Journal of Number Theory **78**, 253–270 (1999)
Article ID jnth.1999.2406, available online at http://www.idealibrary.com on IDEAL®

Remarks on mod-l^n Representations, $l=3, 5$

Brian Conrad

Department of Mathematics, Harvard University, Cambridge, Massachusetts 02138
E-mail: bconrad@math.harvard.edu

and

Siman Wong*

Department of Mathematics, Brown University, Providence, Rhode Island 02912
E-mail: siman@math.brown.edu

Communicated by K. Rubin

Received November 9, 1998

(L, E_1, E_2), where L is a number field with degree $l^{3(n-1)}$ over $\mathbf{Q}$ and E_1 and E_2 are elliptic curves over L with distinct j-invariants lying in $\mathbf{Q}$, such that the following conditions hold: (1) the pairs of j-invariants $\{j(E_1), j(E_2)\}$ are mutually disjoint, (2) the associated mod-l^n representations $G_L = \mathrm{Gal}(\bar{L}/L) \to GL_2(\mathbf{Z}/l^n)$ are surjective, (3) for almost all primes $\mathfrak{p}$ of L, we have $l^n \mid a_{\mathfrak{p}}(E_1)$ if and only if $l^n \mid a_{\mathfrak{p}}(E_2)$, and (4) the two representations $E_i[l^n](\bar{L})$ are not related by twisting by a continuous character $G_L \to (\mathbf{Z}/l^n)^\times$. No such triple satisfying (2)–(4) exists over any number field if we replace l by a prime larger than 5. The proof depends on determining the automorphisms of the group $\mathrm{GL}_2(\mathbf{Z}/l^n)$ for $l=3, 5$ and analyzing ramification in a branched covering of "twisted" modular curves. © 1999 Academic Press

1. INTRODUCTION

Choose a number field K and fix an algebraic closure $\bar{K}$ of K. Denote by G_K the Galois group $\mathrm{Gal}(\bar{K}/K)$. Let E_1, E_2 be elliptic curves over K, $l \in \mathbf{Z}$ a prime, $n \in \mathbf{Z}$ a positive integer, and fix a basis of $E_i[l^n](\bar{K})$ over $\mathbf{Z}/l^n$. Let

$$\rho_{E_i, l^n}: G_K \to \mathrm{Aut}(E_i[l^n](\bar{K})) \simeq \mathrm{GL}_2(\mathbf{Z}/l^n)$$

be the resulting mod-l^n representations associated to E_i, and assume that ρ_{E_1, l^n} and ρ_{E_2, l^n} are surjective. Let Σ be a finite set of non-archimedean primes of K containing all the primes of bad reduction for E_1 and E_2, as well as all of the primes in K lying above l. For any prime $\mathfrak{p}$ of K not in Σ, define $a_{\mathfrak{p}}(E_i)$ to be the trace of the action on the l-adic Tate module of

* Current address: Department of Mathematics, University of Massachusetts, Amherst, MA 01003-4515. E-mail: siman@math.umass.edu.

0022-314X/99 $30.00

E_i by an arithmetic Frobenius element at $\mathfrak{p}$ in G_K. If $\rho_{E_1, l^n} \simeq \chi \rho_{E_2, l^n}$ for a continuous character $\chi: G_K \to (\mathbf{Z}/l^n)^\times$, then for all $\mathfrak{p} \notin \Sigma$, we have

$$l^n \mid a_\mathfrak{p}(E_1) \qquad \text{if and only if} \quad l^n \mid a_\mathfrak{p}(E_2). \tag{1}$$

By the Cebotarev density theorem, this is equivalent to saying that for all $g \in G_K$, $\rho_{E_1, l^n}(g)$ has trace 0 if and only if $\rho_{E_2, l^n}(g)$ has trace 0. It follows from [9, Cor. 1(b)] (and "*Correction to* [9]" below) that if $l > 5$, then the condition (1) implies that the ρ_{E_i, l^n} are equivalent up to twisting by a $(\mathbf{Z}/l^n)^\times$-valued continuous character of G_K. For $l = 3$ or $l = 5$, and $n > 1$, the same conclusion holds for the pair of representations $G_K \to \mathrm{GL}_2(\mathbf{Z}/l^{n-1})$ induced from the *surjective* ρ_i by reduction modulo l^{n-1}, thanks to [9, Cor. 1(c)]. The proofs depend upon determining the automorphisms of $\mathrm{PGL}_2(\mathbf{Z}/l^n)$. For $l > 5$, all such automorphisms turn out to be inner, but for $l = 3$ and $l = 5$ there are non-trivial outer automorphisms. In this paper, we exploit these outer automorphisms to produce elliptic curves E over number fields K for which the associated mod-l^n representation of G_K is surjective but is *not* determined (up to twisting) by the set of primes $\mathfrak{p}$ with $l^n \mid a_\mathfrak{p}(E)$.

THEOREM 1. *Let $l = 3$ or 5, let $n > 1$, and let K be a number field which is linearly disjoint from $\mathbf{Q}(\zeta_{l^n})$, where ζ_{l^n} is a primitive l^nth root of unity. There exist infinitely many triples (L, E_1, E_2) consisting of a finite extension L/K with degree $l^{3(n-1)}$ and elliptic curves E_1, E_2 over L with distinct j-invariants in K such that the pairs $\{j(E_1), j(E_2)\}$ are mutually disjoint, the corresponding mod-l^n representations $\rho_{E_1, l^n}, \rho_{E_2, l^n}: G_L \to GL_2(\mathbf{Z}/l^n)$ satisfy the condition* (1) *and are surjective, and ρ_{E_1, l^n} and ρ_{E_2, l^n} are not equivalent up to twisting by any continuous character $G_L \to (\mathbf{Z}/l^n)^\times$. In fact, infinitely many such triples $\tau = (L, E_1, E_2)$ can be chosen so that each pair of representations ρ_{E_1, l^n} and ρ_{E_2, l^n} has the same common splitting field L_τ over L and as we vary τ, no prime of K away from l with norm $> (l^2 - 3)/2$ is ramified in more than one of the L_τ's.*

In view of our remarks above, for any triple (L, E_1, E_2) in the theorem, the mod-l^{n+1} representations $G_L \to GL_2(\mathbf{Z}/l^{n+1})$ arising from E_1 and E_2 cannot *both* be surjective. To prove the theorem, we use a non-trivial outer automorphism of $\mathrm{PGL}_2(\mathbf{Z}/l^n)$ in order to construct a non-trivial determinant-preserving outer automorphism φ of $GL_2(\mathbf{Z}/l^n)$ which takes trace zero matrices to trace zero matrices. If ρ is a *surjective* mod-l^n representation of an elliptic curve E over a number field K, then ρ and $\rho' = \varphi \circ \rho$ have cyclotomic determinant and are not equivalent up to twists. Moreover, for all but finitely many primes $\mathfrak{p}$ of K, ρ and ρ' are unramified at $\mathfrak{p}$ and $l^n \mid \mathrm{trace}(\rho(\mathrm{Frob}_\mathfrak{p}))$ if and only if $l^n \mid \mathrm{trace}(\rho'(\mathrm{Frob}_\mathfrak{p}))$, where $\mathrm{Frob}_\mathfrak{p}$ is an arithmetic Frobenius element at $\mathfrak{p}$ in G_K. We want to realize ρ' as the mod-l^n representation of an elliptic curve E' over K. This step will require enlarging K a small amount to an extension L, but we will be able to slightly control ramification in L/K.

Here is how we will find E'. There is a proper smooth curve $X(\rho')$ over K which, roughly speaking, classifies elliptic curves whose mod-l^n representation is isomorphic to ρ'. In particular, over $\bar{K}$ there is an isomorphism

$$X(\rho') \times_K \bar{K} \simeq X(l^n) \times_{\mathbf{Z}[1/l]} \bar{K},$$

where $X(l^n)$ denotes the compactified full level l^n moduli scheme over $\mathbf{Z}[1/l]$ in the sense of [5, Sects. 8.6ff.], so $X(\rho')$ is *not* geometrically connected over K. However, since the determinant of ρ' is cyclotomic, the connected components of $X(\rho')$ *are* geometrically connected over K. Let $\bar{\rho}'$ be the mod-l reduction of ρ'. "Reduction mod l" on Galois representations induces a finite flat map $X(\rho') \to X(\bar{\rho}')$ over K whose base change to $\bar{K}$ is the usual projection $X(l^n) \times_{\mathbf{Z}[1/l]} \bar{K} \to X(l) \times_{\mathbf{Z}[1/l]} \bar{K}$.

For $l=3$ and 5, an argument of Mazur shows that the connected components of $X(\bar{\rho}')$ have rational points and so are non-canonically isomorphic to $\mathbf{P}^1_K$. Thus, we can regard the connected components of $X(\rho')$ as branched covers of $\mathbf{P}^1_K$ which are geometrically connected over K. We find the desired elliptic curves in Theorem 1 by looking in the fibers on $X(\rho')$ over well-chosen K-rational points on the connected components $\mathbf{P}^1_K$ of $X(\bar{\rho}')$. We do not know if it is sufficient to only look at K-rational points on $X(\rho')$ (of which there are only finitely many, by Faltings' Theorem), and this is why we cannot precisely control the number fields over which our examples occur.

Correction to [9]. S. W. would like to take this opportunity to correct a confusing terminology mistake in [9], which is needed in the present paper. Let $\mathcal{O}$ be a complete local ring with maximal ideal λ. Consider two continuous representations $\rho_1, \rho_2 \colon G_K \to \mathrm{GL}_n(\mathcal{O})$ which are unramified outside of a finite set of places Σ of K. For any $\mathfrak{p} \notin \Sigma$, define $a_i(\mathfrak{p}) =$ trace $\rho_i(\mathrm{Frob}_\mathfrak{p})$. In [9, Sect. 1] (see in particular the displayed equation (1) there), ρ_1 and ρ_2 are defined to be "λ-adically close at the supersingular primes" if there is a positive integer N_0 such that whenever *both* $a_i(\mathfrak{p})$ lie in λ^{N_0}, one has for all $w \geqslant N_0$ that $a_1(\mathfrak{p}) \in \lambda^w$ if and only if $a_2(\mathfrak{p}) \in \lambda^w$. This definition is inadequate for the proofs in [9], and is automatically satisfied whenever $\lambda^{N_0} = 0$ (a case of interest for the present paper)! The definition of λ-adic closeness should have been modified to require that if *one of the two* $a_i(\mathfrak{p}) \in \lambda^{N_0}$, then for any $w \geqslant N_0$, $a_1(\mathfrak{p}) \in \lambda^w$ if and only if $a_2(\mathfrak{p}) \in \lambda^w$. Note, for example, that this is a non-trivial condition even if $\lambda^{N_0} = 0$.

It is only under this modified definition of λ-adic closeness that the arguments in [9] yield the results as claimed there. However, the statement of [9, Lemma 7] needs to be slightly modified. Beginning with the phrase *Suppose one of the following holds...*, the lemma should be replaced by the following:

Suppose one of the following holds:

- n is even and either $k \not\simeq \mathbf{F}_2$ or 2 is not a zero-divisor in $\mathcal{O}$; or
- $n \geqslant 5$ is odd and either $k \not\simeq \mathbf{F}_3$ or 3 is not a zero-divisor in $\mathcal{O}$; or
- $n = 3$ and $k \not\simeq \mathbf{F}_2$, $k \not\simeq \mathbf{F}_3$.

Then there exists an automorphism φ of $\mathrm{PGL}_n(\mathcal{O})$ such that $\varphi \circ \tilde{\rho}_2 = \tilde{\rho}_1$.

Suppose instead that n is even and $k = \mathbf{F}_2$, or that $n = 3$ and $k = \mathbf{F}_3$. Let p denote the characteristic of k and let $\mathfrak{a}$ denote the annihilator of p in $\mathcal{O}$. Then the analogous conclusion holds for the pair of representations $G_K \to \mathrm{PGL}_n(\mathcal{O}/\mathfrak{a})$ induced from the $\tilde{\rho}_i$.

2. BRANCHED COVERS OF $\mathbf{P}^1_K$

In this section, we recall some results related to the Hilbert Irreducibility Theorem, stated in a geometric form.

Let K be a number field and let $\pi: X \to \mathbf{P}^1_K$ be a finite map, where X is a smooth connected curve over K. The Hilbert Irreducibility Theorem says that for infinitely many K-rational points $a \in \mathbf{P}^1_K$, the fiber $\pi^{-1}(a)$ has the form $\pi^{-1}(a) \simeq \mathrm{Spec}(L_a)$ for a finite extension field L_a/K. In more algebraic terms, if we identify $K(\mathbf{P}^1_K) \simeq K(t)$ and we choose a primitive element for the finite separable extension $K(X)/K(\mathbf{P}^1_K)$ of function fields, then $K(X) \simeq K(t)[Y]/(f)$ for some monic $f \in K(t)[Y]$. The Hilbert Irreducibility Theorem in the geometric form just given is equivalent to the statement that for infinitely many $t_0 \in K$, the polynomial $f(t_0, Y) \in K[Y]$ is irreducible, in which case $L_{t_0} = K[Y]/f(t_0, Y)$. Of course, we avoid the finitely many $t_0 \in K$ where some coefficient of f in $K(t)$ has a pole.

We will need a milder stronger formulation, which is well-known:

LEMMA 1. *Let π be as above and choose a finite extension E/K. Assume that X is geometrically connected over K, or more generally that E is linearly disjoint (over K) from the algebraic closure of K in $K(X)$. Then there exist infinitely many K-rational points $a \in \mathbf{P}^1_K$ for which $\pi^{-1}(a) \simeq \mathrm{Spec}(L_a)$ for a finite extension L_a/K which is linearly disjoint from E over K. In other words, $\pi^{-1}(a) \times_K E$ is irreducible for infinitely many K-rational points $a \in \mathbf{P}^1_K$.*

Proof. Since E/K is a finite separable extension, by [6, Prop 3.3, Sect. 9] every Hilbert set in E contains a Hilbert set in K. Put in more algebraic terms, for any irreducible monic polynomial $f \in E(t)[Y]$, there exists an irreducible monic polynomial $g_f \in K(t)[Y]$ such that for all but finitely many $t_0 \in K$, $f(t_0, Y) \in E[Y]$ is irreducible whenever $g_f(t_0, Y) \in K[Y]$ is irreducible. Thus, by the Hilbert Irreducibility Theorem for the number field K and the polynomial $g_f \in K(t)[Y]$, we conclude that for any irreducible monic $f \in E(t)[Y]$, there are infinitely many $t_0 \in K$ (rather than just $t_0 \in E$) such that $f(t_0, Y) \in E[Y]$ is irreducible. In particular, for any irreducible monic $f \in K(t)[Y]$ which remains irreducible in $E(t)[Y]$, there are infinitely many $t_0 \in K$ so that $f(t_0, Y)$ is irreducible in $E[Y]$. Of course, this is just the usual proof that a finite (separable) extension of a Hilbertian field is again Hilbertian.

In order to use this to deduce the lemma, we just have to show that if we choose an isomorphism $K(X) \simeq K(t)[Y]/(f)$ for some irreducible monic $f \in K(t)[Y]$, then f is irreducible in $E(t)[Y]$. It is not difficult to show that this is equivalent to the irreducibility of $X \times_K E$, or even the connectedness of $X \times_K E$ (by smoothness). If K' denotes the algebraic closure of K in $K(X)$ then X is naturally a proper smooth curve over K' and is geometrically connected as such [3, IV$_2$, 4.5.15]. Since $X \times_K E = X \times_{K'} \operatorname{Spec}(K' \otimes_K E)$ and $K' \otimes_K E$ is a field by the linear disjointness hypothesis, it follows that $X \times_K E$ is connected. ∎

3. AUTOMORPHISMS OF $\mathrm{GL}_2(\mathbf{Z}/l^n)$

LEMMA 2. *Let R be a local ring with residue field k and maximal ideal $\mathfrak{m}$. The natural map $\mathrm{SL}_n(R) \to \mathrm{SL}_n(k)$ is surjective. The same holds with PSL_n replaced by PSL_n, PGL_n and GL_n.*

Proof. Given a matrix $A = (a_{ij})$ in $\mathrm{SL}_n(k)$, let $\mathfrak{a} = (\alpha_{ij})$ be an $n \times n$ matrix over R with $\alpha_{ij} \bmod \mathfrak{m} = a_{ij}$ for all i, j. Denote by $\mathfrak{a}_{ij}$ the $(n-1) \times (n-1)$ matrix obtained by removing the ith row and the jth column of $\mathscr{A}$. Define A_{ij} similarly. Then

$$\sum_{j=1}^{n} (-1)^j \alpha_{1j} \det(\mathfrak{a}_{1j}) = \det(\mathfrak{a}) \equiv 1 \qquad (\mathrm{mod}\ \mathfrak{m}). \tag{2}$$

If we fix the entries α_{ij} with $i \geqslant 2$, then any lift $\mathfrak{a}$ of A with these α_{ij} for $i > 2$ gives rise to a solution mod $\mathfrak{m}$ of the linear equation (2). Moreover, since $\det(\mathfrak{a}_{1j}) \bmod \mathfrak{m} = \det(A_{1j})$ for all j, at least one of the $\det(\mathfrak{a}_{ij})$ is a unit. Thus, we can easily find elements $\alpha_{11}, ..., \alpha_{1n}$ in R so that the left side of (2) is equal to 1 in R. This takes care of the lemma for SL_n; the other cases are similar. ∎

LEMMA 3. *Let R be a Noetherian local ring with maximal ideal $\mathfrak{m}$ and finite residue field k with characteristic $l > 0$. Denote by K_n and L_n the kernel* *of the natural maps from* $\mathrm{PSL}_n(R)$ *to* $\mathrm{PSL}_n(R/\mathfrak{m})$ *and* $\mathrm{PSL}_n(R/\mathfrak{m}^2)$, *respectively. Let* $M \subset \mathrm{PSL}_n(R)$ *be a normal subgroup such that* ML_n/L_n *is a finite* l*-group. Then* $M \subset K_n$.

The same conclusion holds if $l \nmid n$ *and if we replace* PSL_n *by* PGL_n.

Remark 1. The group ML_n/L_n is always *finite*: it is a subgroup of $\mathrm{PSL}_n(R)/K_n$, which injects into $\mathrm{PSL}_n(R/\mathfrak{m}^2)$, which is finite since k is finite and $\mathfrak{m}$ is finitely generated.

Proof. We first deal with the case of PSL_n. Then there are no non-trivial normal l-subgroups in $\mathrm{PSL}_n(k)$: for $n \neq 2$ or $k \neq \mathbf{F}_2, \mathbf{F}_3$ this follows from the simplicity of $\mathrm{PSL}_n(k)$, and the remaining cases follow from the isomorphisms $\mathrm{PSL}_2(\mathbf{F}_2) \simeq S_3$ and $\mathrm{PSL}_2(\mathbf{F}_3) \simeq A_4$.

Since $\mathfrak{m}/\mathfrak{m}^2$ is a finite-dimensional k-vector space, K_n/L_n is a finite elementary l-group, and hence so is MK_n/ML_n. The exact sequence

$$1 \to ML_n/L_n \to MK_n/L_n \to MK_n/ML_n \to 1$$

and the hypothesis on M then imply that MK_n/L_n, and hence MK_n/K_n, is a finite l-group. The latter is a normal l-subgroup of $\mathrm{PSL}_n(R)/K_n$, which by Lemma 2 is isomorphic to $\mathrm{PSL}_n(k)$. Thus $MK_n = K_n$, as desired.

The quotient group $\mathrm{PGL}_n(R)/\mathrm{PSL}_n(R) \simeq R^\times/R^{\times^n}$ has exponent dividing n, so the above argument applies to PGL_n if $l \nmid n$.

COROLLARY 1. *Let* R *be a Noetherian local ring with maximal ideal* $\mathfrak{m}$ *and a finite residue field* k *with characteristic* $l > 0$. *Define* K_n *as in Lemma* 3. *Every automorphism* φ *of* $\mathrm{PSL}_n(R)$ (*resp.* $\mathrm{PGL}_n(R)$ *with* $l \nmid n$) *takes* K_n *to itself, thereby giving an automorphism* $\bar{\varphi}$ *of* $\mathrm{PSL}_n(k)$ (*resp.* $\mathrm{PGL}_n(k)$) *such that* $\bar{\varphi}(\bar{g}) = \overline{\varphi(g)}$ *for all* $g \in \mathrm{PSL}_n(R)$ (*resp.* $g \in \mathrm{PGL}_n(R)$), *where* $\overline{(\cdot)}$ *denotes the image under the natural map* $\mathrm{PSL}_n(R) \to \mathrm{PSL}_n(k)$ (*resp.* $\mathrm{PGL}_n(R) \to \mathrm{PGL}_n(k)$).

Proof. Apply Lemma 3 to $M = \varphi(K_n)$. ∎

For the rest of this section, fix a prime l, let $\alpha \in (\mathbf{Z}/l^n)^\times$ be a choice of generator of the unique cyclic subgroup order $l-1$, and let Γ be the subgroup of $GL_2(\mathbf{Z}/l^n)$ generated by $\left(\begin{smallmatrix}\alpha & 0\\ 0 & 1\end{smallmatrix}\right)$ and $\mathrm{SL}_2(\mathbf{Z}/l^n)$. Thus, Γ is abstractly a semi-direct product $\mathbf{Z}/(l-1) \ltimes \mathrm{SSL}_2(\mathbf{Z}/l^n)$, where the $\mathbf{Z}/(l-1)$ is generated by $\left(\begin{smallmatrix}\alpha & 0\\ 0 & 1\end{smallmatrix}\right)$. Since $\mathrm{SL}_2(\mathbf{Z}/l^n)$ contains all elements in Γ with l-power order and it is generated by such elements (e.g., $\left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}1 & 0\\ 1 & 1\end{smallmatrix}\right)$), we see that $\mathrm{SL}_2(\mathbf{Z}/l^n)$ is stable under $\mathrm{Aut}(\Gamma)$. The natural map $\Gamma \to \mathrm{GL}_2(\mathbf{Z}/l)$ is clearly surjective, and if $l > 2$, then the scalar matrices in Γ are those of order dividing $l-1$. Also, note that if $l > 2$, then the restriction of the canonical map $GL_2(\mathbf{Z}/l^n) \xrightarrow{\pi} \mathrm{PGL}_2(\mathbf{Z}/l^n)$ to Γ is surjective.

LEMMA 4. *If $l>2$, then every automorphism of* $\mathrm{PGL}_2(\mathbf{Z}/l^n)$ *lifts to an automorphism of* Γ.

Proof. Choose an automorphism φ of $\mathrm{PGL}_2(\mathbf{Z}/l^n)$. Since

$$\begin{pmatrix}\alpha & 0\\ 0 & \alpha\end{pmatrix}=\begin{pmatrix}\alpha & 0\\ 0 & 1\end{pmatrix}^2\begin{pmatrix}\alpha^{-1} & 0\\ 0 & \alpha\end{pmatrix},$$

we see that $H=\ker(\pi|_\Gamma)$ is a cyclic group (of scalar matrices) of order $l-1$, and

$$1\to H\to\Gamma\xrightarrow{\pi}\mathrm{PGL}_2(\mathbf{Z}/l^n)\to 1 \tag{3}$$

is a central extension, corresponding to a cohomology class $\phi\in H^2(\mathrm{PGL}_2(\mathbf{Z}/l^n),H)$ (the surjectivity of π in (3) requires $l>2$). Since the automorphism group of the cyclic group H is commutative, an easy calculation shows that the automorphism φ of $\mathrm{PGL}_2(\mathbf{Z}/l^n)$ lifts to an automorphism of Γ if and only if $\varphi^*(\phi)\in H^2(\mathrm{PGL}_2(\mathbf{Z}/l^n),H)$ is equal to the image $\varphi_H(\phi)$ for some *automorphism* $\varphi_H\colon H\simeq H$. The point is that when such a φ_H exists, there is a lift $\tilde\varphi$ of φ to an endomorphism of Γ which induces the automorphism φ_H on H. A simple diagram chase then shows that $\tilde\varphi$ is actually an *automorphism* of Γ.

The only possibilities for φ_H are multiplication by $m\in(\mathbf{Z}/(l-1))^\times$, and if $\varphi^*(\phi)=m\phi$ for some $m\in\mathbf{Z}/(l-1)$, then (by the Chinese Remainder Theorem) m *can* be chosen to lie in $(\mathbf{Z}/(l-1))^\times$ (since φ^* is an automorphism). Thus, φ lifts to an automorphism of Γ if and only if the cohomology class $\varphi^*(\phi)=\varphi_H(\phi)$ for some endomorphism φ_H of the group H. By an argument in terms of central extensions, it is clear that the elements of the form $\varphi_H(\phi)$ for variable φ_H are precisely the elements in the kernel of $\pi^*\colon H^2(\mathrm{PSL}_2(\mathbf{Z}/l^n),H)\to H^2(\Gamma,H)$. Thus, φ lifts to an automorphism of Γ if and only if $(\varphi\circ\pi)^*\,\phi=\pi^*\varphi^*\phi=0$ in $H^2(\Gamma,H)$. We will show that $(\varphi\circ\pi)^*\,\phi=0$.

Let $K=\ker(\Gamma\to GL_2(\mathbf{Z}/l))$ and let $P=\ker(\Gamma\to\mathrm{PGL}_2(\mathbf{Z}/l))$. Since (3) is a central extension, P and K act trivially on H. Also, since K is a finite l-group and H has order prime to l, $H^i(K,H)=0$ for all $i>0$. Since $\pi(P)$ is the kernel of the natural map $\mathrm{PGL}_2(\mathbf{Z}/l^n)\to\mathrm{PGL}_2(\mathbf{Z}/l)$, it follows from Lemma 3 that φ takes $\pi(P)$ isomorphically back to itself. The induced automorphism $\bar\varphi$ of $\mathrm{PGL}_2(\mathbf{Z}/l^n)/\pi(P)\simeq\mathrm{PGL}_2(\mathbf{Z}/l)$ is exactly the map in Corollary 1, so composing the map $\Gamma/K\to\mathrm{PGL}_2(\mathbf{Z}/l^n)/\pi(K)$ (induced by π) with the projection $\mathrm{PGL}_2(\mathbf{Z}/l^n)/\pi(K)\to\mathrm{PGL}_2(\mathbf{Z}/l^n)/\pi(P)$ and the automorphism $\bar\varphi$, we get a map of groups $\psi\colon\Gamma/K\to\mathrm{PGL}_2(\mathbf{Z}/l^n)/\pi(P)$. Using the identification $\Gamma/K\simeq GL_2(\mathbf{Z}/l)$, this map ψ is exactly the composite of the canonical projection $\bar{\pi}: GL_2(\mathbf{Z}/l) \to \mathrm{PGL}_2(\mathbf{Z}/l)$ and the automorphism $\bar{\varphi}$ of $\mathrm{PGL}_2(\mathbf{Z}/l)$. The kernel of $\bar{\pi}$ is just the mod l "reduction" of H, which is canonically identified with H, due to how H is defined.

Functoriality and the inflation-restriction sequence therefore yield the commutative diagram

$$\begin{array}{ccc} H^2(\mathrm{PGL}_2(\mathbf{Z}/l^n)/\pi(P), H) & \xrightarrow{\beta} & H^2(\mathrm{PGL}_2(\mathbf{Z}/l^n), H) \\ \downarrow \psi^* & & \downarrow (\varphi \circ \pi)^* \\ H^2(\Gamma/K, H) & \xrightarrow{\sim} & H^2(\Gamma, H). \end{array} \qquad (4)$$

in which the bottom row is an isomorphism and the left column is identified with the map

$$(\bar{\varphi} \circ \bar{\pi})^*: H^2(\mathrm{PGL}_2(\mathbf{Z}/l), H) \hookrightarrow H^2(GL_2(\mathbf{Z}/l), H).$$

The cohomology class $\bar{\phi}$ in $H^2(\mathrm{PGL}_2(\mathbf{Z}/l), H)$ corresponding to the central extension

$$1 \to H \to GL_2(\mathbf{Z}/l) \xrightarrow{\bar{\pi}} \mathrm{PGL}_2(\mathbf{Z}/l) \to 1 \qquad (5)$$

satisfies $\beta(\bar{\phi}) = \phi$. Thus, $(\varphi \circ \pi)^* \phi = 0$ if and only if $(\bar{\varphi} \circ \bar{\pi})^* (\bar{\phi}) = 0$, which is to say that the automorphism $\bar{\varphi}$ of $\mathrm{PGL}_2(\mathbf{Z}/l)$ can be lifted to an automorphism of $\mathrm{GL}_2(\mathbf{Z}/l)$. The liftability of all such automorphisms is classical [2, Thm. V.5]. ∎

For any ring R, if φ is an automorphism of $\mathrm{GL}_2(R)$, then φ takes the diagonal matrices of $\mathrm{GL}_2(R)$ to themselves (since these matrices constitute the center of $\mathrm{GL}_2(R)$). Thus φ induces a group homomorphism $r_\varphi: R^\times \to R^\times$.

LEMMA 5. *Let R be a local ring whose residue field is not $\mathbf{F}_2$. Then every automorphism φ of $\mathrm{GL}_2(R)$ takes $\mathrm{SL}_2(R)$ to itself. Moreover, if φ_1 and φ_2 are two automorphisms of $\mathrm{GL}_2(R)$, then φ_1 and φ_2 coincide on $\mathrm{SL}_2(R)$ if and only if there is a map of groups $\lambda: R^\times \to R^\times$ such that $\varphi_1(g) = \lambda(\det(g))\, \varphi_2(g)$ for all $g \in \mathrm{GL}_2(R)$. Conversely, for any map of groups $\lambda: R^\times \to R^\times$ and any automorphism φ of $\mathrm{GL}_2(R)$, $\lambda^2 r_\varphi$ is an automorphism of $R^\times$ if and only if the map $g \mapsto \lambda(\det(g))\, \varphi(g)$ defines an automorphism of $\mathrm{GL}_2(R)$.*

Proof. For a local ring R as above, the commutator subgroup of $\mathrm{GL}_2(R)$ is $\mathrm{SL}_2(R)$ [1, Thm 4.1, Prop 9.2]. The first part of the lemma then follows, and any group map $\mathrm{GL}_2(R) \to R^\times$ must factor through the determinant map. To prove the second part, it suffices to consider an endomorphism φ of the group $\mathrm{GL}_2(R)$ such that φ is the identity on $\mathrm{SL}_2(R)$, and to show that $\varphi(g) = \lambda(\det(g))\, g$ for all $g \in \mathrm{GL}_2(R)$, where

$\lambda\colon R^\times \to R^\times$ is some map of groups. Pick an element $\mu \in R^\times$ and write $\varphi\left(\begin{smallmatrix}1&0\\0&\mu\end{smallmatrix}\right) = \left(\begin{smallmatrix}x&y\\z&w\end{smallmatrix}\right)$. We have the identities

$$\begin{pmatrix}1&0\\0&\mu\end{pmatrix}\begin{pmatrix}1&\lambda\\0&1\end{pmatrix}\begin{pmatrix}1&0\\0&\mu\end{pmatrix}^{-1} = \begin{pmatrix}1&\lambda/\mu\\0&1\end{pmatrix},$$
$$\begin{pmatrix}1&0\\0&\mu\end{pmatrix}\begin{pmatrix}1&0\\\lambda&1\end{pmatrix}\begin{pmatrix}1&0\\0&\mu\end{pmatrix}^{-1} = \begin{pmatrix}1&0\\\lambda\mu&1\end{pmatrix}.$$

Since φ is trivial on $\mathrm{SL}_2(R)$, applying φ to these identities and comparing the entries yields $y = z = 0$ and $\mu = w/x$. Thus $\varphi\left(\begin{smallmatrix}1&0\\0&\mu\end{smallmatrix}\right) = \lambda(\mu)\left(\begin{smallmatrix}1&0\\0&\mu\end{smallmatrix}\right)$ for some $\lambda(\mu) \in R^\times$. Since φ is multiplicative, λ is an endomorphism of the group $R^\times$. Every element g of $\mathrm{GL}_2(R)$ can be written uniquely as $g'\left(\begin{smallmatrix}1&0\\0&\det(g)\end{smallmatrix}\right)$ with $g' \in \mathrm{SL}_2(R)$, so $\varphi(g) = \lambda(\det(g))\,g$ for all $g \in \mathrm{GL}_2(R)$.

Finally, let φ be an automorphism of the group $\mathrm{GL}_2(R)$ and let $\lambda\colon R^\times \to R^\times$ be a map of groups. Then $\varphi_\lambda\colon g \mapsto \lambda(\det(g))\,\varphi(g)$ is an endomorphism of $\mathrm{GL}_2(R)$ which induces an automorphism on $\mathrm{SL}_2(R)$. Suppose

$$\varphi_\lambda(g) = \varphi_\lambda(h) \tag{6}$$

for some $g, h \in \mathrm{GL}_2(R)$. Then $\lambda(\det(g))\,\lambda(\det(h))^{-1}\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right) = \varphi(g^{-1}h)$. Since φ induces an automorphism of the scalar matrices, we have $h = g\left(\begin{smallmatrix}s&0\\0&s\end{smallmatrix}\right)$ for some $s \in R^\times$. Since φ_λ is a homomorphism, it follows from (6) that $\varphi_\lambda(h) = \varphi_\lambda(g)\,\varphi_\lambda\left(\begin{smallmatrix}s&0\\0&s\end{smallmatrix}\right)$, and hence $\lambda^2(s)\,r_\varphi(s) = 1$. Conversely, if $(\lambda^2 r_\varphi)(s) = 1$ for some $s \in R^\times$, then $\varphi_\lambda\left(\begin{smallmatrix}s&0\\0&s\end{smallmatrix}\right) = 1$. Thus φ_λ is injective if and only if $\lambda^2 r_\varphi$ is injective.

Denote by $\mathscr{S}$ the subgroup of $\mathrm{GL}_2(R)$ generated by $\mathrm{SL}_2(R)$ and by the scalar matrices. Note that φ_λ takes $\mathscr{S}$ to itself, and induces an automorphism of $\mathscr{S}$ if φ_λ is an automorphism. Since $\varphi_\lambda\left(\begin{smallmatrix}\beta&0\\0&\beta\end{smallmatrix}\right) = \lambda^2 r_\varphi(\beta)\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)$, we conclude that $\lambda^2 r_\varphi$ is an automorphism (of the scalar matrices) if and only if φ_λ induces an automorphism of $\mathscr{S}$. Thus φ_λ always induces a map $\tilde{\varphi}_\lambda$ on $\mathrm{GL}_2(R)/\mathscr{S}$, and φ_λ is an automorphism if and only if $\lambda^2 r_\varphi$ is an automorphism and $\tilde{\varphi}_\lambda$ is surjective on $\mathrm{GL}_2(R)/\mathscr{S}$. But the action of $\tilde{\varphi}_\lambda$ on $\mathrm{GL}_2(R)/\mathscr{S}$ is the same as that of φ on $\mathrm{GL}_2(R)/\mathscr{S}$, which is surjective since φ is an automorphism of $\mathrm{GL}_2(R)$, so we are done. ∎

LEMMA 6. *Let $l = 3$ or 5, and let $n > 1$. Let $v, t \in \mathbf{Z}/l^n$ be divisible by l^{n-1}, with $t = 0$ or 3 if $l = 3$ and $n = 2$. Then the following*

$$\begin{pmatrix}1&1\\0&1\end{pmatrix} \mapsto \begin{pmatrix}1&1\\t&1+t\end{pmatrix}, \qquad \begin{pmatrix}0&-1\\1&0\end{pmatrix} \mapsto \begin{pmatrix}0&t-1\\t+1&0\end{pmatrix},$$
$$\begin{pmatrix}\alpha&0\\0&1\end{pmatrix} \mapsto \begin{pmatrix}\alpha&v\\v&1\end{pmatrix}, \qquad \begin{pmatrix}\beta&0\\0&\beta\end{pmatrix} \mapsto \begin{pmatrix}\beta&0\\0&\beta\end{pmatrix}$$

determine a unique automorphism $\phi_{v,t}$ *of* $\mathrm{GL}_2(\mathbf{Z}/l^n)$, *and* $\phi_{v,t}$ *is determinant-preserving. When* $v \neq 0$ *or* $t \neq 0$, *then* $\phi_{v,t}$ *is not an inner automorphism.*

Every automorphism of $\mathrm{GL}_2(\mathbf{Z}/l^n)$ *has the form*

$$\phi_{v,t,\lambda,h}: g \mapsto \lambda(\det(g))\, h\phi_{v,t}(g)\, h^{-1}$$

for $h \in \mathrm{GL}_2(\mathbf{Z}/l^n)$ *and a map of groups* $\lambda: (\mathbf{Z}/l^n)^\times \to (\mathbf{Z}/l^n)^\times$. *Such automorphisms take elements with trace zero to elements with trace zero. Finally, for any* v, t, λ, h *as above, the map* $\phi_{v,t,\lambda,h}$ *is an automorphism of* $\mathrm{GL}_2(\mathbf{Z}/l^n)$ *if and only if* $\lambda^2(a) \neq a^{-1}$ *for all* $a \in (\mathbf{Z}/l^n)^\times$ *with* $a \neq 1$.

Proof. With t and v as in the lemma, it follows from [9, Thm. 3] and our hypothesis that $l=3$ or $l=5$ that

$$\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix} \mapsto \begin{pmatrix}1 & 1\\ t & t+1\end{pmatrix}, \quad \begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix} \mapsto \begin{pmatrix}0 & t-1\\ t+1 & 0\end{pmatrix}, \quad \begin{pmatrix}\alpha & 0\\ 0 & 1\end{pmatrix} \mapsto \begin{pmatrix}\alpha & v\\ v & 1\end{pmatrix} \tag{7}$$

determines a unique automorphism $\varphi_{v,t}$ of $\mathrm{PGL}_2(\mathbf{Z}/l^n)$, and that every automorphism of $\mathrm{PGL}_2(\mathbf{Z}/l^n)$ is the compositum of an inner one with some $\varphi_{v,t}$. Moreover, by [9, Cor 2] and our hypothesis that $l=3$ or $l=5$, the first two conditions in (7) determine a unique automorphism of $\mathrm{SL}_2(\mathbf{Z}/l^n)$. Since $-1 \in (\mathbf{Z}/l^n)^\times$ does not have l-power order, by Lemma 4 and our earlier observation that $\mathrm{SL}_2(\mathbf{Z}/l^n) \subseteq \Gamma$ is stable under $\mathrm{Aut}(\Gamma)$ we see that there exists an automorphism $\Phi_{v,t}$ of Γ satisfying the first two conditions of (7), with

$$\Phi_{v,t}\begin{pmatrix}\alpha & 0\\ 0 & 1\end{pmatrix} = \begin{pmatrix}\alpha & v\\ v & 1\end{pmatrix}\begin{pmatrix}\gamma & 0\\ 0 & \gamma\end{pmatrix}$$

for some $\gamma \in (\mathbf{Z}/l^n)^\times$. Since $\left(\begin{smallmatrix}\alpha & v\\ v & 1\end{smallmatrix}\right)$ has order $l-1$ in $\mathrm{GL}_2(\mathbf{Z}/l^n)$, we have $\gamma^{l-1}=1$, so we can write

$$\Phi_{v,t}\begin{pmatrix}\alpha & 0\\ 0 & 1\end{pmatrix} = \det\begin{pmatrix}\alpha & 0\\ 0 & 1\end{pmatrix}^A \begin{pmatrix}\alpha & v\\ v & 1\end{pmatrix}$$

for some $A \in \mathbf{Z}$. The scalars in Γ are the powers of $\left(\begin{smallmatrix}\alpha & 0\\ 0 & \alpha\end{smallmatrix}\right)$ since $l>2$, and it is easy to compute that

$$\begin{pmatrix}\alpha & 0\\ 0 & \alpha\end{pmatrix} = \begin{pmatrix}\alpha & 0\\ 0 & 1\end{pmatrix}\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}\begin{pmatrix}\alpha & 0\\ 0 & 1\end{pmatrix}\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}^{-1},$$

so $\Phi_{v,t}$ acts as multiplication by α^{2A} on $\left(\begin{smallmatrix}\alpha & 0\\ 0 & \alpha\end{smallmatrix}\right)$. Since $\mathrm{GL}_2(\mathbf{Z}/l^n)$ is generated by the commuting subgroups Γ and $(\mathbf{Z}/l^n)^\times$ (i.e., the scalar matrices), we can extend $\det^{-A}\Phi_{v,t}$ to an endomorphism $\phi_{v,t}$ of the group $\mathrm{GL}_2(\mathbf{Z}/l^n)$ by letting it acts trivially on the scalar matrices. It is easy to see that $\phi_{v,t}$ is an automorphism. Moreover, since $\phi_{v,t}$ does not preserve the trace function if $t \neq 0$, it is easy to see that $\phi_{v,t}$ is not an inner automorphism unless $v = t = 0$, in which case it is the identity.

If φ is an automorphism of $\mathrm{GL}_2(\mathbf{Z}/l^n)$, then by [9, Cor. 2] the restriction of φ to $\mathrm{SL}_2(\mathbf{Z}/l^n)$ coincides with that of the composite of some $\phi_{v,t}$ with an inner automorphism. Applying the last part of Lemma 5 and noting that $r_{\phi_{v,t,1,h}}$ is the identity map for any v and t, we have now determined the automorphisms of $\mathrm{GL}_2(\mathbf{Z}/l^n)$.

Finally, since $l > 2$, the trace zero elements of $GL_2(\mathbf{Z}/l^n)$ are precisely those whose squares are scalar matrices. Thus, they are taken to themselves under any automorphism, as desired. ∎

4. TWISTED MODULAR CURVES

In this section, we fix a positive integer $N \geqslant 3$ and let S be a $\mathbf{Z}[1/N]$-scheme. Denote by $\mathbf{Sch}_{/S}$ and **Sets** the category of S-schemes and sets, respectively. We define the (open) modular curve $Y(N)$ over S as in [5, Cor. 4.7.2]. For any S-scheme T, we will denote $Y(N) \times_S T$ by $Y(N)$ when T is understood from context.

Given an elliptic curve E over a S-scheme T, denote by $E[N]$ the N-torsion subgroup scheme of E. Since N is invertible over S, the finite locally free commutative group scheme $E[N]$ is étale over T and after a finite étale surjective base change is isomorphic to the constant group scheme $(\underline{\mathbf{Z}/N})^2$. For any finite étale commutative group scheme G over S which is étale locally isomorphic to the constant group scheme $(\underline{\mathbf{Z}/N})^2$, we denote by $\det G$ the finite étale S-group scheme which represents the étale sheaf $\wedge^2_{\underline{\mathbf{Z}/N}}(G)$.

The following result is well-known to experts, but for the sake of completeness (and to assist the non-expert reader), we give a proof via reduction to standard results which are completely proven in [5].

THEOREM 2. *Let S and G be as above. For $N \geqslant 3$, the functor F_G: $\mathbf{Sch}_{/S} \to$ **Sets** given by*

$$T \mapsto \left\{ \begin{array}{c} \textit{isomorphism classes of pairs } (E, \alpha), \textit{ with } E_{/T} \textit{ an elliptic curve} \\ \textit{and } \alpha\colon E[N] \simeq G \times_S T \textit{ an isomorphism of } T\textit{-group schemes} \end{array} \right\}$$

is represented by an S-scheme $Y(G)$ which becomes isomorphic to $Y(N)$ over a finite étale cover of S (so $Y(G) \to S$ is smooth and affine of pure relative dimension 1).

Suppose we are given an isomorphism of S-group schemes i: $\det G \simeq \mu_N$. *Then for* $N \geqslant 3$, *the functor* F_G^i: $\mathbf{Sch}_{/S} \to \mathbf{Sets}$ *given by*

$$T \mapsto \left\{ \begin{array}{c} \textit{isomorphism classes of pairs } (E, \alpha), \textit{ such that } E_{/T} \textit{ is an elliptic} \\ \textit{curve, } \alpha\colon E[N] \simeq G \times_S T \textit{ is an isomorphism of } T\textit{-group schemes,} \\ \textit{and } \det \alpha\colon \det E[N] \simeq (\det G) \times_S T \simeq^{i} \mu_{N_{/T}} \textit{ is the Weil pairing} \end{array} \right\}$$

is represented by an open and closed subscheme $Y(G, i)$ *in* $Y(G)$, *and* $Y(G)$ *is covered by the disjoint open subschemes* $Y(G, i^n)$ *for* $n \in (\mathbf{Z}/N)^\times$, *where the isomorphism* i^n *is the composite of* i *and the* n*th power map on* μ_N. *The scheme* $Y(G, i)$ *has geometrically connected fibers over* S.

Proof. We begin by showing that the functor F_G on $\mathbf{Sch}_{/S}$ is an étale sheaf. Since F_G is trivially a Zariski sheaf (due to the rigidity of level N structures for $N \geqslant 3$ [5, Cor. 2.7.2]), it remains to show that if $T' \to T$ is a quasi-compact étale surjective map of S-schemes, then the diagram of sets

$$F_G(T) \to F_G(T') \rightrightarrows F_G(T' \times_T T') \tag{8}$$

is exact. Indeed, once such exactness is proven we can use étale descent theory to see that the representability of F_G by an affine smooth S-scheme with pure relative dimension 1 can be checked after we make a finite étale surjective base change $S' \to S$ (the effectiveness of the descent data on affine S'-schemes with respect to $S' \to S$ follows from [4, Cor. 7.6, Exp. VIII]). We can find such a base change so that $G \times_S S' \simeq (\underline{\mathbf{Z}/N})^2$, so the representability over S' by the affine smooth S'-scheme $Y(N)$ with pure relative dimension 1 follows from [5, Cor. 4.7.2].

By the rigidity of level N structures for $N \geqslant 3$, $F_G(T) \to F_G(T')$ is injective. Indeed, if (E_1, α_1), (E_2, α_2) over T become isomorphic over T', via an isomorphism φ': $E_1 \simeq E_2$ over T' that takes α_1' to α_2', then both pullbacks of φ' to $T'' = T' \times_T T'$ take α_1'' to α_2''. By rigidity, we conclude that the two pullbacks of φ' to $T' \times_T T'$ coincide, so by fpqc descent of morphisms we have $\varphi' = \varphi \times_T T'$ for a unique map φ: $E_1 \to E_2$ which is necessarily an isomorphism of elliptic curves taking α_1 to α_2, as these properties all hold after the fpqc base change $T' \to T$. This establishes injectivity on the left of (8).

Now suppose that for some (E', α') in $F_G(T')$ there is an isomorphism φ: $(E_1, \alpha_1) \simeq (E_2, \alpha_2)$ over $T'' = T' \times_T T'$, where (E_i, α_i) is the base change by the ith projection $T'' \to T'$. We want to construct an (E, α) in $F_G(T)$ inducing (E', α') in $F_G(T')$. By descent of schemes (using canonical projectiveness of elliptic curves to get effectiveness of descent data [4, Prop. 7.8, Exp. VIII]), it suffices to check that φ satisfies a "cocycle" condition. But this condition over $T' \times_T T' \times_T T'$ is forced by the rigidity of level N structures for $N \geqslant 3$. This yields the desired exactness, so F_G is indeed an étale sheaf on $\mathbf{Sch}_{/S}$. As we noted above, this implies the first part of the theorem, via reduction to the special case $G=(\underline{\mathbf{Z}/N})^2$.

To prove the second part of the theorem, denote by $E^{\text{univ}} \to Y(G)$ the universal elliptic curve over $Y(G)$. The Weil pairing and $\det \alpha$ give rise to a composite isomorphism

$$j\colon \mu_N \simeq \det E^{\text{univ}}[N] \simeq \det(G) \overset{i}{\simeq} \mu_N$$

over $Y(G)$, which is an automorphism μ_N over $Y(G)$. Since $\underline{\text{Aut}}(\mu_N) \simeq (\underline{\mathbf{Z}/N})^{\times}$ as étale sheaves on $\mathbf{Sch}_{/S}$, j must be given Zariski locally on $Y(G)$ by raising to the dth power for various $d \in (\mathbf{Z}/N)^{\times}$. It is obvious that $F_G^{i^n}$ is represented by the open and closed subscheme $Y(G, i^n)$ corresponding to $d=n$, and as n runs through the elements of $(\mathbf{Z}/N)^{\times}$, the $Y(G, i^n)$'s give a covering of $Y(G)$ by disjoint open subschemes. Passing to geometric fibers, we may study the geometric connectedness of the fibers in the case $S=\operatorname{Spec} k$, with k an algebraically closed field of characteristic not dividing N and $G=(\underline{\mathbf{Z}/N})^2$. In this case, $\det G \simeq^{i} \mu_N$ corresponds to a choice of primitive Nth root of unity $\zeta_N \in \mu_N(k)$. This choice makes k a $\mathbf{Z}[1/N, \zeta_N]$-algebra and $Y(G, i)$ is exactly the k-fiber of the $\mathbf{Z}[1/N, \zeta_N]$-scheme $Y(N)^{\text{can}}$ as defined in [5, 9.1.6]. However, it follows from [5, 10.9.2(2)] (which makes essential use of the complex analytic theory of modular curves and its compatibility with the algebraic theory) that $Y(N)^{\text{can}}$ has geometrically connected fibers over $\mathbf{Z}[1/N, \zeta_N]$. ∎

5. PROOF OF THEOREM 1

Let $n>1$ and choose a prime $l=3$ or 5. Fix a number field K which is linearly disjoint from $\mathbf{Q}(\zeta_{l^n})$. Choose any $r \in (\mathbf{Z}/l)^{\times}$ which is not a square. Let $\mathcal{O}$ be the integer ring of K. By the Cebotarev density theorem and the linear disjointness of K and $\mathbf{Q}(\zeta_l)$, there exist infinitely many primes $p \neq l$ in $\mathbf{Z}$ such that p is totally split in K and $p \equiv -r \pmod{l}$. Fix a choice of such a p. In particular, X^2+p does not have a root in the finite field $\mathbf{F}_l$. By Honda–Tate theory [8], there exists an elliptic curve $\bar{E}_p$ over $\mathbf{F}_p$ which is supersingular, which is to say that the characteristic polynomial of the arithmetic Frobenius action on the l-adic Tate module of $\bar{E}_p$ is X^2+p. Fix a choice of such a $\bar{E}_p$ and choose a Weierstrass model for this over $\mathbf{F}_p$. Pick a prime $\mathfrak{p}$ of K over p and choose a Weierstrass equation over $\mathcal{O}_{\mathfrak{p}}$ whose reduction is the equation for $\bar{E}_p$. This defines an elliptic curve E_1 over $\mathcal{O}_{\mathfrak{p}}$ with reduction at $\mathfrak{p}$ isomorphic to $\bar{E}_p$. Thus, the G_K-module action on $E_1[l](\bar{K})$ must be irreducible, since X^2+p has no roots in $\mathbf{F}_l$, and the same holds for any elliptic curve over K given by a Weierstrass equation which is $\mathfrak{p}$-adically close to that of E_1.

Choose any prime $\mathfrak{q}$ of K not equal to $\mathfrak{p}$ and not lying over l. From the theory of Tate curves [7, Ch. V, Thm. 5.3], we can find a Weierstrass equation over K which defines an elliptic curve E_2 over K with split multiplication reduction at $\mathfrak{q}$ and $\mathrm{ord}_{\mathfrak{q}}(j(E_2)) = -1$. Moreover, any Weierstrass equation over K which is $\mathfrak{q}$-adically close to that of E_2 will also have these properties. Now consider any elliptic curve E/K defined by a Weierstrass equation which is $\mathfrak{p}$-adically close to E_1 and $\mathfrak{q}$-adically close to E_2. Clearly there are infinitely many j-invariant values $j(E) \in K$ which arise in this way, and (by weak approximation) we can even find such E with good reduction at any desired finite set of places away from $\mathfrak{q}$, and split multiplicative reduction at $\mathfrak{q}'$ with $\mathrm{ord}_{\mathfrak{q}'}(j(E)) = -1$ for any desired finite set of other places $\mathfrak{q}'$ away from $\mathfrak{p}$. In particular, we can find an infinite set of such E's so that the sets of ramified primes in the mod-l^n representations of G_K are non-empty and mutually disjoint away from l.

We claim that the representation $\rho_{E,l^n}: G_K \to \mathrm{Aut}(E[l^n](\bar{K})) \simeq \mathrm{GL}_2(\mathbf{Z}/l^n)$ is surjective for all such E. Since K is linearly disjoint from $\mathbf{Q}(\zeta_{l^n})$, it suffices to prove that $\mathrm{SL}_2(\mathbf{Z}/l^n)$ lies in the image of ρ_{E,l^n}. From the Tate parameterization of elliptic curves with split multiplicative reduction and the condition $\mathrm{ord}_{\mathfrak{q}}(j(E)) = -1$, there is a basis $\{e_1, e_2\}$ of $E[l^n](\bar{K})$ over $\mathbf{Z}/l^n$ with respect to which $\sigma = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ lies in the image of ρ_{E,l^n} on the inertia group at $\mathfrak{q}$. Since $\rho_{E,l^n} \pmod{l}$ is irreducible, there exists $g \in G_K$ such that $e_2' = ge_1 \notin (\mathbf{Z}/l^n)e_1$. With respect to the basis $\{e_1, e_2'\}$, the automorphism σ becomes $\left(\begin{smallmatrix} 1 & \alpha \\ 0 & 1 \end{smallmatrix}\right)$, whence $g\sigma g^{-1} = \left(\begin{smallmatrix} 1 & 0 \\ \beta & 1 \end{smallmatrix}\right)$, with $\alpha, \beta \in \mathbf{Z}/l^n$. Since $\left(\begin{smallmatrix} 1 & \alpha \\ 0 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & 0 \\ \beta & 1 \end{smallmatrix}\right)$ are conjugate to $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ in $\mathrm{GL}_2(\mathbf{Z}/l^n)$, these matrices have order l^n. Consequently, the image of ρ_{E,l^n} contains $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$, which generate $\mathrm{SL}_2(\mathbf{Z}/l^n)$. Thus the image of ρ_{E,l^n} contains $\mathrm{SL}_2(\mathbf{Z}/l^n)$, so the representation ρ_{E,l^n} is surjective, as desired. Fix such an E as above and choose a basis of $E[l^n](\bar{K})$ over $\mathbf{Z}/l^n$. Let $\rho = \rho_{E,l^n}: G_K \to \mathrm{GL}_2(\mathbf{Z}/l^n)$ be the corresponding representation.

Let $\phi = \phi_{v,t}$ be an automorphism of $GL_2(\mathbf{Z}/l^n)$ as furnished by Lemma 6 with $v, t \not\equiv 0 \pmod{l^n}$. Define $\rho' = \phi \circ \rho$, and let $\bar{\rho}'$ be the induced mod-l representation. Note that by the definition of $\phi_{v,t}$, the mod-l representation $\bar{\rho}$ obtained from ρ is literally equal to $\bar{\rho}'$. However, ρ and ρ' are *not* equivalent up to a twist. To see this, we note that if ρ and ρ' were equivalent up to a twist, then the corresponding projective representations would be conjugate. Since ρ is surjective and $\rho' = \phi_{v,t} \circ \rho$, it would follow that $\phi_{v,t}$ induces an inner automorphism of $\mathrm{PGL}_2(\mathbf{Z}/l^n)$, a contradiction (due to our choices of v and t).

Viewing ρ' and $\bar{\rho}'$ as finite étale group schemes over K with cyclotomic determinant, we denote by $X(\rho')$ and $X(\bar{\rho}')$ the canonical compactifications of the smooth affine curves as furnished by the first part of Theorem 2. There is an obvious natural K-morphism $\pi: X(\rho') \to X(\bar{\rho}')$ which corresponds (away from the cuspidal part) to "reduction mod l" in terms of

Yoneda's lemma. By the second part of Theorem 2, the connected components of $X(\rho')$ and $X(\bar{\rho}')$ are geometrically connected over K. We claim that the induced maps between connected components have degree $l^{3(n-1)}$ (and in particular, π is finite flat). This can be checked after base change to $\bar{K}$, over which π becomes the canonical map $X(l^n)\times_{\mathbf{Z}[1/l]}\bar{K}\to X(l)\times_{\mathbf{Z}[1/l]}\bar{K}$, which is well-known to be a generically Galois covering between connected components, with Galois group $\ker(\mathrm{PSL}_2(\mathbf{Z}/l^n)\to \mathrm{PSL}_2(\mathbf{Z}/l))$ having order $l^{3(n-1)}$ (moreover, the branch locus is supported in the *cuspidal part*).

Since $l=3$ or $l=5$ and the genus of a proper smooth geometrically connected curve over a field can be computed after arbitrary change of the base field, the connected components of the proper smooth K-curve $X(\bar{\rho}')=X(\bar{\rho})$ have genus 0. We claim that each of these connected components is K-isomorphic to $\mathbf{P}^1_K$. Let X be one of the connected components of $X(\bar{\rho}')=X(\bar{\rho})$, so X is a proper smooth *geometrically connected* curve over K with genus 0. In order to show that $X\simeq\mathbf{P}^1_K$, it suffices to show that $X(K)$ is non-empty. There is a connected component X_1 of $X(\bar{\rho}')=X(\bar{\rho})$ which contains a K-rational point corresponding to the given elliptic curve E over K and the identity of G_K-modules $E[l](\bar{K})=\bar{\rho}$. Since $X_1(K)$ is non-empty, $X_1\simeq\mathbf{P}^1_K$. It suffices below to just work with this component, but we want to briefly explain Mazur's elegant proof of the stronger result that all connected components of $X(\bar{\rho}')$ are K-isomorphic to $\mathbf{P}^1_K$.

We see from the proof of Theorem 2 that the connected components of $X(\bar{\rho})$ are indexed by elements v of $(\mathbf{Z}/l)^\times$ (i.e., automorphisms of μ_l), and there is an obvious K-isomorphism of connected components $X_v\simeq X_{vw^2}$ for any two $v, w\in(\mathbf{Z}/l)^\times$, by using Yoneda's Lemma and "multiplication by w" on the level of l-torsion group schemes. Thus, to show that all connected components of $X(\bar{\rho}')=X(\bar{\rho})$ are K-isomorphic to $\mathbf{P}^1_K$, it suffices to show that $X_v\simeq\mathbf{P}^1_K$ for a single non-square $v\in(\mathbf{Z}/l)^\times$. Since $l=3$ or $l=5$, we may consider $v=2$. It is a classical observation that in order to show $X(K)$ is non-empty, it suffices to construct a divisor D on X with odd degree. Indeed, adding a suitable multiple of the canonical divisor (which has degree -2) to D gives a divisor D' on X with degree 1. By the Riemann–Roch Theorem for the *geometrically connected* proper smooth curve X over K, we have $H^0(X,\mathscr{L}(D'))=1>0$, so there is an effective divisor on X with degree 1, which is to say that $X(K)$ is non-empty. Thus, it suffices to construct a divisor with odd degree on X_2. Mazur observed that an étale-twisted version of the Hecke operator T_2 gives a correspondence between X_1 and X_2 with degree 3 over both X_1 and X_2. By using this correspondence and the existence of a K-rational point on X_1, we can construct an effective divisor on X_2 with odd degree (1 or 3). This completes the sketch of Mazur's proof that every connected component of $X(\bar{\rho}')$ is K-isomorphic to $\mathbf{P}^1_K$.

Fix a connected component $C \simeq \mathbf{P}^1_K$ of $X(\bar{\rho}')$ and a connected component C' in $X(\rho')$ over C, so $\pi_{C'}: C' \to C$ is a finite map with degree $l^{3(n-1)}$. By Theorem 2, the proper smooth curve C' over K is geometrically connected. Therefore, by Theorem 1, there exist infinitely many non-cuspidal $a \in C(K)$ such that $\pi_{C'}^{-1}(a) = \mathrm{Spec}(L_a)$, where L_a is a finite extension of K which is linearly disjoint from the splitting field of ρ (which coincides with the splitting field of ρ'). Obviously $[L_a : K]$ is equal to the degree of $\pi_{C'}$, which is $l^{3(n-1)}$. From the linear disjointness, it follows that the representations $\rho|_{G_{L_a}}$ and $\rho'|_{G_{L_a}}$ are surjective and come from the mod-l^n representations of elliptic curves over L_a with j-invariants in K (since $a \in C(K)$). Of course, we can choose these j-invariants to avoid any desired finite set of elements of K. By the the choice of ϕ, $\rho|_{G_{L_a}}$ and $\rho'|_{G_{L_a}}$ satisfy the condition (1) in the Introduction and are not equivalent up to twists.

It remains to analyze ramification in L_a/K. Recall that in our construction of elliptic curves above via Tate models, we saw that we can choose the mod-l^n representation ρ coming from our elliptic curve E over K to be ramified at any desired finite set of primes of K away from l and to be unramified at any desired finite set of other primes of K away from l. In order to complete the proof of the theorem, we need to check that the ramification in L_a outside of l can be chosen to avoid any desired finite set of primes of K with norm $> (l^2 - 3)/2$.

Choose a prime $\mathfrak{p}$ of K not over l at which E has good reduction. Thus, ρ and ρ' are *unramified* at $\mathfrak{p}$. By étale descent, we can identify ρ' with the generic fiber of a finite étale group scheme $\mathscr{G}$ over $\mathcal{O}_\mathfrak{p}$ which is étale-locally isomorphic to the constant group scheme $(\underline{\mathbf{Z}/l^n})^2$. The l-torsion subgroupscheme $\mathscr{G}[l] \simeq \mathscr{G}/l^{n-1}$ is an analogous $\mathcal{O}_\mathfrak{p}$-model for $\bar{\rho}'$. Since $\mathcal{O}_\mathfrak{p}$ is a $\mathbf{Z}[1/l]$-scheme, we can use Theorem 2 and the compactification theory of modular curves [5, 8.6.7, 10.9.5] to realize the map $\pi: X(\rho') \to X(\bar{\rho}')$ as the K-fiber of a finite flat map $\pi_\mathfrak{p}: X(\mathscr{G}) \to X(\mathscr{G}[l])$ between proper smooth $\mathcal{O}_\mathfrak{p}$-schemes with geometric fibers of pure dimension 1. This map $\pi_\mathfrak{p}$ is just an étale twist of the finite flat map $X(l^n) \times_{\mathbf{Z}[1/l]} \mathcal{O}_\mathfrak{p} \to X(l) \times_{\mathbf{Z}[1/l]} \mathcal{O}_\mathfrak{p}$.

Since the natural map $X(l^n) \to X(l)$ over $\mathbf{Z}[1/l]$ is Galois away from the cusps, the branch locus of $\pi_\mathfrak{p}$ is supported in the cuspidal subscheme of $X(\mathscr{G}[l])$, which is étale over $\mathcal{O}_\mathfrak{p}$ with degree $(l^2-1)/2$ (as the same holds for the cuspidal subscheme of $X(l)$ over $\mathbf{Z}[1/l]$). Consider $a \in C(K) \subseteq X(\bar{\rho}')(K) = X(\mathscr{G}[l])(K)$ as above. The scheme-theoretic closure of $a \in X(\mathscr{G}[l])(K)$ in $X(\mathscr{G}[l])$ is a point $\bar{a} \in X(\mathscr{G}[l])(\mathcal{O}_\mathfrak{p})$, by the valuative criterion for properness. If we can choose a so that the closed point of $\bar{a}$ is not a cusp, then $\pi_{C'}^{-1}(a) = \mathrm{Spec}(L_a)$ is a component of the generic fiber of the finite *étale* scheme $\pi_\mathfrak{p}^{-1}(\bar{a})$ over $\bar{a} = \mathrm{Spec}(\mathcal{O}_\mathfrak{p})$. Thus, the prime $\mathfrak{p}$ would not ramify in L_a. In order to check that a can be chosen in the manner desired, consider the connected component $\bar{C}$ of $X(\mathscr{G}[l])$ which has generic fiber C (so $\bar{a} \in \bar{C}(\mathcal{O}_{\mathfrak{p}})$). Since $\bar{C} \to \mathrm{Spec}(\mathcal{O}_{\mathfrak{p}})$ is proper and smooth with geometric fibers of pure dimension 1 and generic fiber $\mathbf{P}^1_K$, it must be the case that $\bar{C} \simeq \mathbf{P}^1_{\mathcal{O}_{\mathfrak{p}}}$, thanks to the following well-known lemma. We give a proof due to lack of an adequate reference.

LEMMA 7. *Let R be a discrete valuation ring with fraction field K, X a proper smooth R-scheme with pure relative dimension* 1 *and generic fiber $X \times_R K \simeq \mathbf{P}^1_K$. Then $X \simeq \mathbf{P}^1_R$ over R.*

Proof. Since the generic fiber of X is geometrically connected, the closed fiber is also geometrically connected [3, IV_3, 12.2.4(vi)], necessarily with genus 0. By the valuative criterion for properness, we have $X(R) = X(K)$. This set is non-empty, so choose a section $\mathrm{Spec}(R) \to X$ over R. This defines a relative effective Cartier divisor D on X over R with degree 1. By Grothendieck's theory of cohomology and base change, as well as the Riemann–Roch theorem for genus 0 curves over fields, $\mathscr{L}(D)$ is generated by its global sections $H^0(X, \mathscr{L}(D))$ and this R-module is locally free of rank 2 over R, commuting with arbitrary base change over R. Since R is local, $H^0(X, \mathscr{L}(D))$ is *free* of rank 2. Choosing a basis gives a map $X \to \mathbf{P}^1_R$ which commutes with arbitrary base change over R. We claim this map is an isomorphism. Since both sides are smooth over R, by [3, IV_4, 17.9.5] it suffices to show that the induced map on fibers over $\mathrm{Spec}(R)$ is an isomorphism. But over a field k, it is classical that for a proper, smooth, geometrically connected curve C over k with genus 0, and a rational function $f \in k(C)$ with a simple pole at a k-rational point and no other poles, the map $f: C \to \mathbf{P}^1_k$ is an isomorphism. ∎

Thus, as long as the number of rational points $|\mathcal{O}/\mathfrak{p}| + 1$ in the closed fiber of $\bar{C} \simeq \mathbf{P}^1_{\mathcal{O}_{\mathfrak{p}}}$ is larger than the degree $(l^2 - 1)/2$ ($=4$ or 12) of the cuspidal subscheme on $X(\mathscr{G}[l])$, then a $\mathfrak{p}$-adic congruence condition on $a \in C(K) = \mathbf{P}^1_K$ ensures that the closed point of $\bar{a}$ is non-cuspidal. This implies that $\bar{a}$ is disjoint from the branch locus of $\pi_{\mathfrak{p}}$, so L_a is unramified over $\mathfrak{p}$. Thus, we can indeed force $\mathfrak{p}$ to be unramified in L_a if the norm of $\mathfrak{p}$ exceeds $(l^2 - 3)/2$. The same argument allows us to handle any finite number of such $\mathfrak{p}$'s simultaneously.

ACKNOWLEDGMENTS

S.W. thanks Karl Rubin for a useful discussion on twisted modular curves. Both authors thank the referee for helpful comments.

REFERENCES

1. P. M. Cohn, On the structure of the GL_2 of a ring, *Publ. Math. IHES* **30** (1966), 5–54.
2. M. H. Dull, Automorphisms of the two-dimensional linear groups over integral domains, *Amer. J. Math.* **96** (1974), 1–40.
3. A. Grothendieck, Éléments de géométrie algébrique, *Publ. Math. IHES* **24**, **28**, **32** (1966).
4. A. Grothendieck, "Revêtements étales et groupe fondamental," Lecture Notes in Mathematics, Vol. 224, Springer-Verlag, New York, 1971.
5. N. Katz and B. Mazur, "Arithmetic Moduli of Elliptic Curves," Princeton Univ. Press, Princeton, NJ, 1985.
6. S. Lang, "Fundamentals of Diophantine Geometry," Springer-Verlag, Berlin/New York, 1983.
7. J. Silverman, "Advanced Topics in the Arithmetic of Elliptic Curves," Springer-Verlag, New York/Berlin, 1994.
8. J. Tate, Classes d'isogénie des variétes abéliennes sur un corps fini (d'aprés T. Honda), *Sém. Bourbaki* **352** (1968).
9. S. Wong, Twists of Galois representations and projective automorphisms, *J. Number Theory*, to appear.