The old subvariety of $J_o(pq)$*

Kenneth A. Ribet†

Introduction

Let p and q be distinct primes. The old part of $J_o(pq)$ is the abelian subvariety $A+B$ of $J_o(pq)$ generated by the images

$$A = \mathrm{Image}(J_o(p)^2 \xrightarrow{\alpha} J_o(pq)), \qquad B = \mathrm{Image}(J_o(q)^2 \xrightarrow{\beta} J_o(pq))$$

of the two indicated degeneracy maps. Here, $J_o(N)$ denotes the Jacobian $\mathrm{Pic}^o(X_o(N))$ of the standard modular curve $X_o(N)$, for each integer $N \geq 1$. Also, we have written $J_o(p)^2$ for the product $J_o(p) \times J_o(p)$, and have used analogous notation for $J_o(q)^2$. The definitions of α and β will be given below; see also [6], §2a.

The structure of A was determined in [14]. Namely, the kernel of α is the Shimura subgroup Σ_p of $J_o(p)$, viewed as a subgroup of $J_o(p)^2$ via the antidiagonal embedding $x \mapsto (x, -x)$. Thus we have $A = J_o(p)^2/\Sigma_p$ and, analogously, $B = J_o(q)^2/\Sigma_q$. Since A and B are known, we consider that to understand $A+B$ is to understand $A \cap B$, which is a finite abelian group. The main purpose of this note is to identify $A \cap B$, up to groups of 2-power order. In other words, we identify the ℓ-primary part of $A \cap B$ for each *odd* prime ℓ.

Let C_p be the cuspidal subgroup of $J_o(p)$. This group is cyclic of order $\mathrm{num}(\frac{p-1}{12})$, and appears frequently in [5]. (The symbol "num" denotes the

*Published in: Arithmetic Algebraic Geometry (G. van der Geer, F. Oort, J. Steenbrink, eds.) *Progress in Mathematics* **89**, 293–307 (1990)

†Partially supported by the National Science Foundation

numerator of a rational number. Thus, for $r \in \mathbf{Q}^*$, $\mathrm{num}(r)$ is the order of $\frac{1}{r}$ in $\mathbf{Q}/\mathbf{Z}$.) For the moment, view C_p in $J_o(p)^2$ by the antidiagonal embedding, and let $\bar{C}_p$ be the image of the antidiagonal C_p in A. Since $C_p \cap \Sigma_p$ is known to be the group $C_p[2]$ of elements of order dividing 2 in C_p ([5], p. 102), the group $\bar{C}_p$ is cyclic of order $\mathrm{num}\,\frac{p-1}{24}$. After consulting Ogg [9], and performing some computations, one checks that $\bar{C}_p$ is a subgroup of the cyclic subgroup $\mathcal{C}$ of $J_o(pq)$ generated by the class of the divisor

$$P_1 - P_p - P_q + P_{pq}$$

on $X_o(pq)$. (See §5 below.) According to [9], p. 459, the order of $\mathcal{C}$ is $\mathrm{num}\left(\frac{(p-1)(q-1)}{24}\right)$.

Let $\bar{C}_q \subset B$ be the analogue of $\bar{C}_p$ with p replaced by q. Then $\bar{C}_q$ has order $\mathrm{num}(\frac{q-1}{24})$, and again lies in the cyclic group $\mathcal{C}$. (The primes p and q play symmetric roles in the formation of $\mathcal{C}$.) It follows that the group $\bar{C}_p \cap \bar{C}_q$ has order

$$n := \gcd\left(\mathrm{num}\left(\frac{p-1}{24}\right), \mathrm{num}\left(\frac{q-1}{24}\right)\right).$$

Our main result is

THEOREM **1** *The finite abelian group $A \cap B$ and its subgroup $\bar{C}_p \cap \bar{C}_q$ are equal up to 2-groups. In other words, the quotient $Q = (A \cap B)/(\bar{C}_p \cap \bar{C}_q)$ has 2-power order.*

COROLLARY **1** *The order of the odd part of $A \cap B$ is the odd part of the integer n.*

As explained above this Corollary follows from the Theorem, together with the computation of §5.

A simple application of Theorem 1 concerns the kernel κ of the natural map

$$\gamma : J_o(p)^2 \times J_o(q)^2 \longrightarrow J_o(pq)$$

which is obtained from α and β. The image of γ is the abelian variety $A + B$ mentioned above; it is the old subvariety of $J_o(pq)$. View γ as the composite of the surjection $\alpha \times \beta : J_o(p)^2 \times J_o(q)^2 \to A \times B$ and the map $A \times B \to J_o(pq)$, $(a, b) \mapsto a + b$, whose kernel is identified with $A \cap B$ by the map $x \in A \cap B \mapsto (x, -x) \in A \times B$. We find an exact sequence

$$0 \to \Sigma_p \times \Sigma_q \to \kappa \to A \cap B \to 0.$$

Let κ_o be the inverse image of $\bar{C}_p \cap \bar{C}_q$ in κ; then we have an exact sequence

$$0 \to \Sigma_p \times \Sigma_q \to \kappa_o \to \bar{C}_p \cap \bar{C}_q \to 0.$$

This sequence is "nearly" split in the sense that there is a cyclic subgroup of κ_o which maps onto $\bar{C}_p \cap \bar{C}_q$ and whose intersection with $\Sigma_p \times \Sigma_q$ has order dividing 2. Indeed, to find such a subgroup, we can choose a generator t of $\bar{C}_p \cap \bar{C}_q$ and lifts x and y of t in C_p and C_q, respectively. The element $(x, -x, -y, y)$ of $J_o(p)^2 \times J_o(q)^2$ maps to the element $(t, -t)$ of $A \times B$, which we have identified with $t \in A \cap B$; it therefore is a lift of t to κ_o. The cyclic subgroup of $J_o(p)^2 \times J_o(q)^2$ which is generated by $(x, -x, -y, y)$ has an intersection with $\Sigma_p \times \Sigma_q$ which is of order 1 or 2, since $\Sigma_p \cap C_p = C_p[2]$ in $J_o(p)$, and $\Sigma_q \cap C_q = C_q[2]$ in $J_o(q)$.

Corollary **2** *The groups κ_o and κ are equal up to groups of 2-power order. More precisely, κ/κ_o is a 2-abelian group.*

Proof. Indeed, the indicated quotient is isomorphic to the quotient Q which appears in Theorem 1. ■

Another application of Theorem 1 concerns a question which was raised by Mazur ([6], §2b, Remark). For brevity, let us set $J = J_o(pq)$ and let J_{old} be the old subvariety $A + B$ of J. Let $J^{\text{new}} = J/J_{\text{old}}$, so that we have a tautological exact sequence

$$0 \to J_{\text{old}} \to J \to J^{\text{new}} \to 0.$$

Dualizing, we obtain a second sequence

$$0 \to (J^{\text{new}})^\vee \to J^\vee \to (J_{\text{old}})^\vee \to 0.$$

Since there is a canonical polarization $J \approx J^\vee$ (the *theta polarization*, coming from the fact that J is a Jacobian), we may regard $(J^{\text{new}})^\vee$ as an abelian subvariety of J. This subvariety of J is the *new subvariety* J_{new} of J, and the quotient J/J_{new} is the old quotient J^{old} of J. The composite of the inclusion $J_{\text{old}} \hookrightarrow J$ and the projection $J \to J^{\text{old}}$ is an isogeny

$$\lambda : J_{\text{old}} \to J^{\text{old}}.$$

Mazur asks for information about the *degree* of λ.

By the reasoning employed in §3 of [14], we obtain a direct relation between the kernel of λ and the group κ which appears above. Namely, let Θ be a line bundle on J corresponding to the "theta divisor" of J, and let M be the pullback of Θ to $J_{\text{old}} \subseteq J$. The isogeny λ is then the polarization ϕ_M which is attached to M (as defined in [8], Chapter II, §6). Let L be the pullback of Θ to $J_o(p)^2 \times J_o(q)^2$, and let $\Omega = K(L)$ be the kernel of the polarization

$$\phi_L : J_o(p)^2 \times J_o(q)^2 \to (J_o(p)^2 \times J_o(q)^2)^\vee$$

arising from L. The group Ω contains κ, and Ω is endowed with a canonical skew-symmetric $\mathbf{G}_{\mathtt{m}}$-valued pairing. Let $\kappa^\perp$ be the annihilator of κ in this pairing. As explained in [8], §23, we have $\kappa^\perp \supseteq \kappa$, and a canonical isomorphism

$$\ker(\lambda) \approx \kappa^\perp/\kappa.$$

In particular, we have

$$\text{degree}(\lambda) = \text{card}(\Omega)/\,\text{card}(\kappa)^2.$$

To identify Ω, we rewrite $(J_o(p)^2 \times J_o(q)^2)^\vee$ as $J_o(p)^2 \times J_o(q)^2$, again using the autoduality of the Jacobian, and view ϕ_L as an endomorphism of $J_o(p)^2 \times J_o(q)^2$. Note, for the purposes of orientation, that any such endomorphism decomposes *a priori* as the "external product" of an endomorphism of $J_o(p)^2$ and an endomorphism of $J_o(q)^2$, since there are no homomorphisms in either direction between $J_o(p)$ and $J_o(q)$. (One can see this, for example, from the fact that $J_o(p)$ has good reduction at q, while $J_o(q)$ has purely toric reduction at q.) Hence Ω is automatically the product of a subgroup Ω_p of $J_o(p)^2$ and a subgroup Ω_q of $J_o(q)^2$. By the method of [14], §3, we find that ϕ_L may be decomposed as the the product of the endomorphism $\begin{pmatrix} 1+q & T_q \\ T_q & 1+q \end{pmatrix}$ of $J_o(p)^2$ and the endomorphism $\begin{pmatrix} 1+p & T_p \\ T_p & 1+p \end{pmatrix}$ of $J_o(q)^2$. These endomorphisms are both isogenies, and their degrees are respectively

$$\prod_f \Big((1+q)^2 - a_q(f)^2\Big)^2, \qquad \prod_g \Big((1+p)^2 - a_p(g)^2\Big)^2,$$

where f and g run over the sets of weight-2 newforms on $\Gamma_o(p)$ and $\Gamma_o(q)$, respectively. The notation $a_q(f)$, for instance, indicates the q^{th} coefficient of the Fourier expansion of f. Hence we have

$$\text{card}(\Omega) = \prod_f \Big((1+q)^2 - a_q(f)^2\Big)^2 \cdot \prod_g \Big((1+p)^2 - a_p(g)^2\Big)^2.$$

Meanwhile, we have determined that card(κ) is the product of an integer of the form 2^t ($t \geq 0$) with the quantity

$$\mathrm{card}(\kappa_o) = \mathrm{num}\left(\tfrac{p-1}{12}\right) \cdot \mathrm{num}\left(\tfrac{q-1}{12}\right) \cdot \gcd\left(\mathrm{num}\left(\tfrac{p-1}{24}\right), \mathrm{num}\left(\tfrac{q-1}{24}\right)\right).$$

Refer to card(κ_o) as P. Summing up the discussion, we have

Theorem **2** *Let* $D = \mathrm{degree}(\lambda)$ *be the order of the kernel of the natural map* $J_{\mathrm{old}} \to J^{\mathrm{old}}$. *Then* D, a priori *a perfect square, divides the integer*

$$\frac{\prod_f \left((1+q)^2 - a_q(f)^2\right)^2 \cdot \prod_g \left((1+p)^2 - a_p(g)^2\right)^2}{P^2}.$$

The ratio of this integer to D *is a power of 2.*

We prove Theorem 1 by arithmetic methods, combining the main theorem of [15] with an assortment of results from [5]. In particular, we rely on the results of [5] concerning: pure admissible groups, Ogg's Conjecture (Conjecture 2 of [10]), and a "twisted version" of Ogg's Conjecture *(loc. cit.)*. Since the statement of the theorem is purely transcendental, one imagines that the theorem may be proved by transcendental methods. It would be of considerable interest to find such a proof, which would presumably identify all of $A \cap B$, as opposed to its odd part.

It is a pleasure to thank the organizers of the TEXel conference for their kind invitation to an especially enjoyable and productive mathematical encounter. The results contained in this article were discovered in large part at the Weizmann Institute, during a workshop on Iwasawa Theory in May, 1989. The author wishes to thank this institution, and especially Shai Haran, for the hospitality. Finally, thanks go to Ling San for a careful reading of preliminary versions of this article, and to the referee, for helpful comments.

1 Hecke operators on $A \cap B$

For each integer $N \geq 1$, the modular curve $X_o(N)$ carries a family of Hecke correspondences T_n ($n \geq 1$). Further, for each positive divisor D of N

such that D and N/D are relatively prime, one has an Atkin-Lehner involution w_D on $X_o(N)$. (See, for example, [7] for a discussion of these operators in various guises.) These operators induce endomorphisms of $J_o(N) = \mathrm{Pic}^o(X_o(N))$ which are again denoted by the symbols T_n and w_D. The subring of $\mathrm{End}(J_o(N))$ generated by the T_n is denoted $\mathbf{T}_N$. This ring is already generated by the operators T_ℓ for ℓ *prime*. If ℓ is a divisor of N, the operator T_ℓ is often denoted U_ℓ and referred to as an Atkin-Lehner operator.

The modular curves $X_o(N)$ for varying N are connected by *degeneracy operators*, which are discussed, for instance, in [6]. Recall that if N is a product DM, then there is a degeneracy operator $\pi_d : X_o(N) \to X_o(M)$ for each positive divisor d of D. By pullback, we obtain homomorphisms

$$\pi_d^* : J_o(M) \to J_o(N)$$

for each d. Assembling together $\pi_1^*, \pi_q^* : J_o(p) \rightrightarrows J_o(pq)$, we define the map

$$\alpha = \pi_1^* \times \pi_q^* : J_o(p)^2 \to J_o(pq).$$

The map $\beta : J_o(q)^2 \to J_o(pq)$ is defined similarly.

"Formulaire"

The compatibility of α and β with the various operators T_n and w_D is well known. Here is a summary of the behavior of these operators under α (for β, permute the roles of p and q):

1. We have $T_n(\alpha(x, y)) = \alpha(T_n x, T_n y)$ for all n prime to q, and $x, y \in J_o(p)$. In other words, for n prime to q we have $T_n \circ \alpha = \alpha \circ T_n$, where the latter T_n is the Hecke operator labeled T_n in $\mathbf{T}_p$, which is understood to be acting diagonally on $J_o(p)^2$.

2. We have $\alpha \circ w_p = w_p \circ \alpha$.

3. The q^{th} Atkin-Lehner involution w_q on $J_o(pq)$ satisfies $w_q(\alpha(x, y)) = \alpha(y, x)$ for $x, y \in J_o(p)$. Equivalently, we have $w_q \circ \pi_q^* = \pi_1^*$ and $w_q \circ \pi_1^* = \pi_q^*$.

4. The q^{th} Hecke operators T_q on $J_o(p)$ and $J_o(pq)$ satisfy

$$T_q(\alpha(x, y)) = \alpha(T_q x + q y, -x).$$

The last formula is probably clearer if we use the alternative notation U_q for the q^{th} Hecke operator on $J_o(pq)$:

$$U_q(\alpha(x,y)) = \alpha(T_q x + qy, -x).$$

It is frequently advantageous for calculations to use the symbols U_p and U_q for the p^{th} and q^{th} Hecke operators on $J_o(pq)$, reserving T_p and T_q for the p^{th} Hecke operator on $J_o(q)$ and the q^{th} Hecke operator on $J_o(p)$, respectively. In a similar vein, it is probably best to refer to the p^{th} Hecke operator of $J_o(p)$ as U_p, and to the q^{th} Hecke operator of $J_o(q)$ as U_q.

The formulas above show clearly that the subvariety A of $J_o(pq)$ is stable under the ring $\mathbf{T}_{pq}$ and under the involutions w_p and w_q. By symmetry, the intersection $A \cap B$ is $\mathbf{T}_{pq}$-stable, so that it is naturally a module for the algebra $\mathbf{T}_{pq}$.

It is important to note that $A \cap B$ carries, as well, natural actions of the two rings $\mathbf{T}_p$ and $\mathbf{T}_q$. To see this, it is enough, by symmetry, to exhibit a natural action of $\mathbf{T}_p$ on $A \cap B$. The ring $\mathbf{T}_p$ acts diagonally on $J_o(p)^2$, and Σ_p is $\mathbf{T}_p$-stable in $J_o(p)^2$. Therefore, there is a natural action of $\mathbf{T}_p$ on A, and the claim is that $A \cap B$ is stable under this action. The only subtle point is the stability of $A \cap B$ under the operator labeled T_q in $\mathbf{T}_p$, which does *not* coincide in general on A with the operator U_q coming from $\mathbf{T}_{pq}$.

To treat this point, we use the last of the above formulas, plus the Cayley-Hamilton Theorem, to establish the identity $U_q^2 - U_q T_q + q = 0$ on A. On B, U_q is an involution: the negative of the involution w_q. (This follows, for instance, from the proof of Proposition 3.7 of [15]. The endomorphism $w_q + U_q$ of $J_o(q)$ factors through the degeneracy map $\pi^* : J_o(1) \to J_o(q)$, whose source is 0.) We therefore have

$$T_q = U_q(q+1) = -w_q(q+1)$$

on $A \cap B$.

2 Galois action on $A \cap B$

In the above discussion, we have considered $A \cap B$ as a $\mathbf{T}_p$-stable submodule of A. A closely related module is the inverse image $(A \cap B)\tilde{}$ of $A \cap B$ in $J_o(p)^2$. Thus $(A \cap B)\tilde{}$ is an extension of $A \cap B$ by the Shimura subgroup Σ_p

of $J_o(p)$, which we identify with its antidiagonal image in $J_o(p)^2$. The group $(A \cap B)\tilde{}$ is a finite $\mathbf{T}_p$-stable submodule of $J_o(p)^2$. *Until further notice, we shall write simply* $\mathbf{T}$ *for the Hecke algebra* $\mathbf{T}_p$.

Up to now, we have tacitly regarded the curves $X_o(p)$, $X_o(q)$, and $X_o(pq)$, and their Jacobians, as being defined over $\mathbf{C}$. However, one knows from work of Shimura (see, e.g., [18]) that these curves exist over $\mathbf{Q}$. (In fact, by [1] there are even good models for these curves over $\mathbf{Z}$. See also [4].) One sees from their modular definitions that the various Hecke operators, Atkin-Lehner involutions, and degeneracy operators we have considered are all defined over $\mathbf{Q}$. It follows from this that the abelian subvarieties A and B of $J_o(pq)$ are defined over $\mathbf{Q}$, so that the intersection $A \cap B$ is defined over $\mathbf{Q}$. We view it as a finite $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$-module with an equivariant action of the ring $\mathbf{T}$, or, equivalently, as a $\mathbf{T}[\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})]$-module. From the definition of $(A \cap B)\tilde{}$ as an inverse image, we see that this subgroup of $J_o(p)^2$, with its $\mathbf{T}$-action, is defined over $\mathbf{Q}$.

Theorem 3 *The* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$*-modules* $A \cap B$ *and* $(A \cap B)\tilde{}$ *extend to finite flat commutative group schemes over* $\mathrm{Spec}(\mathbf{Z})$.

Proof. The theorem means that there are groups schemes $\mathcal{G}_1$ and $\mathcal{G}_2$ over $\mathrm{Spec}(\mathbf{Z})$ whose associated Galois modules $\mathcal{G}_i(\overline{\mathbf{Q}})$ are isomorphic to $A \cap B$ and $(A \cap B)\tilde{}$, respectively.

The group $A \cap B$ extends to a finite flat group scheme over $\mathrm{Spec}(\mathbf{Z}[\frac{1}{p}])$ because it is a rational subgroup of the abelian variety A, which has good reduction outside p. Symmetrically, $A \cap B$ extends to a finite flat group scheme over $\mathrm{Spec}(\mathbf{Z}[\frac{1}{q}])$. From this, we may deduce that it extends to a finite flat group scheme over $\mathrm{Spec}(\mathbf{Z})$. (For example, we can apply the discussion of [5], Chapter I, §1 to the ℓ-primary part of $A \cap B$, for each prime number ℓ.)

We have an exact sequence

$$0 \to \Sigma_p \to (A \cap B)\tilde{} \to A \cap B \to 0.$$

To show that $(A \cap B)\tilde{}$ extends to $\mathrm{Spec}(\mathbf{Z})$, we may treat separately the ℓ-primary components of $(A \cap B)\tilde{}$. The assertion to be proved is obvious for those ℓ which are prime to the order $n_p = \mathrm{num}\left(\frac{p-1}{12}\right)$ of Σ_p, since the ℓ-primary components of $A \cap B$ and $(A \cap B)\tilde{}$ are isomorphic in that case.

It thus suffices to treat the prime-to-p part of $(A \cap B)^{\tilde{}}$, which is a finite $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$-stable submodule $R \supseteq \Sigma_p$ of $J_o(p)^2(\overline{\mathbf{Q}})$.

We are required to show that R is *unramified at* p. Fix a decomposition group $D = \mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p) \subset \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ for p in $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, and let I be the inertia subgroup of D. We wish to show that I acts trivially on R. More generally:

LEMMA **1** *Let $G \supseteq \Sigma_p$ be a finite I-stable subgroup of $J_o(p)^2(\overline{\mathbf{Q}}_p)$, whose order is prime to p. Assume that I acts trivially on G/Σ_p. Then I acts trivially on G.*

To prove the lemma, we first note the following facts, which are variants for $J_o(p)^2$ of results proved by Mazur [5] for $J_o(p)$:

1. The group Σ_p extends to a finite flat subgroup of the Néron model $\mathcal{J}$ of $J_o(p)^2$ over $\mathrm{Spec}(\mathbf{Z})$. (Compare [5], p. 100.)

2. In characteristic p, Σ_p has trivial intersection with the connected component $\mathcal{J}^o_{/\mathbf{F}_p}$ of $\mathcal{J}$. (Cf. [5], p. 101.)

In the latter statement, the group $T = \mathcal{J}^o_{/\mathbf{F}_p}$ is a torus over $\mathbf{F}_p$. The group $T(\overline{\mathbf{F}}_p)$, which is a torsion abelian group with trivial p-primary component, may be canonically identified with a subgroup of $J_o(p)^2(\overline{\mathbf{Q}}_p)^I$ (for example, by [17], Lemma 2). The second assertion gives the equality $\Sigma_p \cap T(\overline{\mathbf{F}}_p) = 0$ inside $J_o(p)^2(\overline{\mathbf{Q}}_p)$.

With these preliminary facts recorded, we may now prove the lemma by a variant of the argument given for Lemma 16.5 of [5], Chapter II. Take $g \in G$ and $\gamma \in I$. Since I acts trivially on G/Σ_p, we have $(i-1)g \in \Sigma_p$. On the other hand, $(i-1)g$ lies in the group $T(\overline{\mathbf{F}}_p)$. This follows from the fact that $J_o(p)^2$ has purely toric reduction at p, as can be seen from the discussion in Exposé IX, §7 of [3] or the exact sequence which is given as Lemma 3.3.1 of [13]. Hence $(i-1)g = 0$, which gives the desired statement that i acts trivially on g. ■

3 Maximal ideals of the Hecke algebra $\mathbf{T}_p$

The *Eisenstein ideal* of $\mathbf{T} = \mathbf{T}_p$ is the ideal I generated by the elements $T_\ell - \ell - 1$ for prime numbers $\ell \neq p$, together with the difference $U_p - 1$ ([5], p. 95). The Eisenstein primes of $\mathbf{T}$ are the maximal ideals m of $\mathbf{T}$ which contain I. These ideals are in 1-1 correspondence with the prime numbers dividing $n_p = \text{num}\left(\frac{p-1}{12}\right)$, a prime number $\ell \mid n_p$ corresponding to the maximal ideal $\mathsf{m} = (I, \ell)$.

For each maximal ideal m of $\mathbf{T}$, let ρ_m be the usual semisimple two-dimensional representation of $\text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ over $k_\mathsf{m} = \mathbf{T}/\mathsf{m}$ which is associated to m by the constructions of [2]. Thus, ρ_m is unramified outside the primes p and ℓ, where ℓ is the characteristic of the finite field k_m. For r a prime other than ℓ or p, the characteristic polynomial of $\rho_\mathsf{m}(\mathsf{Frob}_r)$, where Frob_r is a Frobenius element for r in the Galois group $\text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, is the polynomial $X^2 - T_r X + r \in k_\mathsf{m}[X]$. One knows ([5], Chap. II, §14) that ρ_m is reducible over k_m if and only m is Eisenstein. In this case, k_m is the prime field $\mathbf{F}_\ell$, and ρ_m is isomorphic to the direct sum of the trivial 1-dimensional representation and the 1-dimensional representation μ_ℓ of $\text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$.

Recall that ρ_m is *finite* at p (cf. [16]) if and only if: the restriction of ρ_m to a decomposition group $\text{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$ for p in $\text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ is isomorphic to the representation arising from a k_m-vector space scheme of rank 2 (in the sense of [12]) over $\mathbf{Z}_p$. For $\ell \neq p$, ρ_m is finite at p if and only if it is unramified at p.

THEOREM 4 *Assume that $\ell \neq 2$. Suppose that ρ_m is finite at p. Then m is Eisenstein.*

Proof. Assume that ρ_m is finite at p, but not Eisenstein. Then, by the main theorem (Theorem 1.1) of [15], the representation ρ_m is "modular of level 1." In particular, ρ_m may be realized by a group of ℓ-torsion points of the abelian variety $J_o(1)$. This is absurd, since $J_o(1)$ is 0. ■

4 Proof of the main theorem

Let M be the "odd part" of $(A \cap B)\tilde{}$, i.e., the direct sum of the ℓ-primary subgroups of $(A \cap B)\tilde{}$, for ℓ odd. Our aim is to show that M is "small." To do this, we first control the set of prime ideals of $\mathbf{T}$ which are in the support of M:

PROPOSITION **1** *If* m *is a maximal ideal of* $\mathbf{T}$ *in the support of* M*, then* m *is an Eisenstein prime.*

Proof. Let m be in the support of M. Then, by the definition of M, m is prime to 2. Let $M[\mathsf{m}]$ be the kernel of m on M, i.e., the set of $m \in M$ which are killed by all elements of m. Since M is finite, and m lies in the support of M, $M[\mathsf{m}]$ is non-zero. Assume that m is in the support of M and that m is non-Eisenstein. Then a well known argument of Mazur ([5], proof of Proposition 14.2 of Chapter II) shows that the $k_{\mathsf{m}}[\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})]$-module $M[\mathsf{m}]$ is a successive extension of copies of the representation ρ_{m}. In other words, let V be a $k_{\mathsf{m}}[\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})]$-module which affords ρ_{m}. Then the semisimplification of $M[\mathsf{m}]$ is some (non-zero) power of V.

In particular, we can find an embedding $V \hookrightarrow M$. By Theorem 3, M extends to a finite flat group scheme $\mathcal{M}$ over $\mathrm{Spec}(\mathbf{Z})$. The Zariski closure of V in $\mathcal{M}$ is then a finite flat group scheme $\mathcal{V}$ over $\mathrm{Spec}(\mathbf{Z})$ which prolongs V. Thus ρ_{m} is finite at p, which contradicts Theorem 4. ■

COROLLARY *For each prime* ℓ*, let* M_ℓ *be the* ℓ*-primary part of the abelian group* M*. Then* M_ℓ *is trivial unless* ℓ *is an odd prime dividing* n_p*, in which case the semisimplification of* M_ℓ *is a direct sum of modules of the form* μ_ℓ *and* $\mathbf{Z}/\ell\mathbf{Z}$*.*

Proof. By construction, the order of M is odd. By the Proposition, only primes ℓ dividing n_p can divide the order of M. Moreover, for $\ell \mid n_p$, only the Eisenstein prime $\mathsf{m} = (I, \ell)$ can intervene in the support of M_ℓ. Hence M_ℓ is annihilated by some power of m, which means that $M_\ell \subseteq J_o(p)^2[\mathsf{m}^\nu]$ for some integer $\nu \geq 0$. All Jordan-Hölder constituents of the latter module are of the form μ_ℓ and $\mathbf{Z}/\ell\mathbf{Z}$ ([5], Chapter II, Proposition 14.1). ■

THEOREM **5** *The module* $M \subset J_o(p) \times J_o(p)$ *is contained in the direct sum* $N \oplus N$*, where* N *is the submodule* $\Sigma_p + C_p$ *of* $J_o(p)$*.*

Proof. The Gal($\overline{\mathbf{Q}}/\mathbf{Q}$)-module M extends to a finite flat group scheme $\mathcal{M}$ over Spec($\mathbf{Z}$) (Theorem 3). In the language of [5], Chapter I, §1(f), the above Corollary states that the ℓ-primary parts of $\mathcal{M}$ are "admissible." Proposition 4.5 of [5], Chapter I then tells us that $\mathcal{M}$ is *pure* in the sense that it is the direct product of a constant group by a group whose dual is constant. (A group whose dual is constant is called a "μ-type group" in [5].)

The largest constant subgroup of $J_o(p)$ is C_p ([5], Chapter III, Theorem 1.2), while the largest μ-type subgroup of $J_o(p)$ is Σ_p ([5], Chapter III, Theorem 1.3.) ■

Note that the sum $\Sigma_p + C_p$ inside $J_o(p)$ is very nearly a direct sum. The intersection $\Sigma_p \cap C_p$ is the group of elements of order dividing 2 in C_p ([5], Chapter II, Proposition 11.11). This group has order 2 if $p \equiv 1 \pmod 8$ and is trivial otherwise.

The Theorem implies that M is contained in the direct sum $J_o(p)[I] \oplus J_o(p)[I]$, where I is again the Eisenstein ideal.

We now prove the main result (Theorem 1), whose statement we reformulate as follows:

> *The odd part of $A \cap B$ is contained in the intersection of the two groups $\bar{C}_p = \alpha(C_p^-)$ and $\bar{C}_q = \beta(C_q^-)$, the exponent $^-$ indicating that C_p and C_q have been embedded antidiagonally in $J_o(p)^2$ and $J_o(q)^2$, respectively.*

Proof. By symmetry, it suffices to show that the odd part of $A \cap B$ is contained in $\bar{C}_p$. We know by Theorem 5 that the odd part of $A \cap B$ is contained in $\alpha(N \oplus N)$. Since α kills the antidiagonal Σ_p^-, the group $\alpha(N \oplus N)$ is, neglecting 2-abelian groups, the sum

$$\alpha(C_p^+) + \alpha(C_p^-) + \alpha(\Sigma_p^+),$$

where the exponent $^+$ is now used for the diagonal embedding. The prime-to-2 part of this sum is direct. By the *formulaire* presented above, the Atkin-Lehner involution w_q operates as $+1$ on the groups with exponent $^+$ and as -1 on the group with exponent $^-$. However, w_p acts on $J_o(p)[I]$ as -1. Therefore, w_p acts on the displayed sum as -1, so that w_p is -1 on the odd part of $A \cap B$.

By symmetry, w_q must act as -1 on the odd part of $A \cap B$. Therefore, this odd part is contained in $\alpha(C_p^-)$, as was claimed. ■

5 Computations with cusps

The aim of this § is to justify the claim, made in the introduction, that the subgroup $\bar{C}_p = \alpha(C_p^-)$ of $J_o(pq)$ lies in the cyclic subgroup of $J_o(pq)$ generated by the class of the divisor $P_1 - P_p - P_q + P_{pq}$. This divisor is formed from the four cusps of the curve $X_o(pq)$, which are in natural 1-1 correspondence with the positive divisors of pq. We have used the notation of Ogg [9], who writes P_d for the cusp corresponding to the divisor d. This notation will apply also for the modular curve $X_o(p)$; thus we will consider that C_p is the cyclic subgroup of $J_o(p)$ generated by the class of the divisor $P_1 - P_p$ on $X_o(p)$. We recall also that the the map α is constructed from the two degeneracy coverings

$$\pi_1, \pi_q : X_o(pq) \rightrightarrows X_o(p)$$

and that the $^-$ in C_p^- indicates the antidiagonal embedding. Therefore, $\bar{C}_p$ is the cyclic group generated by $(\pi_1^* - \pi_q^*)(\overline{P_1 - P_p})$; the "bar" over $P_1 - P_p$ is used here in denote the class of the indicated divisor.

To study this divisor, we will consider the maps π_1^* and π_q^* which are induced by the degeneracy maps *on the level of divisors*. The only points of $X_o(pq)$ lying over the cusp P_1 of $X_o(p)$ are the cusps P_1 and P_q of $X_o(pq)$. Hence we have $\pi_1^*(P_1) = aP_1 + bP_q$ for some integers $a, b \geq 0$; these integers sum to $q+1$, the degree of the covering π_1. [The actual values of a and b, which are not needed here, are the ramification indices of P_1 and P_q in the covering $\pi_1 : X_o(pq) \to X_o(p)$. They are 1 and q, up to permutation. The author computed them by calculating the divisors of the function $\Delta(z)/\Delta(pz)$ on the two curves $X_o(p)$ and $X_o(pq)$, employing the techniques presented in [11]. An alternative approach, suggested by the referee, is to identify a and b with the ramification indices of P_1 and P_q in the covering $\pi_1 : X_o(q) \to X_o(1)$, and to compute these latter indices by techniques involving fundamental domains.]

The covering $\pi_1 : X_o(pq) \to X_o(p)$ is equivariant with respect to the Atkin-Lehner involutions w_p on $X_o(p)$ and $X_o(pq)$. Further, on both of these curves, w_p permutes the cusp labeled P_1 with the cusp labeled P_p. Finally, the involution w_p on $X_o(pq)$ permutes the cusps P_q and P_{pq}. Therefore, $\pi_1^*(P_p) = aP_p + bP_{pq}$. On the other hand, we have $\pi_1 w_q = \pi_q$, and the involution w_q of $X_o(pq)$ permutes P_1 with P_q and P_p with P_{pq}. Therefore, we have:

$$\pi_q^*(P_1) = aP_q + bP_1, \qquad \pi_q^*(P_p) = aP_{pq} + bP_p.$$

Combining everything together gives

$$(\pi_1^* - \pi_p^*)(P_1 - P_p) = (a-b)(P_1 - P_p - P_q + P_{pq}).$$

By passing to the level of divisor classes, we obtain the desired result.

References

[1] Deligne, P., Rapoport, M.: Schémas de modules de courbes elliptiques. Lecture Notes in Mathematics **349**, 143–316 (1973)

[2] Deligne, P., Serre, J-P.: Formes modulaires de poids 1. Ann. Sci. Ecole Norm. Sup. **7**, 507–530 (1974)

[3] (SGA 7 I) Grothendieck, A.: Groupes de monodromie en géométrie algébrique. Lecture Notes in Mathematics **288**. Berlin-Heidelberg-New York: Springer 1972

[4] Katz, N. M., Mazur, B.: Arithmetic Moduli of Elliptic Curves. Annals of Math. Studies **108**. Princeton: Princeton University Press 1985

[5] Mazur, B.: Modular curves and the Eisenstein ideal. Publ. Math. IHES **47**, 33–186 (1977)

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

[7] Mazur, B., Wiles, A.: Class fields of abelian extensions of **Q**. Invent. Math. **76**, 179–330 (1984)

[8] Mumford, D.: Abelian Varieties. London: Oxford University Press 1970

[9] Ogg, A.: Hyperelliptic modular curves. Bull. Soc. Math. France **102**, 449–462 (1974)

[10] Ogg, A.: Diophantine equations and modular forms. Bull. AMS **81**, 14–27 (1975)

[11] Ogg, A.: Rational points on certain elliptic modular curves. Proc. Symp. Pure Math. **24**, 221–231 (1973)

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

[13] Ribet, K.: Galois action on division points of abelian varieties with real multiplications. Am. J. Math. **98**, 751–804 (1976)

[14] Ribet, K.: Congruence relations between modular forms. Proc. International Congress of Mathematicians 1983, 503–514

[15] Ribet, K.: On modular representations of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ arising from modular forms. Invent. Math. To appear

[16] Serre, J-P.: Sur les représentations modulaires de degré 2 de $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. Duke Math. J. **54**, 179–230 (1987)

[17] Serre, J-P., Tate, J.: Good reduction of abelian varieties. Annals of Math. **88**, 492–517 (1968)

[18] Shimura, G.: Introduction to the Arithmetic Theory of Automorphic Functions. Princeton: Princeton University Press 1971

Mathematics Department
University of California
Berkeley CA 94720
USA