the quotients by the sums of images of degeneracy morphisms from lower levels (cf. [10,12]).

Proposition 1.3. *We have*:

$$J_0(p^r) \sim_{\mathbb{Q}} \prod_{t=0}^{r} N_0(p^t)^{r-t+1} \quad \text{and} \quad J_0^+(p^r) \sim_{\mathbb{Q}} \prod_{t=0}^{r} N_0(p^t)^{(r-t+1)/2}$$

where by convention we let

$$N_0(p^t)^{m/2} = \begin{cases} N_0(p^t)^{m/2} & \text{if } m \text{ is even}, \\ N_0(p^t)^{(m-1)/2} \times N_0^+(p^t) & \text{if } m \text{ is odd}. \end{cases}$$

Proof. In both cases one can construct a homomorphism from the left-hand side to the products on the right-hand side using degeneracy morphisms. It suffices to verify that the induced map on the corresponding spaces of cusp forms of weight 2 is an isomorphism. This can be shown using the results of Atkin–Lehner theory [1], Theorem 5 and Lemma 26.

Using the facts that

$$J_N(p^n) \cong_{\mathbb{Q}} J_0^+(p^{2n}),$$
$$J_{T_r}(p^n) \cong_{\mathbb{Q}} J_0(p^{2r}),$$
$$J_{B_{s-1}}(p^n) \cong_{\mathbb{Q}} J_0(p^{2s-1}),$$

which can be obtained from results in [8] or [16], and Theorem 1.2, we deduce that

$$J_{N'}(p^n) \times \prod_{s=1}^{n} J_0(p^{2s-1}) \sim_{\mathbb{Q}} J_0^+(p^{2n}) \times \prod_{r=0}^{n-1} J_0(p^{2r}). \qquad \square \tag{2}$$

Theorem 1.4. *For each $n \in \mathbb{N}$, we have*:

$$J_{N'}(p^n) \sim_{\mathbb{Q}} \prod_{r=0}^{n} N_0^+(p^{2r}).$$

Proof. This can be shown by counting the number of copies of $N_0(p^t)$ up to isogeny over $\mathbb{Q}$ on both sides of (2) using Proposition 1.3. □

We remark that the case $n = 1$ and variants of it with additional level structure have been known to experts for some time (cf. reference to Ligozat in [7] and Elkies in [5]). More recent references in the literature include [2,6,14]. We also note that the special case $N^+ = 1$, $N^- = p^{2n}$ of Corollary 3.3.2 in [13], derived by means of trace formulae and Faltings' isogeny theorem, is a variant of Theorem 1.4 where one considers Cartan subgroups rather than the normalizers of Cartan subgroups N' and N.

Theorem 1.5. *Suppose that the Birch and Swinnerton–Dyer conjecture holds for Abelian varieties. Then for each $n \in \mathbb{N}$, the Abelian variety $J_{N'}(p^n)$ has no non-zero rank* 0 *quotient defined over* $\mathbb{Q}$.

Proof. The L-functions of the simple factors of $N_0^+(p^{2r})$ defined over $\mathbb{Q}$ are forced to vanish at $s = 1$ by consideration of signs in functional equations. Hence, every simple factor defined over $\mathbb{Q}$ of $N_0^+(p^{2r})$ has positive rank over $\mathbb{Q}$ by the Birch and Swinnerton–Dyer conjecture. □

It has been known for some time that the modular curve $X_{N'}(p)$ represents the most difficult case of Serre's question on the surjectivity of Galois representations associated to elliptic curves [15,9]. The results above show that this difficulty does not disappear when the level p is replaced by a power of p.

It would be interesting to determine an explicit description of the isogeny in Theorem 1.2. In the case $n = 1$, an explicit description was conjectured by Mérel [11] and subsequently proven in [3].

Acknowledgement

The author would like to thank M. Grabitz, Mathematisches Institut der Humboldt Universität, and MSRI.

References

[1] A.O.L. Atkin, J. Lehner, Hecke operators on $\Gamma_0(m)$, Math. Ann. 185 (1970) 134–160.
[2] I. Chen, The Jacobians of non-split Cartan modular curves, Proc. London Math. Soc. 77 (1) (1998) 1–38.
[3] I. Chen, On relations between Jacobians of certain modular curves, J. Algebra 231 (2000) 414–448.
[4] I. Chen, B. de Smit, M. Grabitz, Relations between Jacobians of modular curves of level p^2, J. Théor. Nombres Bordeaux, accepted for publication 15 January 2003, 11 p.
[5] H. Darmon, The equations $x^n + y^n = z^2$ and $x^n + y^n = z^3$, Int. Math. Res. Notices 72 (1) (1993) 263–273.
[6] B. de Smit, S. Edixhoven, Sur un résultat d'Imin Chen, Math. Res. Lett. 7 (2/3) (2000) 147–153.
[7] B. Gross, Arithmetic on Elliptic Curves with Complex Multiplication, Lecture Notes in Math., vol. 776, Springer-Verlag, 1980.
[8] N. Katz, B. Mazur, Arithmetic Moduli of Elliptic Curves, Ann. of Math. Stud., vol. 108, Princeton University Press, 1985.
[9] B. Mazur, Modular curves and the Eisenstein ideal, Publ. Math. I.H.E.S. 47 (1977) 33–186.
[10] B. Mazur, Rational isogenies of prime degree, Invent. Math. 44 (1978) 129–162.
[11] L. Mérel, Arithmetic of elliptic curves and diophantine equations, J. Théor. Nombres Bordeaux 11 (1) (1999) 173–200.
[12] K. Ribet, Twists of modular forms and endomorphisms of abelian varieties, Math. Ann. 253 (1980) 43–62.
[13] D. Roberts, Shimura curves analogous to $X_0(N)$, PhD thesis, Harvard University, 1989.
[14] F. Sauvageot, Représentation de Steinberg et identités de projecteurs, C. R. Acad. Sci. Paris, Ser. I 335 (2002) 505–508.
[15] J.-P. Serre, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, Invent. Math. 15 (1972) 259–331.
[16] G. Shimura, Introduction to the Arithmetic Theory of Automorphic Functions, Iwanami Shoten and Princeton University Press, 1971.