An exceptional isomorphism between level 13 modular curves via Torelli's Theorem

Burcu Baran

The Jacobians of the modular curves $X_{\mathrm{ns}}(13)$ and $X_{\mathrm{s}}(13)$ respectively associated with the normalizers of non-split and split Cartan subgroups of level 13 are isogenous over $\mathbb{Q}$. In this note, we construct a $\mathbb{Q}$-isomorphism between these Jacobians which respects their canonical principal polarizations. In particular, we obtain a $\mathbb{Q}$-isomorphism between $X_{\mathrm{ns}}(13)$ and $X_{\mathrm{s}}(13)$; this has no known "modular" explanation.

1. Introduction

For a positive integer n, let $X(n)$ be the modular curve over $\mathbb{Q}$ with full level n structure (connected, but geometrically disconnected for $n > 2$). Let $\mathrm{C}_{ns}^+(n)$ and $\mathrm{C}_s^+(n)$ be the respective normalizers of non-split and split Cartan subgroups of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. The corresponding modular curves $X_{\mathrm{ns}}(n)$ and $X_{\mathrm{s}}(n)$, defined as the quotients $X(n)/\mathrm{C}_{ns}^+(n)$ and $X(n)/\mathrm{C}_s^+(n)$, respectively, are geometrically connected over $\mathbb{Q}$. One source motivation for studying the arithmetic properties of these curves is their relation to the following open problem.

SERRE'S UNIFORMITY PROBLEM OVER $\mathbb{Q}$: *There is a constant $C > 0$ so that if E is an elliptic curve over $\mathbb{Q}$ without complex multiplication then the Galois representation*

$$\rho_{E,p} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\mathbb{F}_p)$$

attached to the elliptic curve E is surjective for all primes $p > C$.

If this map is not surjective then its image is contained in one of the maximal proper subgroups of $\mathrm{GL}_2(\mathbb{F}_p)$. These subgroups are the "exceptional" subgroups, a Borel subgroup, the normalizer of a split Cartan subgroup, and the normalizer of a non-split Cartan subgroup. In [14], Serre showed that if $p > 13$ then the image of $\rho_{E,p}$ is not contained in an exceptional subgroup.

In [8], Mazur proved that for $p > 37$, the image of $\rho_{E,p}$ is not contained in a Borel subgroup.

Recently, in [3] Y. Bilu, P. Parent and M. Rebolledo showed that for $p \geq 11$ with $p \neq 13$ the image of $\rho_{E,p}$ is not contained in the normalizer of a split Cartan subgroup. Their method is not applicable for level 13, which they call "the cursed level". In this paper, we will explain conceptually what makes this level so special that it resists their method. The remaining open and the most difficult part of Serre's uniformity problem is finding a constant so that for primes bigger than this constant the image is not included in the normalizer of a non-split Cartan subgroup.

The elliptic curves over $\mathbb{Q}$ for which the image of $\rho_{E,p}$ is contained in the normalizer of a split Cartan subgroup are parametrized by the non-cuspidal $\mathbb{Q}$-points of $X_{\mathrm{s}}(p)$. In [3] the "split Cartan" case of Serre's uniformity problem is setted by showing that all such points of $X_{\mathrm{s}}(p)$ are CM points for $p \geq 11$ with $p \neq 13$. Their method failed to determine the rational points of $X_{\mathrm{s}}(13)$. Similarly, the elliptic curves over $\mathbb{Q}$ for which the image of $\rho_{E,p}$ is contained in the normalizer of a non-split Cartan subgroup are parametrized by the $\mathbb{Q}$-points of $X_{\mathrm{ns}}(p)$, so the open case of Serre's uniformity problem boils down determining the $\mathbb{Q}$-rational points of $X_{\mathrm{ns}}(p)$ for prime p. Not much is known about the arithmetic of $X_{\mathrm{ns}}(p)$. For $p > 2$, the curve $X_{\mathrm{ns}}(p)$ does not have any $\mathbb{Q}$-rational cusp. This makes it hard to find explicit equations for these curves, especially in the higher genus case. There has been extensive work on finding explicit equations for $X_{\mathrm{ns}}(p)$ over $\mathbb{Q}$ in low-genus cases (≤ 2), and determining their $\mathbb{Q}$-points (see [1] for a detailed discussion). There exists only one curve $X_{\mathrm{ns}}(p)$ with genus 3, the one with $p = 13$.

In [2] we computed an explicit equation for the modular curve $X_{\mathrm{ns}}(13)$. For now this is the highest level for these modular curves that has been worked out. In this particular case we used representation theory to overcome the difficulty of $X_{\mathrm{ns}}(13)$ not having a $\mathbb{Q}$-rational cusp. In the same paper we also computed an explicit equation for $X_{\mathrm{s}}(13)$. Computing this equation is easy, as the modular curves $X_{\mathrm{s}}(p)$ always have a $\mathbb{Q}$-rational cusp. In the end, it turned out that the same equation defines $X_{\mathrm{ns}}(13)$ and $X_{\mathrm{s}}(13)$, so by inspection these curves are $\mathbb{Q}$-isomorphic. Here is the main result of this paper.

Main Result: We give a conceptual construction of the $\mathbb{Q}$-isomorphism between $X_{\mathrm{ns}}(13)$ and $X_{\mathrm{s}}(13)$. As $\mathrm{S}_2(\Gamma_0(13)) = 0$, the Jacobians of $X_{\mathrm{ns}}(13)$ and $X_{\mathrm{s}}(13)$ are $\mathbb{Q}$-isogenous (see [5, 6]). We first compute the endomorphism ring of each of these Jacobians; it is the ring of integers of $K = \mathbb{Q}(\zeta_7)^+$ for each. Using the arithmetic properties of this ring and the isogeny between the

Jacobians, we construct an $\mathbb{Q}$-isomorphism between these Jacobians which respects their *canonical principal polarizations*. Thus, by Torelli's Theorem [9, Corollary 12.2] the curves $X_{\mathrm{ns}}(13)$ and $X_{\mathrm{s}}(13)$ are isomorphic over $\mathbb{Q}$. Since the curves do not have the same number of cusps, it seems unlikely to find a "modular" construction of this $\mathbb{Q}$-isomorphism.

The paper is organized as follows. In Section 2, we show that the endomorphism rings of the Jacobians of $X_{\mathrm{ns}}(13)$ and $X_{\mathrm{s}}(13)$ are $\mathcal{O}_K = \mathbb{Z}[\zeta_7]^+$. In Section 3, we use special arithmetic properties of $\mathcal{O}_K$ to show that it suffices to adjust the $\mathbb{Q}$-isogeny between the Jacobians to obtain a $\mathbb{Q}$-isomorphism between them *without* keeping track of the canonical principal polarizations. In Section 4, we control the primes dividing the degree of the $\mathbb{Q}$-isogeny between the Jacobians. In Section 5, we combine this with a study of residual Galois representations to find a $\mathbb{Q}$-isomorphism between the Jacobians.

2. Endomorphism algebras and endomorphism rings

In this section we determine the endomorphism ring of each of the Jacobian varieties of $X_{\mathrm{ns}}(13)$ and $X_{\mathrm{s}}(13)$. Let $X_0(n)$ be the usual modular curve parametrizing the isomorphism classes of elliptic curves endowed with a cyclic subgroup of order n, and let $X_0^+(n) := X_0(n)/w_n$ be its quotient by the Atkin–Lehner involution.

Notation 2.1. *We denote the Jacobians of $X_0(n)$, $X_0^+(n)$, $X_{\mathrm{s}}(n)$, and $X_{\mathrm{ns}}(n)$ by $J_0(n)$, $J_0^+(n)$, $J_{\mathrm{s}}(n)$, and $J_{\mathrm{ns}}(n)$, respectively.*

Since $X_0^+(p^2)$ is $\mathbb{Q}$-isomorphic to $X_{\mathrm{s}}(p)$, we have an isomorphism

$$J_{\mathrm{s}}(p) \simeq J_0^+(p^2)$$

over $\mathbb{Q}$. This isomorphism commutes with Hecke operators T_ℓ for $\ell \neq p$. Arguments in [5] using Faltings' isogeny theorem and representation–theoretic arguments in [6] establish an isogeny relation $J_{\mathrm{s}}(p) \sim J_0(p) \times J_{\mathrm{ns}}(p)$ over $\mathbb{Q}$ which is also Hecke-compatible away from p. Thus, away from p we have Hecke-compatible isogenies

(2.1) $$J_0^+(p^2) \sim J_{\mathrm{s}}(p) \sim J_0(p) \times J_{\mathrm{ns}}(p)$$

over $\mathbb{Q}$.

Now we focus on the case $p = 13$. Since $S_2(\Gamma_0(13)) = 0$, the isogeny relations in (2.1) become

$$(2.2) \qquad J_0^+(169) \sim J_s(13) \sim J_{ns}(13)$$

over $\mathbb{Q}$. Each of these Jacobians has dimension 3. Using SAGE, we computed a $\mathbb{C}$-basis $\{g_1, g_2, g_3\}$ for $S_2(\Gamma_0^+(169))$ consisting of normalized newforms. The $\mathbb{Q}$-algebra generated by the Hecke operators acting on this space is the cubic field $\mathbb{Q}(\zeta_7)^+$ (see [2]). By inspection, $\{g_1, g_2, g_3\}$ constitutes an orbit under the action of $\mathrm{Gal}(\mathbb{Q}(\zeta_7)^+/\mathbb{Q})$.

Notation 2.2. *In the rest of the paper we denote the cubic field $\mathbb{Q}(\zeta_7)^+$ by K.*

For any $g \in \{g_1, g_2, g_3\}$, let A_g be the abelian variety over $\mathbb{Q}$ associated to g, constructed by Shimura. The abelian variety A_g is $\mathbb{Q}$-simple of dimension 3 and we have the isogeny

$$(2.3) \qquad J_0^+(169) \sim A_g$$

over $\mathbb{Q}$. The abelian variety A_g does not have CM over $\mathbb{Q}$. Indeed, inspection of a table of Fourier coefficients of $\{g_1, g_2, g_3\}$ shows that the eigenvalues of the Frobenius automorphisms Frob_q acting on the Tate module of $J_0^+(169)$ generate a different quadratic extension of K as q varies.

Notation 2.3. *For an abelian variety A over $\mathbb{Q}$, let $End_{\mathbb{Q}}(A)$ be the endomorphism ring of A. We denote its endomorphism algebra $End_{\mathbb{Q}}(A) \otimes \mathbb{Q}$ by $End_{\mathbb{Q}}^0(A)$.*

By [12, Corollary 4.2], since A_g does not have CM, the existence of the isogeny in (2.3) implies that $\mathrm{End}_{\mathbb{Q}}^0(J_0^+(169)) \simeq K$. Thus, by (2.2) we have

$$(2.4) \qquad \mathrm{End}_{\mathbb{Q}}^0(J_s(13)) \simeq \mathrm{End}_{\mathbb{Q}}^0(J_{ns}(13)) \simeq K.$$

The field K is the $\mathbb{Q}$-algebra generated by the Hecke operators T_ℓ for $\ell \neq 13$ acting on the space $S_2(\Gamma_s(13))$ (resp. $S_2(\Gamma_{ns}(13))$); see [2] for a detailed discussion. Thus, it defines an embedding of K into $\mathrm{End}_{\mathbb{Q}}^0(J_s(13))$ (resp. $\mathrm{End}_{\mathbb{Q}}^0(J_{ns}(13))$), and these embeddings are equalities by (2.4).

Proposition 2.4. *Let J be the Jacobian of either of the curves $X_{ns}(13)$ or $X_s(13)$. The inclusion $\mathrm{End}_{\mathbb{Q}}(J) \subseteq \mathcal{O}_K$ inside $\mathrm{End}_{\mathbb{Q}}^0(J) = K$ is an equality.*

Proof. First we consider the curve $X_s(13)$ which is $\mathbb{Q}$-isomorphic to $X_0^+(169)$. Using SAGE, we find that the eigenvalues of the Hecke operator T_2 acting on $S_2(\Gamma_0^+(169))$ are zeroes of the polynomial $x^3 + 2x^2 - x - 1$ of discriminant 49. Since the discriminant of $\mathcal{O}_K$ is also equal to 49, the subring of $\mathrm{End}_{\mathbb{Q}}(J_s(13))$ generated by T_2 must be equal to $\mathcal{O}_K$.

Now consider the curve $X_{\mathrm{ns}}(13)$. As we noted earlier, there is a $\mathbb{Q}$-isogeny $f : J_{\mathrm{ns}}(13) \to J_{\mathrm{ns}}(13)$ compatible with the Hecke operator T_ℓ for every prime $\ell \neq 13$. Thus, under the isomorphism $\mathrm{End}_{\mathbb{Q}}^0(J_{\mathrm{ns}}(13)) \simeq \mathrm{End}_{\mathbb{Q}}^0(J_s(13)) = K$, the subrings of $\mathrm{End}_{\mathbb{Q}}(J_{\mathrm{ns}}(13))$ and $\mathrm{End}_{\mathbb{Q}}(J_s(13))$ generated over $\mathbb{Z}$ by the Hecke operators T_ℓ for all primes $\ell \neq 13$ are identified. Inside $\mathrm{End}_{\mathbb{Q}}(J_s(13))$ the element T_2 generates $\mathcal{O}_K$ over $\mathbb{Z}$, so the same holds for $T_2 \in \mathrm{End}_{\mathbb{Q}}(J_{\mathrm{ns}}(13))$. $\square$

3. Polarizations

In this section, we will exploit the arithmetic properties of K to obtain results about all principal polarizations of $J_{\mathrm{ns}}(13)$ and $J_s(13)$. Because of these results we will be able to avoid directly verifying the compatibility with canonical principal polarizations when searching for a $\mathbb{Q}$-isomorphism between these Jacobians.

In this section, we denote the element $\zeta_7 + \zeta_7^{-1}$ of $\mathcal{O}_K$ by ε. The following are the arithmetic facts about K that we will use:

- K has class number 1;

- the unit group $\mathcal{O}_K^\times$ is generated by the elements -1, ε and $\varepsilon + 1$.

Lemma 3.1. *The subgroup of totally positive units in $\mathcal{O}_K^\times$ is $(\mathcal{O}_K^\times)^2$.*

Proof. The lemma follows immediately by computing the signs of ε, $\varepsilon + 1$ and $\varepsilon(\varepsilon + 1)$ under the three distinct real embeddings of K.

$\square$

In Proposition 2.4, we showed that the endomorphism ring of each of the Jacobians of $X_{\mathrm{ns}}(13)$ and $X_s(13)$ is $\mathcal{O}_K$. We let $\mathcal{O}_K$ act on the dual varieties of these Jacobians via dual functoriality.

Proposition 3.2. *Let J be the Jacobian of either of the curves $X_{\mathrm{ns}}(13)$ or $X_s(13)$. Any polarization $\phi : J \to J^\vee$ is $\mathcal{O}_K$-linear.*

Proof. As ϕ is an isogeny $J \to J^\vee$, it has an inverse in $\mathrm{Hom}_{\mathbb{Q}}(J^\vee, J) \otimes \mathbb{Q}$. The Rosati involution on $K = \mathrm{End}_{\mathbb{Q}}^0(J)$ corresponding to ϕ is the algebra

homomorphism

$$\alpha \mapsto \phi \circ \alpha \circ \phi^{-1}.$$

Since $[K : \mathbb{Q}] = 3$, the field K has no nontrivial automorphism of order 2. Thus the map is the identity. Hence, the proposition follows by restricting this map to $\mathcal{O}_K$. $\qquad\square$

Now, with the following result we will be able to identify principal polarizations in a convenient manner.

Proposition 3.3. *Let J be a Jacobian variety of odd dimension of g over a field of characteristic 0, and assume $F := \mathrm{End}^0(J)$ is a totally real number field of degree g over $\mathbb{Q}$. Let $\lambda : J \simeq J^\vee$ be the canonical principal polarization of J. Then every principal polarization of J is of the form $\lambda \circ \alpha$ for some totally positive unit α in $\mathrm{End}(J)$.*

Proof. This is a basic fact; we provide a proof for the convenience of the reader. Let f be any principal polarization of J, so $f^{-1} \circ \lambda \in \mathrm{Aut}(J)$. Thus, $f = \lambda \circ u$ for some $u \in \mathrm{Aut}(J)$. Hence, we have to show that if $u \in \mathrm{Aut}(J)$ then the isomorphism $\lambda \circ u$ is a polarization if and only if u is totally positive in $\mathrm{End}(J)$.

The polarization property for an isogeny from an abelian variety to its dual can be checked after a ground field extension, so we seek to characterize those $u \in \mathrm{Aut}(J)$ such that the isomorphism $\lambda \circ u : J \to J^\vee$ becomes a polarization when viewed over $\mathbb{C}$. Consider the g-dimensional complex torus $J(\mathbb{C}) = V/L$. Since λ is a polarization, there is an associated skew-symmetric $\mathbb{R}$-bilinear form $E_\lambda : V \times V \to \mathbb{R}$ which satisfies the following Riemann relations:

1) $E_\lambda(iv, iw) = E_\lambda(v, w)$ for every $v, w \in V$,

2) the associated Hermitian form $H_\lambda(v, w) = E_\lambda(iv, w) + iE_\lambda(v, w)$ is positive-definite.

For $u \in \mathrm{Aut}(J)$, consider the skew-symmetric $\mathbb{R}$-bilinear form $E_{\lambda \circ u} : V \times V \to \mathbb{R}$ given by $E_{\lambda \circ u} = E_\lambda(u.v, w)$ for all $v, w \in V$. To determine when $\lambda \circ u$ is a polarization, we seek constraints on u so that $E_{\lambda \circ u}$ satisfies the Riemann relations. Since $L \otimes_\mathbb{Z} \mathbb{Q}$ is a 2-dimensional F-vector space, V is free of rank 2 over $F_\mathbb{R} := F \otimes_\mathbb{Q} \mathbb{R}$. Thus, since F is totally real, V is free of rank 1 over $F_\mathbb{C} := F \otimes_\mathbb{Q} \mathbb{C}$. Fix an $F_\mathbb{C}$-basis of V to identify it with $F_\mathbb{C}$. We will use this to convert our problems with V and $E_{\lambda \circ u}$ into concrete questions with $F_\mathbb{C}$. On $F_\mathbb{C} = F \otimes_\mathbb{Q} \mathbb{C}$ we define $z \mapsto \bar{z}$ via $\overline{a \otimes c} = a \otimes \bar{c}$ for $a \in F$ and $c \in \mathbb{C}$.

For any $x, y \in V$ and $a \in F$ we have $E_\lambda(ax, y) = E_\lambda(x, a^\dagger y)$ where $a \mapsto a^\dagger$ is the Rosati involution arising from λ. As in the proof of Proposition 3.2, since $[F : \mathbb{Q}]$ is odd, the Rosati involution on F is trivial. Thus, we have $E_\lambda(ax, y) = E_\lambda(x, ay)$ for all $a \in F$. The same holds for all $a \in \mathbb{R}$ since E_λ is $\mathbb{R}$-bilinear, and hence the same holds for all $a \in F_\mathbb{R}$. The first Riemann relation therefore says exactly that $E_\lambda(v, w) = E_\lambda(v\bar{w}, 1)$ for all $v, w \in F_\mathbb{C}$. The skew-symmetry property of E_λ says that $E_\lambda(v\bar{w}, 1) = -E_\lambda(w\bar{v}, 1)$. Hence, the Riemann relations are:

- $E_\lambda(v, w) = \ell(v\bar{w})$ for an $\mathbb{R}$-linear map $\ell : F_\mathbb{C} \to \mathbb{R}$ such that $\ell(z) = -\ell(\bar{z})$ for all $z \in F_\mathbb{C}$,

- $\ell(iz) + i\ell(z) > 0$ whenever $z \in F_\mathbb{C} = \mathbb{C}^g$ has all components in $\mathbb{R}_{>0}$ (since those are the elements of the form $v\bar{v}$ for $v \in F_\mathbb{C}^\times$). It is equivalent to say $\ell(iz) > 0$ whenever $z \in F_\mathbb{C}$ has all components in $\mathbb{R}_{>0}$, as E_λ is a skew-symmetric form (so $E_\lambda(v, v) = 0$).

Since $F_\mathbb{C}$ is a product of copies of $\mathbb{C}$ as a $\mathbb{C}$-algebra, every $\mathbb{R}$-linear map $F_\mathbb{C} \to \mathbb{R}$ has the form $z \mapsto \operatorname{Tr}_{F_\mathbb{C}/\mathbb{R}}(\zeta z)$ for a unique $\zeta \in F_\mathbb{C}$. Hence, $\ell(z) = \operatorname{Tr}_{F_\mathbb{C}/\mathbb{R}}(\zeta z)$ for a unique $\zeta \in F_\mathbb{C}$. But

$$\ell(z) = -\ell(\bar{z}) = -\operatorname{Tr}_{F_\mathbb{C}/\mathbb{R}}(\zeta\bar{z}) = -\operatorname{Tr}_{F_\mathbb{C}/\mathbb{R}}(\bar{\zeta}z) = \operatorname{Tr}_{F_\mathbb{C}/\mathbb{R}}(-\bar{\zeta}z)$$

for all $z \in F_\mathbb{C}$, so by uniqueness we get $-\bar{\zeta} = \zeta$. That is, $\zeta \in iF_\mathbb{R}$. For $z = (z_1, \ldots, z_g) \in F_\mathbb{R} = \mathbb{R}^g$ we have $\ell(iz) = \operatorname{Tr}_{F_\mathbb{R}/\mathbb{R}}(\zeta iz) = -2\sum \zeta_j z_j$ where $\zeta = i(\zeta_1, \ldots, \zeta_g)$. Thus, the condition that $\ell(iz) > 0$ whenever all $z_j > 0$ is exactly that $\zeta_j < 0$ for all j.

Finally, for $u \in \operatorname{Aut}(J)$ consider the effect of replacing λ with $\lambda \circ u$. We have

$$E_{\lambda \circ u}(v, w) = E_\lambda(u.v, w) = \operatorname{Tr}_{F_\mathbb{C}/\mathbb{R}}(\zeta uv\bar{w}) = \ell(uv\bar{w}),$$

so ℓ is replaced with $z \mapsto \ell(uz)$. The first Riemann relation is therefore always satisfied since $\overline{uz} = u\bar{z}$. The second Riemann relation is that $\ell(uiz) > 0$ for all $(z_1, \ldots, z_g) \in F_\mathbb{R}$ with $z_j > 0$ for all j. In other words, $-2\sum \zeta_j u_j z_j$ in $\mathbb{R}_{>0}$ for all j, where u_j is the jth embedding of u in $\mathbb{R}$. Since $\zeta_j < 0$ for all j, this exactly says that u is a totally positive element of $\operatorname{End}(J)$, as desired. $\qquad\square$

Corollary 3.4. *Let J be the Jacobian of either of the curve $X_{\mathrm{ns}}(13)$ or $X_{\mathrm{s}}(13)$. Let $\lambda : J \simeq J^\vee$ be the canonical principal polarization of J. The principal polarizations of J are precisely the composition of λ with the action of squares in $\mathcal{O}_K^\times$.*

Proof. By Lemma 3.1, since all totally positive units in $\mathcal{O}_K$ are the squares in $\mathcal{O}_K^\times$, the corollary follows immediately from the above proposition.

$\square$

Notation 3.5. *In the rest of this paper we denote the Jacobians of $X_{\mathrm{ns}}(p)$ and $X_{\mathrm{s}}(p)$ by $J_{\mathrm{ns}}(p)$ and $J_{\mathrm{s}}(p)$, respectively.*

To see the significance of Corollary 3.4, let $\lambda_{\mathrm{s}}\colon J_{\mathrm{s}}(13) \to J_{\mathrm{s}}(13)^\vee$ and $\lambda_{\mathrm{ns}}\colon J_{\mathrm{ns}}(13) \to J_{\mathrm{ns}}(13)^\vee$ denote the canonical principal polarizations over $\mathbb{Q}$. Suppose we have an $\mathcal{O}_K$-linear $\mathbb{Q}$-isomorphism $\theta\colon J_{\mathrm{s}}(13) \to J_{\mathrm{ns}}(13)$. We claim that for some $v \in \mathcal{O}_K^\times$ the isomorphism $\theta \circ v$ respects the canonical principal polarizations. Since the isomorphisms

$$\theta^\vee \circ \lambda_{\mathrm{ns}} \circ \theta, \ \lambda_{\mathrm{s}} \in \mathrm{Isom}_{\mathbb{Q}}(J_{\mathrm{s}}(13), J_{\mathrm{s}}(13)^\vee)$$

are principal polarizations, Corollary 3.4 says that there exists $v \in \mathcal{O}_K^\times$ such that

$$\theta^\vee \circ \lambda_{\mathrm{ns}} \circ \theta \circ v^2 = \lambda_{\mathrm{s}}.$$

Using Proposition 3.2 and the fact that θ is $\mathcal{O}_K$-linear, we have $(\theta \circ v)^\vee \circ \lambda_{\mathrm{ns}} \circ (\theta \circ v) = \lambda_{\mathrm{s}}$, so $\theta \circ v$ respects the canonical principal polarizations.

To summarize, we know that there is an abstract $\mathcal{O}_K$-linear $\mathbb{Q}$-isogeny $\theta\colon J_{\mathrm{s}}(13) \to J_{\mathrm{ns}}(13)$ over $\mathbb{Q}$ (see [5, 6]) and we shall adjust θ to obtain an $\mathcal{O}_K$-linear isomorphism $\theta'\colon J_{\mathrm{s}}(13) \to J_{\mathrm{ns}}(13)$ over $\mathbb{Q}$. But in order to use Torelli's Theorem, we need to arrange that the isomorphism respects the canonical principal polarizations. This is not a problem, because as we saw above there is always some $v \in \mathcal{O}_K^\times$ so that the isomorphism $\theta' \circ v$ respects the canonical principal polarizations.

4. Isogenies between $J_{\mathrm{ns}}(13)$ and $J_{\mathrm{s}}(13)$

By [5, 6] we know that there exists an $\mathcal{O}_K$-linear $\mathbb{Q}$-isogeny between the Jacobians $J_{\mathrm{ns}}(13)$ and $J_{\mathrm{s}}(13)$. In this section, by refining some results in [6] we will control the degree of this isogeny.

Notation 4.1. *For a prime p, denote the normalizer of a split Cartan subgroup, the normalizer of a non-split Cartan subgroup, and a Borel subgroup of $GL_2(\mathbb{F}_p)$ by $C_{\mathrm{s}}^+(p)$, $C_{\mathrm{ns}}^+(p)$, and $B(p)$ respectively. We also denote the group $GL_2(\mathbb{F}_p)$ by G.*

Notation 4.2. *For a finite set S of primes, $\mathbb{Z}_S$ denotes the semi-local ring of rational numbers whose denominators have all prime factors not in S.*

It is well known (see [6], proof of Theorem 2) that there is an isomorphism of $\mathbb{Q}[G]$-modules

$$\text{(4.1)} \qquad \mathbb{Q}[G/\mathrm{C}_{\mathrm{s}}^+(p)] \oplus \mathbb{Q} \simeq \mathbb{Q}[G/\mathrm{C}_{\mathrm{ns}}^+(p)] \oplus \mathbb{Q}[G/B(p)].$$

In the proof of Theorem 3 in [6], it is shown that if a prime number ℓ does not divide $p-1$ then the isomorphism (4.1) remains true when $\mathbb{Q}$ is replaced by the localization $\mathbb{Z}_{(\ell)}$ of $\mathbb{Z}$ at ℓ. In this section, we will improve this result for $\mathbb{Z}_S$ instead of $\mathbb{Z}_{(\ell)}$, where S is a fixed finite set of primes which do not divide $p-1$.

Proposition 4.3. *Let Γ be a finite group and let R be a semi-local Noetherian ring with maximal ideals $\{m_1, m_2, \ldots, m_n\}$. Let $J = \bigcap m_i$ be its Jacobson radical. Let $\widehat{R}$ be the J-adic completion of R. Let M_1 and M_2 be $R[\Gamma]$-modules that are finite free over R. If the completions $\widehat{M_1}$ and $\widehat{M_2}$ are isomorphic as $\widehat{R}[\Gamma]$-modules then M_1 and M_2 are isomorphic as $R[\Gamma]$-modules.*

Proof. The R-module $\mathrm{Hom}_{R[\Gamma]}(M_1, M_2)$ is dense in $\mathrm{Hom}_{\widehat{R}[\Gamma]}(\widehat{M_1}, \widehat{M_2})$ because the natural map

$$\widehat{R} \otimes_R \mathrm{Hom}_{R[\Gamma]}(M_1, M_2) \simeq \mathrm{Hom}_{\widehat{R}[\Gamma]}(\widehat{M_1}, \widehat{M_2})$$

is an isomorphism. Indeed, this follows from tensoring the R-linear exact sequence

$$0 \longrightarrow \mathrm{Hom}_{R[\Gamma]}(M_1, M_2) \longrightarrow \mathrm{Hom}_R(M_1, M_2) \longrightarrow \prod_{\gamma \in \Gamma} \mathrm{Hom}_R(M_1, M_2)$$

$$T \longrightarrow (T \circ \gamma - \gamma \circ T)_\gamma$$

with $\widehat{R}$ over R.

Now consider the subset $\mathrm{Isom}_{\widehat{R}[\Gamma]}(\widehat{M_1}, \widehat{M_2})$ of isomorphisms in $\mathrm{Hom}_{\widehat{R}[\Gamma]}(\widehat{M_1}, \widehat{M_2})$. By assumption it is non-empty. Since $\mathrm{Isom}_{\widehat{R}[\Gamma]}(\widehat{M_1}, \widehat{M_2})$ is the inverse image of $\widehat{R}^\times$ under the determinant map, it is an open subset of $\mathrm{Hom}_{\widehat{R}[\Gamma]}(\widehat{M_1}, \widehat{M_2})$. Thus, being dense in $\mathrm{Hom}_{\widehat{R}[\Gamma]}(\widehat{M_1}, \widehat{M_2})$, the intersection of $\mathrm{Hom}_{R[\Gamma]}(M_1, M_2)$ with $\mathrm{Isom}_{\widehat{R}[\Gamma]}(\widehat{M_1}, \widehat{M_2})$ is non-empty. But this intersection is the set $\mathrm{Isom}_{R[\Gamma]}(M_1, M_2)$. Hence the proposition follows. $\qquad \square$

Corollary 4.4. *Let S be a finite set of primes which do not divide $p-1$. There is an isomorphism of $\mathbb{Z}_S[G]$-modules*

$$(4.2) \qquad \mathbb{Z}_S[G/\mathrm{C}_{\mathrm{s}}^+(p)] \oplus \mathbb{Z}_S \simeq \mathbb{Z}_S[G/\mathrm{C}_{\mathrm{ns}}^+(p)] \oplus \mathbb{Z}_S[G/B(p)].$$

Proof. Since each $\ell_i \in S$ does not divide $p-1$, by the proof of Theorem 3 in [6] the isomorphism (4.1) remains true when $\mathbb{Q}$ is replaced by $\mathbb{Z}_{(\ell_i)}$. Thus, the same holds when $\mathbb{Q}$ is replaced by $\prod_{\ell_i \in S} \mathbb{Z}_{\ell_i}$ where $\mathbb{Z}_{\ell_i}$ is the completion of $\mathbb{Z}_{(\ell_i)}$ at its maximal ideal. But $\prod_{\ell_i \in S} \mathbb{Z}_{\ell_i}$ is the completion of the semi-local $\mathbb{Z}_S$ for its Jacobson radical, so by using Proposition 4.3 we obtain the desired isomorphism.

$\square$

Theorem 4.5. *Let S be a finite set of primes which do not divide $p-1$. There exists an isogeny*

$$J_{\mathrm{s}}(p) \sim J_{\mathrm{ns}}(p) \times J_0(p)$$

over $\mathbb{Q}$ whose degree is relatively prime to the primes in the set S.

Proof. Consider the isomorphism (4.2) of $\mathbb{Z}_S[G]$-modules. Multiplying through some sufficiently divisible nonzero integer that is a unit in $\mathbb{Z}_S$, we arrive at inclusions of $\mathbb{Z}[G]$-modules

$$(4.3) \qquad \mathbb{Z}[G/\mathrm{C}_{\mathrm{s}}^+(p)] \oplus \mathbb{Z} \longrightarrow \mathbb{Z}[G/\mathrm{C}_{\mathrm{ns}}^+(p)] \oplus \mathbb{Z}[G/B(p)]$$

and

$$(4.4) \qquad \mathbb{Z}[G/\mathrm{C}_{\mathrm{ns}}^+(p)] \oplus \mathbb{Z}[G/B(p)] \longrightarrow \mathbb{Z}[G/\mathrm{C}_{\mathrm{s}}^+(p)] \oplus \mathbb{Z}.$$

Their composition in either order is multiplication by some nonzero integer with all prime factors not in S.

Let $\mathcal{C}$ be the category of commutative algebraic groups over $\mathbb{Q}$. The Jacobian $J(p)$ of $X(p)$ over $\mathbb{Q}$ is an object of $\mathcal{C}$. For any $\mathbb{Q}$-algebra R the functor $R \mapsto J(p)(R)$ is valued in $\mathbb{Z}[G]$-modules via the group structure and the G-action on $J(p)$. For any subgroup H of G, the $\mathbb{Q}$-subgroup $J(p)^H$ of H-invariants in $J(p)$ is also in the category $\mathcal{C}$. It has the functor of points $J(p)^H(R) = \mathrm{Hom}(\mathbb{Z}[G/H], J(p)(R))$ for any $\mathbb{Q}$-algebra R. Consider the identity component $J(p)_0^H$ of $J(p)^H$. Since it is closed and connected, it is an abelian variety.

Now apply $\mathrm{Hom}_{\mathbb{Z}[G]}(-, J(p)(R))$ to (4.3) and (4.4) with varying $\mathbb{Q}$-algebras R. This gives morphisms

$$J(p)^{\mathrm{C}_{\mathrm{ns}}^+(p)} \times J(p)^{B(p)} \longrightarrow J(p)^{\mathrm{C}_{\mathrm{s}}^+(p)} \times J(p)^G \quad \text{and}$$

$$J(p)^{\mathrm{C}_{\mathrm{s}}^+(p)} \times J(p)^G \longrightarrow J(p)^{\mathrm{C}_{\mathrm{ns}}^+(p)} \times J(p)^{B(p)}$$

between commutative algebraic groups over $\mathbb{Q}$ with composition in either order equal to multiplication by a nonzero integer whose prime factors are not in S. Passing to their identity components, as $J(p)_0^G = 0$ we obtain isogenies

$$(4.5) \qquad \xi_1 : J(p)_0^{\mathrm{C}_{\mathrm{ns}}^+(p)} \times J(p)_0^{B(p)} \longrightarrow J(p)_0^{\mathrm{C}_{\mathrm{s}}^+(p)} \quad \text{and}$$

$$\xi_2 : J(p)_0^{\mathrm{C}_{\mathrm{s}}^+(p)} \longrightarrow J(p)_0^{\mathrm{C}_{\mathrm{ns}}^+(p)} \times J(p)_0^{B(p)}$$

over $\mathbb{Q}$ whose degree is not divisible by any prime in the set S.

Let H be one of the groups $\mathrm{C}_{\mathrm{s}}^+(p)$, $\mathrm{C}_{\mathrm{ns}}^+(p)$, or $B(p)$. The covering map $X(p) \to X(p)/H$ has induced pullback map $\mathrm{Jac}(X(p)/H) \to J(p)$ with finite kernel. This induced map lands in $J(p)_0^H$, so we have a map of abelian varieties

$$(4.6) \qquad \psi_H : \mathrm{Jac}(X(p)/H) \to J(p)_0^H$$

over $\mathbb{Q}$ with finite kernel. Since the source and the target have the same dimension, the map ψ_H is an isogeny.

Now we want to show that the kernel of ψ_H has order with no prime factors in S. We may assume that $p \geq 5$, as for $p < 5$ the Jacobians all vanish. The kernel of ψ_H is the same as that of $\mathrm{Jac}(X(p)/H) \to J(p)$, so we will consider the latter map. To analyze the order of the kernel, we can extend the ground field to $\overline{\mathbb{Q}}$, and we have

$$X(p)_{\overline{\mathbb{Q}}} = \coprod_{\zeta \in \mu_p^*} X_\zeta(p), \qquad \text{so } J(p)_{\overline{\mathbb{Q}}} = \prod_{\zeta \in \mu_p^*} \mathrm{Jac}(X_\zeta(p)),$$

where μ_p^* is the set of primitive pth roots of unity in $\overline{\mathbb{Q}}$ and $X_\zeta(p)$ is the modular curve over $\overline{\mathbb{Q}}$ classifying full level p structures with Weil pairing ζ. Thus, the kernel of interest is the intersection of the kernels of the maps

$$(4.7) \qquad \mathrm{Jac}(X(p)_{\overline{\mathbb{Q}}}/H) \longrightarrow \mathrm{Jac}(X_\zeta(p))$$

induced by the covering map

$$X_\zeta(p) \longrightarrow X(p)_{\overline{\mathbb{Q}}}/H = X_\zeta(p)/(H \cap \mathrm{SL}_2(\mathbb{F}_p)).$$

In other words, for $H' := H \cap \mathrm{SL}_2(\mathbb{F}_p)$ and $X = X_\zeta(p)$ it suffices to show that for the covering map $X \to X/H'$ between connected curves, the pullback map on Jacobians has kernel with order whose prime factors all divide $p - 1$.

The kernel of (4.7) is dual to the cokernel of the homomorphism

$$(4.8) \qquad\qquad \pi_1(X(\mathbb{C}))^{\mathrm{ab}} \longrightarrow \pi_1((X/H')(\mathbb{C}))^{\mathrm{ab}}$$

between abelianized fundamental groups. By Lemma 4.6 below, the cokernel of (4.8) is a quotient of the maximal abelian quotient H'^{ab} of H'. Since $p \geq 5$, the abelianizations of $\mathrm{C}_{\mathrm{s}}^+(p) \cap \mathrm{SL}_2(\mathbb{F}_p)$ and $\mathrm{C}_{\mathrm{s}}^+(p) \cap \mathrm{SL}_2(\mathbb{F}_p)$ are 2-groups and the abelianization of $B(p) \cap \mathrm{SL}_2(\mathbb{F}_p)$ is given by its natural projection into $\mathbb{F}_p^\times$. Hence, the kernel of (4.6) has order whose prime factors all divide $p - 1$. Therefore, we can build a $\mathbb{Q}$-isogeny ψ_H' in the other direction so that their composition in either order is a multiplication by a nonzero integer whose prime factors all divide $p - 1$.

Consider the $\mathbb{Q}$-isogenies

$$\psi_{\mathrm{C}_{\mathrm{s}}^+(p)} : J_{\mathrm{s}}(p) \longrightarrow \mathrm{Jac}(X(p))_0^{\mathrm{C}_{\mathrm{s}}^+(p)},$$

$$\xi_2 : \mathrm{Jac}(X(p))_0^{\mathrm{C}_{\mathrm{s}}^+(p)} \longrightarrow \mathrm{Jac}(X(p))_0^{\mathrm{C}_{\mathrm{ns}}^+(p)} \times \mathrm{Jac}(X(p))_0^{B(p)},$$

$$\psi_{\mathrm{C}_{\mathrm{ns}}^+(p)}' \times \psi_{B(p)}' : \mathrm{Jac}(X(p))_0^{\mathrm{C}_{\mathrm{ns}}^+(p)} \times \mathrm{Jac}(X(p))_0^{B(p)} \longrightarrow J_{\mathrm{ns}}(p) \times J_0(p).$$

Their degrees have no prime factors in S, so by composing them we obtain the desired $\mathbb{Q}$-isogeny. $\qquad\square$

Lemma 4.6. *Let $Y \to Y'$ be a finite surjective morphism between smooth connected varieties over $\mathbb{C}$. Assume the extension of function fields is Galois with Galois group H. The natural map $\pi_1(Y(\mathbb{C})) \to \pi_1(Y'(\mathbb{C}))$ between their fundamental groups has normal image with cokernel that is a quotient of H. Likewise, the homomorphism between abelianized π_1's has cokernel that is a quotient of H^{ab}.*

Proof. A proper Zariski-closed subset Z' of Y' has complex codimension at least 1, hence $Z(\mathbb{C})$ has real codimension at least 2 in $Y(\mathbb{C})$, so $\pi_1(Y'(\mathbb{C}) - Z'(\mathbb{C})) \to \pi_1(Y'(\mathbb{C}))$ is surjective and likewise $\pi_1(Y(\mathbb{C}) - Z(\mathbb{C})) \twoheadrightarrow \pi_1(Y(\mathbb{C}))$ for the preimage Z of Z' in Y. Thus, we can pass to the complement of the branch locus in Y' to arrange that the branch locus is empty, so $Y(\mathbb{C})$ is a connected Galois finite covering space of $Y'(\mathbb{C})$ with covering group H. The Galois correspondence in covering space theory now gives the result.

$\qquad\square$

Corollary 4.7. *Let S be any finite set of primes that do not divide* 12. *There exists an $\mathcal{O}_K$-linear isogeny $J_{\mathrm{s}}(13) \sim J_{\mathrm{ns}}(13)$ over $\mathbb{Q}$ whose degree is relatively prime to the primes in the set S.*

Proof. Since $S_2(\Gamma_0(13)) = 0$, we have $J_0(13) = 0$. Thus, by Theorem 4.5 there is a $\mathbb{Q}$-isogeny $J_{\mathrm{s}}(13) \sim J_{\mathrm{ns}}(13)$. In the proof of Theorem 4.5, we actually obtain this isogeny from the $\mathbb{Z}[G]$-module inclusions (4.3) and (4.4) which are defined by an element in $\mathbb{Z}[G]$. Since actions of $\mathrm{GL}_2(\mathbb{F}_{13})$ and the Hecke operators away from 13 commute, this isogeny is Hecke compatible away from 13. Since the common endomorphism ring $\mathcal{O}_K$ is generated by the Hecke operators away from 13, the isogeny is $\mathcal{O}_K$-linear. $\square$

5. Residual irreducibility and the isomorphism

In this section, we will use Corollary 4.7 and a study of residual Galois representations to obtain an $\mathcal{O}_K$-linear $\mathbb{Q}$-isomorphism between $J_{\mathrm{s}}(13)$ and $J_{\mathrm{ns}}(13)$. As we saw at the end of Section 3, this would yield a $\mathbb{Q}$-isomorphism between these Jacobians which respects canonical principal polarizations, so we could conclude via Torelli's Theorem that $X_{\mathrm{ns}}(13)$ and $X_{\mathrm{s}}(13)$ are isomorphic over $\mathbb{Q}$.

Let

$$(5.1) \qquad\qquad \theta : J_{\mathrm{s}}(13) \to J_{\mathrm{ns}}(13)$$

be an $\mathcal{O}_K$-linear isogeny over $\mathbb{Q}$ whose degree is coprime to 7 and 13 (see Theorem 5.5). We can choose such an isogeny by Corollary 4.7.

Notation 5.1. *In this section we denote the Jacobians $J_{\mathrm{s}}(13)$ and $J_{\mathrm{ns}}(13)$ by J_{s} and J_{ns} respectively.*

Let $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. The kernel $\ker \theta$ is a finite $\mathcal{O}_K[G_{\mathbb{Q}}]$-submodule of $J_{\mathrm{s}}(\overline{\mathbb{Q}})$. The torsion subgroups $J_{\mathrm{s}}[I]$ for nonzero ideals I of $\mathcal{O}_K$ are a natural class of finite $\mathcal{O}_K[G_{\mathbb{Q}}]$-submodules of $J_{\mathrm{s}}(\overline{\mathbb{Q}})$. Assume $\ker \theta = J_{\mathrm{s}}[I]$ for some I. Since K has class number 1, we have $I = (\alpha)$ for some nonzero $\alpha \in \mathcal{O}_K$. Hence, $\theta = \psi \circ \alpha$ for some $\mathcal{O}_K$-linear $\psi : J_{\mathrm{s}} \to J_{\mathrm{ns}}$ with $\ker \psi = 0$. Thus, ψ would be a $\mathcal{O}_K$-linear $\mathbb{Q}$-isomorphism.

It remains to analyze the structure of all finite $\mathcal{O}_K[G_{\mathbb{Q}}]$-submodules M of $J_{\mathrm{s}}(\overline{\mathbb{Q}})$ whose order is not divisible by the primes 7 and 13. Such a module M decomposes into $\mathfrak{p}$-primary parts for the finitely many maximal ideals $\mathfrak{p}$ of $\mathcal{O}_K$ in its support. Let $M_{\mathfrak{p}}$ be a $\mathfrak{p}$-primary part of M for some $\mathfrak{p} \in \mathrm{Supp}(M)$.

In order to prove that $M = J_s[I]$ for some ideal I in $\mathcal{O}_K$, it suffices to show that $M_{\mathfrak{p}} = J_s[\mathfrak{p}^r]$ for some $r \geq 1$ (depending on $\mathfrak{p}$).

Proposition 5.2. *Let $\mathfrak{p}$ be a maximal ideal in $\mathcal{O}_K$ and let $M_{\mathfrak{p}}$ be a finite nonzero $\mathfrak{p}$-primary $\mathcal{O}_K[G_{\mathbb{Q}}]$-submodule of $J_s(\overline{\mathbb{Q}})$. If $J_s[\mathfrak{p}]$ is irreducible as an $(\mathcal{O}_K/\mathfrak{p})[G_{\mathbb{Q}}]$-module, then $M_{\mathfrak{p}} = J_s[\mathfrak{p}^r]$ for some $r \geq 1$.*

Proof. Since $J_s[\mathfrak{p}]$ is an irreducible $(\mathcal{O}_K/\mathfrak{p})[G_{\mathbb{Q}}]$-module, we have $M_{\mathfrak{p}}[\mathfrak{p}] = J_s[\mathfrak{p}]$. We will now induct on the $\mathcal{O}_K$-length of $M_{\mathfrak{p}}$. Since $\mathfrak{p}$ is principal, we consider the $\mathcal{O}_K[G_{\mathbb{Q}}]$-submodule $\frac{M_{\mathfrak{p}}}{J_s[\mathfrak{p}]} \subset \frac{J_s}{J_s[\mathfrak{p}]} \simeq J_s$ where the isomorphism is induced by the multiplication with a generator of $\mathfrak{p}$. This $\mathcal{O}_K[G_{\mathbb{Q}}]$-submodule $\frac{M_{\mathfrak{p}}}{J_s[\mathfrak{p}]}$ has smaller $\mathcal{O}_K$-length than $M_{\mathfrak{p}}$ and $\frac{M_{\mathfrak{p}}}{J_s[\mathfrak{p}]}[\mathfrak{p}]$ is $J_s[\mathfrak{p}]$ or 0. Thus $\frac{M_{\mathfrak{p}}}{J_s[\mathfrak{p}]} = J_s[\mathfrak{p}^r]$ for some $r \geq 0$. Now consider the map $J_s \to \frac{J_s}{J_s[\mathfrak{p}]}$. Since the preimage of $\mathfrak{p}^r$-torsion subgroup is $J_s[\mathfrak{p}^{r+1}]$, we have $M_{\mathfrak{p}} = J_s[\mathfrak{p}^{r+1}]$ for $r \geq 0$. Hence, the proposition follows. $\square$

For all $\mathfrak{p}$ which do not divide the primes 7 and 13, to show that a $\mathfrak{p}$-primary finite $\mathcal{O}_K[G_{\mathbb{Q}}]$-submodule of J_s is $J_s[\mathfrak{p}^r]$ for some $r \geq 1$, it suffices, by Proposition 5.2, to show that the residual Galois representation of $J_s[\mathfrak{p}]$ is irreducible over $\mathcal{O}_K/\mathfrak{p}$.

Let $\mathbb{F}_{\mathfrak{p}}$ be the finite field $\mathcal{O}_K/\mathfrak{p}$ and let p be its characteristic. Consider the Galois representation

$$(5.2) \qquad \rho_{\mathfrak{p}} : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\mathbb{F}_{\mathfrak{p}})$$

attached to $J_s[\mathfrak{p}]$. The $\mathfrak{p}$-adic Tate module $T_{\mathfrak{p}}(J_s)$ is free of rank 2 over the completion $\mathcal{O}_{K,\mathfrak{p}}$, with determinant as such equal to the p-adic cyclotomic character. Thus, $\det \rho_{\mathfrak{p}} = \omega_p$ where ω_p is the mod-p cyclotomic character. If ℓ is a prime which does not divide $13p$ then $\rho_{\mathfrak{p}}$ is unramified at ℓ and the characteristic polynomial of $\rho_{\mathfrak{p}}(\mathrm{Frob}_\ell)$ is

$$x^2 - a_\ell x + \ell \pmod{\mathfrak{p}},$$

where a_ℓ is the element of $\mathcal{O}_K$ corresponding to the Hecke operator T_ℓ acting on $\mathrm{S}_2(\Gamma_s(13))$ (i.e., the ℓ-th eigenvalue of a newform in $\mathrm{S}_2(\Gamma_s(13))$).

Proposition 5.3. *Consider $\rho_{\mathfrak{p}}$ in (5.2). If $\rho_{\mathfrak{p}}$ is reducible with $p \neq 2, 7, 13$ then the diagonal characters of $\rho_{\mathfrak{p}}$ are $\{\psi, \omega_p \psi^{-1}\}$ for some $\psi : G_{\mathbb{Q}} \to (\mathbb{Z}/13^k\mathbb{Z})^\times \to \mathbb{F}_{\mathfrak{p}}^\times$ for some $k \geq 1$.*

Proof. Since $\det \rho_{\mathfrak{p}} = \omega_p$, the Galois representation $\rho_{\mathfrak{p}}$ has diagonal characters $\{\psi, \omega_p \psi^{-1}\}$ for some character $\psi : G_{\mathbb{Q}}^{\mathrm{ab}} \to \mathbb{F}_{\mathfrak{p}}^\times$ unramified away from p

and 13. We will determine this ψ. Note that J_s has good reduction at p since $p \neq 13$, and p is inert or split in $K = \mathbb{Q}(\zeta_7)$ since $p \neq 7$.

We first assume that p splits in $\mathcal{O}_K$. Let $\mathfrak{p}$ be a maximal ideal of $\mathcal{O}_K$ that divides p. Then the $\mathbb{F}_p$-dimension of $J_\mathrm{s}[\mathfrak{p}]$ is 2. Since $\rho_\mathfrak{p}$ is reducible, there exists a Galois stable $\mathbb{F}_p$-line M in $J_\mathrm{s}[\mathfrak{p}]$. By the Oort-Tate classification (Theorem 3 in [10]), the Galois character ψ of M is either unramified outside 13 or is ω_p times a character unramified outside 13. In either case we obtain the diagonal characters in the proposition.

Now we assume that p is inert in $\mathcal{O}_K$. Let $\mathfrak{p}$ be the maximal ideal of $\mathcal{O}_K$ that divides p. The dimension of $J_\mathrm{s}[\mathfrak{p}]$ over $\mathbb{F}_\mathfrak{p} = \mathbb{F}_{p^3}$ is 2. Since $\rho_\mathfrak{p}$ is reducible, there exists a Galois stable $\mathbb{F}_{p^3}$-line M of $J_\mathrm{s}[\mathfrak{p}]$. Consider an inertia subgroup $H = \mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p^\mathrm{unr})$ of $G_\mathbb{Q}$ and the character $\psi|_H$. By (Corollary 3.4.4 in [11]), as $\mathbb{Q}_p^\mathrm{unr}$ is unramified over $\mathbb{Q}_p$ and $p > 2$, we have $\psi|_H = \theta^{\epsilon_0 + p\epsilon_1 + p^2\epsilon_2}$ where θ is a fundamental character of level 3 and $\epsilon_i \in \{0, 1\}$. The action of H on M through $\psi|_H$ is tame as $p \nmid p^3 - 1$. Since this action is also abelian over $\mathbb{Q}$, the order of $\psi|_H$ divides $p - 1$. Therefore either $\epsilon_i = 0$ for all i, in which case $\psi|_H = 1$, or $\epsilon_i = 1$ for all i, so $\psi|_H = \omega_p$. Hence again ψ is either a character unramified outside 13 or is ω_p times a character unramified outside 13. $\qquad\square$

Lemma 5.4. *Let $\mathfrak{p}$ be a prime in $\mathcal{O}_K$ which does not divide 13. The Galois action on $J_\mathrm{s}[\mathfrak{p}]$ is tamely ramified at 13.*

Proof. This lemma follows from Corollary 3.4 in [4] and Remark 1 of section 2 in [13]. $\qquad\square$

Theorem 5.5. *Let $\mathfrak{p}$ be a prime in $\mathcal{O}_K$ and let the Galois representation $\rho_\mathfrak{p}$ be as in (5.2). If $\rho_\mathfrak{p}$ is reducible then $\mathfrak{p}$ divides 7 or 13.*

Proof. The Galois representation ρ_2 is unramified at 11. We compute the characteristic polynomial of $\rho_2(\mathrm{Frob}_{11})$ and we see that it is irreducible mod 2. This tells us that ρ_2 is irreducible. We do the same thing with $\rho_{53}(\mathrm{Frob}_2)$ and $\rho_{79}(\mathrm{Frob}_3)$ and see that the representations ρ_{53} and ρ_{79} are also irreducible.

Now suppose that the prime $\mathfrak{p}$ in $\mathcal{O}_K$ does not divide 2, 7, 13, 53 or 79 and that the representation $\rho_\mathfrak{p}$ is reducible. By Proposition 5.3 the diagonal characters of $\rho_\mathfrak{p}$ are $\{\psi, \omega_p \psi^{-1}\}$ where ψ is unramified outside 13. By Lemma 5.4 the character ψ factors through $\mathrm{Gal}(\mathbb{Q}(\zeta_{13})/\mathbb{Q})$. Now for the primes

$q = 53$ and 79, consider a Frobenius element Frob_q. Since $q = 1 \bmod 13$ we have $\psi(\mathrm{Frob}_q) = 1$. It follows that

$$1 + q \equiv \mathrm{trace}\,\rho_{\mathfrak{p}}(\mathrm{Frob}_q) \equiv a_q \pmod{\mathfrak{p}}$$

in $\mathcal{O}_K$. Here a_q is the element of $\mathcal{O}_K$ corresponding to the Hecke operator T_q. This congruence relation implies that $p = \mathrm{char}(\mathfrak{p})$ divides the norm of $q + 1 - a_q$. Inspection of the values a_{53} and a_{79} in [15] shows that this implies that p divides both $7.13^2.127$ and $7.13^2.449$. This means that $\mathfrak{p}$ divides either 7 or 13.

$\square$

Now we prove the main result of this paper. As in (5.1), we choose an $\mathcal{O}_K$-linear isogeny

$$\theta : J_{\mathrm{s}} \to J_{\mathrm{ns}}$$

over $\mathbb{Q}$ with degree coprime to the primes 7 and 13. Then Proposition 5.2 and Theorem 5.5 imply that $\ker\theta = J_{\mathrm{s}}[I]$ for some nonzero ideal I in $\mathcal{O}_K$. As we saw in the discussion preceding Proposition 5.2, this yields an $\mathcal{O}_K$-linear $\mathbb{Q}$-isomorphism. By the discussion at the end of section 3, there exists $v \in \mathcal{O}_K^{\times}$ such that the $\mathbb{Q}$-isomorphism that we obtain by composing this isomorphism with v respects the canonical principal polarizations of J_{s} and J_{ns}. Therefore, by Torelli's Theorem, we conclude that $X_{\mathrm{s}}(13)$ and $X_{\mathrm{ns}}(13)$ are isomorphic over $\mathbb{Q}$.

Remark 5.6.　*The group $J_{\mathrm{s}}[7]$ of 7-torsion points of J_{s} is free of rank 2 over $\mathcal{O}_K/(7)$. The ideal (7) ramifies completely in $\mathcal{O}_K$ and we have $(7) = (\pi)^3$ where $\pi = \zeta_7 + \zeta_7^{-1} - 2$. It follows that $J_{\mathrm{s}}[\pi]$ has dimension 2 over $\mathbb{F}_7$. Consider its associated Galois representation ρ_{π}. We computed characteristic polynomials of $\rho_{\pi}(\mathrm{Frob}_{\ell})$ for $\ell \neq 7, 13$ and $\ell < 100$. They always factor in $\mathbb{F}_7[x]$ with roots $\chi_{13}(\ell)$ and $\chi_{13}\omega_7(\ell)$, where χ_{13} the quadratic character modulo 13 and ω_7 is the mod 7 cyclotomic character. This suggests that ρ_{π} is reducible with diagonal characters $\{\chi_{13}, \chi_{13}\,\omega_7\}$.*

We did a similar calculation at the prime 13 which completely splits in $\mathcal{O}_K$, say $(13) = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$. For a suitable labeling of the primes dividing (13), the calculation proves that $\rho_{\mathfrak{p}_1}$ has image $GL_2(\mathbb{F}_{13})$ and that $\rho_{\mathfrak{p}_2}$ and $\rho_{\mathfrak{p}_3}$ are reducible with respective pairs of diagonal characters $\{\omega_{13}^3, \omega_{13}^{10}\}$ and $\{\omega_{13}^5, \omega_{13}^8\}$. Here ω_{13} is the mod 13 cyclotomic character.

Acknowledgments

References

[1] B. Baran, *Normalizers of non-split Cartan subgroups, modular curves and the class number one problem*, J. Number Theory **130**(12) (2010), 2753–2772.

[2] B. Baran, *An exceptional isomorphism between modular curves of level 13*, (2012) preprint.

[3] Y. Bilu, P. Parent and M. Rebolledo, *Rational points on $X_0^+(p^r)$*, to appear in Ann. Inst. Fourier.

[4] I. Bouw and S. Wewers, *Stable reduction of modular curves*, in: J. Cremona, J.-C. Lario, J. Quer and K. Ribet (eds.): *Modular Curves and Abelian Varieties*, Progress in Mathematics **224**, Birkhäuser, Basel (2004), 1–22.

[5] I. Chen, *The Jacobians of non-split Cartan modular curves*, Proc. London Math. Soc. (3) **77** (1998), Part 1, 1–38.

[6] B. de Smit and S. Edixhoven, *Sur un résultat d'Imin Chen*, Math. Res. Lett. (7) **2–3** (2000), 147–153.

[7] A. Grothendieck, *Groupes de monodromie en géométrie algébrique*, Lecture Notes in Mathematics **288**, New York, 1972.

[8] B. Mazur, *Rational isogenies of prime degree*, Inv. Math. **44** (1978), 129–162.

[9] J. Milne, *Jacobian varieties* in Arithmetic Geometry (Cornell/ Silverman), Springer–Verlag, New York, 1986.

[10] F. Oort and J. Tate, *Group schemes of prime order*, Ann. Sci. École Norm. Sup. (4) **3** (1970), 1–21.

[11] M. Raynaud, *Schémas en groupes de type $(p, p, ..., p)$*, Bull. Soc. Math. France **102** (1974), 241–280.

[12] K.A. Ribet, *Twists of modular forms and endomorphisms of abelian varieties*, Math. Ann. **253** (1980), 43–62.

[13] R. Schoof, *Abelian varieties over $\mathbb{Q}$ with bad reduction in one prime only*, Composit. Math. **141** (2005), 847–868.

[14] J-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Inv. Math. **15** (1972), 259–331.

[15] W. Stein, *The Modular Forms Database*, `http://modular.math.washington.edu/Tables/tables.html`.

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF MICHIGAN
ANN ARBOR, MI 48109
USA
E-mail address: `baran.burcu@gmail.com`