Congruences between cusp forms and the geometry of Jacobians of modular curves

San Ling[⋆]

Department of Mathematics, University of California,
Berkeley, CA, 94720, USA

For $N \geqq 1$ an integer and $N' \geqq 1$ a divisor of N, let $X_0(N)$ and $X_0(N')$ be the classical modular curves over $\mathbf{Q}$, and let $J_0(N)$ and $J_0(N')$ denote their Jacobian varieties, also defined over $\mathbf{Q}$. If $D \geqq 1$ is an integer such that DN' divides N, then one can define the degeneracy map $v_D : X_0(N) \to X_0(N')$ (cf. [13] and [11, Sect. 6.1]). Recall that v_D is defined as the map deduced from the transformation $\tau \mapsto D\tau$ of the compactified Poincaré upper half plane. The Riemann surface $Y_0(N) = X_0(N) - \{\text{cusps}\}$ parametrises the isomorphism classes $[E, C]$ of pairs (E, C), where E is an elliptic curve and C is a cyclic subgroup of E of order N. On $Y_0(N)$, the action of v_D is given by

$$v_D([E, C]) = [E/C_D, C_{N'D}/C_D]\,,$$

where C_D and $C_{N'D}$ denote the unique subgroups of C of orders D and $N'D$ respectively.

The map v_D induces, via Pic functoriality, a map $v_D^* : J_0(N') \to J_0(N)$ of abelian varieties.

Given an integer $M \geqq 1$, let $p \geqq 5$ be a prime not dividing M. Let $N = p^r M$ and $N' = pM$ in the notation above. Then we obtain r degeneracy maps $v_1, \ldots, v_{p^{r-1}}$. Let γ be the map

$$\gamma = v_1^* \times \cdots \times v_{p^{r-1}}^* : J_0(pM)^r \to J_0(p^r M)\,.$$

Let $T(pM)$ and $T(p^r M)$ denote the tori in the reduction modulo p of $J_0(pM)$ and $J_0(p^r M)$ respectively. In Sect. 1 of this article, we prove

Theorem 1. *The map* $\gamma : J_0(pM)^r \to J_0(p^r M)$ *induces an isomorphism* $(T(pM))^r \xrightarrow{\simeq} T(p^r M)$.

⋆ Present address: Department of Mathematics, National University of Singapore, Singapore 0511

To prove Theorem 1, we first summarize in Sect. 1 a method to calculate the torus in a Jacobian as outlined in SGA 7I, Exposé IX [8], and then apply the method to the minimal resolutions of $X_0(p^rM)$ as constructed by Edixhoven [7].

As a consequence of Theorem 1, we obtain in Sect. 2 (by setting $M = 1$)

Theorem 2. *The kernel K of the map $\gamma : J_0(p)^r \to J_0(p^r)$ is the group*

$$\left\{ \begin{pmatrix} x_1 \\ \vdots \\ x_r \end{pmatrix} \middle| x_i \in \Sigma(p) \quad \textit{for all } i, \sum_{i=1}^{r} x_i = 0 \right\},$$

where $\Sigma(p)$ denotes the Shimura subgroup of $J_0(p)$.

Theorem 2 should be regarded as a counterpart to Theorem 4.3 of [19], which says that: if p is a prime not dividing a given positive integer N, then the kernel K' of the map $v_1^* \times v_p^* : J_0(N) \times J_0(N) \to J_0(Np)$ is the group $\left\{ \begin{pmatrix} x \\ y \end{pmatrix} \middle| x, y \in \Sigma(N),\ x + y = 0 \right\}$, where $\Sigma(N)$ denotes the Shimura subgroup of $J_0(N)$.

The proof of Theorem 2 here and that of Theorem 4.3 in [19] are completely different. The proof in [19] is cohomological in nature, while the proof of Theorem 2 we give in this article is done by passing to the reduction modulo p of the Jacobians $J_0(p)$ and $J_0(p^r)$.

Theorem 2 has several applications, of which we discuss two in Sects. 3 and 4 of this article. The first application concerns the problem of establishing congruence relations between weight-2 cusp forms of level p and p^2 (p a prime), and the second determines the degree of an isogeny from the old subvariety of $J_0(p^2)$ to the old quotient of $J_0(p^2)$.

Let $S = S_2(\Gamma_0(p^2))$ be the space of weight-2 cusp forms of level p^2 and trivial character. Let X be the subspace (of S) of oldforms associated to $\Gamma_0(p)$. Let Y be the orthogonal complement to X under the Petersson inner product on S. Hence, $S = X \oplus Y$. There are Hecke operators acting on S (cf. [1]). For a prime $n \nmid p$, we denote the n^{th} Hecke operator acting on S by T_n; for $n = p$, we use U_p for the p^{th} Hecke operator. We use the same notations for the Hecke operators acting on $J_0(p^2)$. Let $\mathbf{T}_{p^2}$ be the subring of $\mathrm{End}(S)$ generated by these Hecke operators. The space Y is $\mathbf{T}_{p^2}$-stable by Theorem 3 of [1]. It is easy to see that X is also $\mathbf{T}_{p^2}$-stable. We may therefore define $\mathbf{T}_X$ (resp. $\mathbf{T}_Y$) to be the subring of $\mathrm{End}(X)$ (resp. $\mathrm{End}(Y)$) generated by the Hecke operators. The rings $\mathbf{T}_X$ and $\mathbf{T}_Y$ are quotients of $\mathbf{T}_{p^2}$, and $\mathbf{T}_{p^2}$ is a subring of $\mathbf{T}_X \oplus \mathbf{T}_Y$. A prime ideal $\wp$ of $\mathbf{T}_{p^2}$ is a *prime of fusion* if it contains the conductor of the ring extension $\mathbf{T}_{p^2} \hookrightarrow \mathbf{T}_X \oplus \mathbf{T}_Y$. The image of $\wp$ in $\mathbf{T}_X$ (resp. $\mathbf{T}_Y$) is a prime ideal $\wp_X$ (resp. $\wp_Y$). (By abuse of language, we shall call them primes of fusion as well.) Moreover, we have isomorphisms

$$\mathbf{T}_X/\wp_X \cong \mathbf{T}_{p^2}/\wp \cong \mathbf{T}_Y/\wp_Y\,. \tag{1}$$

The Hecke operators T_n also act on $S_2(\Gamma_0(p))$ (resp. $J_0(p)$). Let T_p denote the p^{th} Hecke operator on $S_2(\Gamma_0(p))$ (resp. $J_0(p)$). Let $\mathbf{T}$ be the Hecke algebra generated by T_p and the T_n's. There is a well-defined map $\psi : \mathbf{T}_X \to \mathbf{T}$ (see Sect. 3.6) that sends T_n to T_n, and U_p to 0.

We construct in Sect. 3 a $\mathbf{T}_X$-module Ω whose support contains only primes of fusion, as well as another $\mathbf{T}_X$-module Δ which turns out to be $\left\{ \begin{pmatrix} -T_p y \\ y \end{pmatrix} \middle| y \in J_0(p)[p^2-1] \right\}$. The ring $\mathbf{T}$ also acts on Ω and Δ. The support of Δ (in both $\mathbf{T}_X$ and $\mathbf{T}$) contains the support of Ω. Then we prove in Sect. 3 the following theorems about the primes of fusion:

Theorem 3. *Let λ be in* $\mathrm{Supp}_{\mathbf{T}} \Delta$.

(i) *If λ is non-Eisenstein, then* $\lambda \in \mathrm{Supp}_{\mathbf{T}} \Omega$.

(ii) *If λ is the Eisenstein prime $(\mathfrak{I}, l)$, where $\mathfrak{I}$ is the Eisenstein ideal in* $\mathbf{T}$, *and* $l \neq 2, 3$ *is a prime dividing* $\mathrm{num}\left(\frac{p-1}{12}\right)$, *then* $\lambda \in \mathrm{Supp}_{\mathbf{T}} \Omega \Leftrightarrow \mathbf{T}_\lambda \neq \mathbf{Z}_l$.

Remarks. 1. The notation $\mathrm{num}\left(\frac{p-1}{12}\right)$ refers to the numerator of $\frac{p-1}{12}$ when it is expressed in lowest terms. It is equal to $\frac{p-1}{(p-1, 12)}$.

2. From [12], we see that the only instances (for $p < 250$, $p \neq 2$) where $\mathbf{T}_\lambda \neq \mathbf{Z}_l$ ($l \neq 2, 3$) are: $p = 31$, $l = 5$; $p = 103$, $l = 17$; $p = 127$, $l = 7$; $p = 131$, $l = 5$; $p = 181$, $l = 5$; and $p = 211$, $l = 5$.

Theorem 3 is then used to obtain

Theorem 4. *Let* $\mathfrak{m} \in \mathrm{Supp}_{\mathbf{T}_X} \Delta$. *Then there exists a maximal ideal λ of* $\mathbf{T}$ *such that* $\psi^{-1}(\lambda) = \mathfrak{m}$ *and* $\lambda \in \mathrm{Supp}_{\mathbf{T}} \Delta$.

(i) *If there exists one such λ such that* $\lambda \in \mathrm{Supp}_{\mathbf{T}} \Omega$, *then* $\mathfrak{m} \in \mathrm{Supp}_{\mathbf{T}_X} \Omega$.

(ii) *If, for all such λ, we have* $\lambda \notin \mathrm{Supp}_{\mathbf{T}} \Omega$, *then λ is unique, it is an Eisenstein prime, and* $\mathfrak{m} \notin \mathrm{Supp}_{\mathbf{T}_X} \Omega$.

Let $\mathfrak{I}_X$ be the annihilator in $\mathbf{T}_X$ of the kernel K of $\gamma : J_0(p)^2 \to J_0(p^2)$. We also give in Sect. 3 a direct characterization of the primes of fusion:

Theorem 5. *Let* $l \neq 2, 3$ *be a prime dividing* $\mathrm{num}\left(\frac{p-1}{12}\right)$. *We have the equality*

$$\mathrm{Ann}_{\mathbf{T}_X} \Omega_l = \mathrm{Ann}_{\mathbf{T}_X}(\mathfrak{I}_X / (\mathrm{Ann}_{\mathbf{T}_X} \Delta_l \cap \mathfrak{I}_X)),$$

where Ω_l and Δ_l denote the l-primary parts of Ω and Δ respectively.

The task of determining whether a given prime in $\mathbf{T}_X$ is a prime of fusion is in fact closely related to the problem of establishing congruence relations between weight-2 cusp forms (and especially newforms) on $\Gamma_0(p)$ and $\Gamma_0(p^2)$.

Let $f = \sum a_n q^n$ be a normalized Hecke eigenform on $\Gamma_0(p)$. Then the extension L of $\mathbf{Q}$ generated by the coefficients a_n is a number field; let $\mathcal{O}$ denote its ring of integers. We have naturally the homomorphism

$$\phi_X : \mathbf{T}_X \longrightarrow \mathcal{O}$$

defined by $\phi_X(T_n) = a_n$ and $\phi_X(U_p) = 0$.

Suppose λ is a maximal ideal in $\mathcal{O}$ such that the characteristic of the residue field $k = \mathcal{O}/\lambda$ is not p, and let $\wp_X = \phi_X^{-1}(\lambda)$. Since $\mathbf{T}_X/\wp_X$ injects into the finite field k, $\wp_X$ is also maximal. The injection $\mathbf{T}_X/\wp_X \hookrightarrow k$ is given by $T_n \bmod \wp_X \mapsto a_n \bmod \lambda$.

Theorem 6. *Let f, L, $\mathcal{O}$, λ, k, ϕ_X and $\wp_X$ be as defined hereabove. If $\wp_X$ is a prime of fusion, then there exist a finite extension L' of L and a newform $g = \sum b_n q^n$ of level p^2 such that g is an eigenform for the Hecke operators T_n, and $b_r \equiv a_r \bmod \lambda'$ for all r prime to p, where λ' is a prime ideal in the ring of integers $\mathcal{O}'$ of L' such that $\lambda' \cap \mathcal{O} = \lambda$.*

Proof. First, we note that the isomorphism (1) gives the injection $\mathbf{T}_Y/\wp_Y \hookrightarrow k$.

If we let $S_{\mathbf{Q}}$ denote the subset of S consisting of forms with rational q-expansions, it is known that $S = S_{\mathbf{Q}} \otimes_{\mathbf{Q}} \mathbf{C}$. We also have $S_{\mathbf{Q}} = X_{\mathbf{Q}} \oplus Y_{\mathbf{Q}}$ (cf. [26]). These two facts, together with the fact that forms with rational q-expansions have bounded denominators, imply that $\mathscr{R}$ is a free $\mathbf{Z}$-module of rank $d = \dim_{\mathbf{C}} Y$, where $\mathscr{R}$ is the subspace of Y consisting of forms with integral coefficients. If g denotes the dimension of $S_2(\Gamma_0(p))$, then $\dim_{\mathbf{C}} X = 2g$. If $g' = \dim_{\mathbf{C}} S$, then $d = g' - 2g$. In $\mathbf{T}_X$, since U_p satisfies $U_p^2 - T_p U_p = 0$ (see Lemma 1 in Sect. 3), the rank of $\mathbf{T}_X$ as a $\mathbf{Z}$-module is $2g$. Since $\mathbf{T}_{p^2}$ and $\mathbf{T}_X \oplus \mathbf{T}_Y$ have the same $\mathbf{Z}$-rank and $g' = \operatorname{rank}_{\mathbf{Z}} \mathbf{T}_{p^2}$ is well known, $\mathbf{T}_Y$ is a free $\mathbf{Z}$-module of rank d. The q-expansion map $\mathscr{R} \to \mathbf{Z}[[q]]$ has torsion-free cokernel, which implies that the map

$$\mathscr{R} \otimes_{\mathbf{Z}} k \longrightarrow k[[q]]$$

is injective. Consider the bilinear pairing

$$(\mathscr{R} \otimes_{\mathbf{Z}} k) \times (\mathbf{T}_Y \otimes_{\mathbf{Z}} k) \longrightarrow k$$

taking (f, T) to the coefficient of q in the q-expansion of $f|T$. The argument in [20] gives an isomorphism

$$\mathscr{R} \otimes_{\mathbf{Z}} k \xrightarrow{\simeq} \quad \operatorname{Hom}_{\mathbf{Z}}(\mathbf{T}_Y, k)\,.$$

Considering the map $T_n \mapsto (a_n \bmod \lambda)$ in $\operatorname{Hom}_{\mathbf{Z}}(\mathbf{T}_Y, k)$, we find a form $h \in \mathscr{R} \otimes_{\mathbf{Z}} k$ whose q-expansion coefficients are $t_n = a_n \bmod \lambda$. The form h is clearly an eigenform for the Hecke operators T_n with eigenvalues $a_n \bmod \lambda$.

Theorem 6 then follows from Lemme 6.11 of [5]. □

Since any newform is a finite linear combination of normalized Hecke eigenforms, Theorem 6 enables us to determine, given a newform $f = \sum a_n q^n$ on $\Gamma_0(p)$, when there exists an extension $\tilde{L}$ of $\mathbf{Q}$ and a newform $g = \sum b_n q^n$ on $\Gamma_0(p^2)$ such that $b_r \equiv a_r \bmod \tilde{\lambda}$ for all r prime to p, where $\tilde{\lambda}$ is a prime ideal in the ring of integers in $\tilde{L}$.

Finally, in Sect. 4, we discuss the second application of Theorem 2. If A is the old subvariety of $J_0(p^2)$ and $A^\vee$ is the old quotient, Mazur [13, Sect. 2b, remark] has asked for information about the degree of the isogeny $\Lambda : A \to A^\vee$, obtained by composing the inclusion $A \hookrightarrow J_0(p^2)$ with the projection $J_0(p^2) \cong J_0(p^2)^\vee \to A^\vee$. Using Theorem 2 and our knowledge of the Δ defined in Sect. 3, we show that the degree of Λ is $\dfrac{(p^2-1)^{2g}}{n^2}$, where $n = \operatorname{num}\left(\dfrac{p-1}{12}\right)$ and g is the dimension of $J_0(p)$.

1 The tori of $J_0(p^rM)_{/\mathbf{F}_p}$ ($p \nmid M$)

1.1 Calculating the torus

Let C be a curve over a p-adic field E of characteristic 0, with residue field k of characteristic p. To find the torus in the reduction mod p of the Jacobian of C, we apply the following method.

Let P denote the Néron model of the Jacobian $\mathrm{Pic}^o(C)$ of C and let P_k^o be the connected component in the special fibre. Let $\tilde{C}$ be a regular model of C over the ring of integers of E, and let $\mathscr{C}$ be the special fibre of $\tilde{C}$. Suppose that the greatest common divisor of the multiplicities of the irreducible components of $\mathscr{C}$ is 1. Then the results of Raynaud (cf. [8, Sect. 12] and [17]) imply that

$$P_k^o \cong \mathrm{Pic}^o_{\mathscr{C}/k}$$

We can calculate the maximal torus of $\mathrm{Pic}^o_{\mathscr{C}/k}$, where $\mathscr{C}$ is a separable and proper curve over a field k (which is assumed to be separably closed for simplicity), as follows (cf. SGA 7I, Exposé IX [8]).

Let $\tilde{\mathscr{Y}}$ be the set of irreducible components of $\tilde{\mathscr{C}}$, the normalization of $\mathscr{C}$, and for each $x \in \mathscr{C}$ that is a singular point (i.e. x belongs to ≥ 2 components), let $\tilde{\mathscr{Y}}(x)$ be the set of 'branches' of $\mathscr{C}$ passing by x (i.e. points of $\tilde{\mathscr{C}}$ lying over x). Let $\tilde{R}(x) = \mathbf{Z}_0^{\tilde{\mathscr{Y}}(x)}$ be the set of elements of $\mathbf{Z}^{\tilde{\mathscr{Y}}(x)}$ of degree 0. (This set is denoted $R(x)_0$ in [8].) Labelling the components in $\tilde{\mathscr{Y}}$ in some fixed way, we can define a map $\tilde{\theta} : \oplus_x \tilde{R}(x) \to \mathbf{Z}^{\tilde{\mathscr{Y}}}$ as follows: each $\tilde{R}(x)$ may be regarded as a subgroup of $\mathbf{Z}^{\tilde{\mathscr{Y}}}$ by the obvious injection (since $\tilde{\mathscr{Y}}(x)$ is a subset of $\tilde{\mathscr{Y}}$), and then $\tilde{\theta}$ is the component-wise addition. If we let $\mathscr{T}$ denote the torus of $\mathrm{Pic}^o_{\mathscr{C}/k}$, then the character group $\mathscr{X}(\mathscr{T})$ satisfies

$$\mathscr{X}(\mathscr{T}) \overset{\mathrm{def}}{=} \mathrm{Hom}(\mathscr{T}, \mathbf{G}_m) \cong \ker(\oplus_x \tilde{R}(x) \xrightarrow{\tilde{\theta}} \mathbf{Z}^{\tilde{\mathscr{Y}}}) .$$

We have implicitly assumed $\mathscr{C}$ to be reduced. However, even if $\mathscr{C}$ is not reduced, we can still use the recipe. In fact, we have the following

Proposition 1. *Let k be a perfect field. Let $\mathscr{C}/k$ be a non-reduced curve, and let $\mathscr{C}_{\mathrm{red}}$ denote the reduced scheme associated to $\mathscr{C}$. Then $\mathrm{Pic}^o_{\mathscr{C}/k}$ and $\mathrm{Pic}^o_{\mathscr{C}_{\mathrm{red}}/k}$ have the same maximal torus.*

For the proof, see, for example, [17, Sect. 6.2.3].

1.2 Regular models of $X_0(p^rM)$ ($p \nmid M$)

In order to apply the above recipe to calculate the torus of the Jacobian $J_0(p^rM)$, we need a model of $X_0(p^rM)$ that is regular. It is well-known that $X_0(p^rM) \otimes_{\mathbf{Z}} \bar{\mathbf{F}}_p$ consists of $r+1$ irreducible components, each of which is isomorphic to $X_0(M) \otimes_{\mathbf{Z}} \bar{\mathbf{F}}_p$, crossing at every supersingular point and nowhere else. The components are indexed by pairs of non-negative integers (a, b), where $a + b = r$. The (a, b)-component has

multiplicity $p^t(p-1)$, where $t = \min(a,b) - 1$. We shall use j_a to denote the (a,b)-component. A regular model of $X_0(p^rM)$, called the minimal resolution and denoted by $\tilde{X}_0(p^rM)$, is obtained by blowing up the model of $X_0(p^rM)$ over Spec($\mathbf{Z}$) at all the singular points until it is regular (cf. [4] and [7]). Here, we give a summary of the complete description of $\tilde{X}_0(p^rM) \otimes_{\mathbf{Z}} \bar{\mathbf{F}}_p$ in terms of $X_0(M) \otimes_{\mathbf{Z}} \bar{\mathbf{F}}_p$. The reader is referred to [7, Sect. 1] for more details.

Step I. Take the disjoint union of $r+1$ copies of $X_0(M) \otimes_{\mathbf{Z}} \bar{\mathbf{F}}_p$ and let Φ be the morphism

$$\Phi\colon \coprod_{a+b=r} X_0(M) \otimes_{\mathbf{Z}} \bar{\mathbf{F}}_p \to X_0(M) \otimes_{\mathbf{Z}} \bar{\mathbf{F}}_p$$

defined by $\begin{cases} \text{the identity morphism} & \text{if } a \geqq b, \\ (\text{absolute Frobenius})^{b-a} \otimes \mathrm{id}_{\bar{\mathbf{F}}_p} & \text{if } a \leqq b. \end{cases}$

Step II. At every supersingular point x of $X_0(M) \otimes_{\mathbf{Z}} \bar{\mathbf{F}}_p$, $\Phi^{-1}x$ is contracted to one point with local equation

$$(x - y^{p^r})(x^{p^r} - y) \prod_{\substack{a+b=r \\ a,b>0}} (x^{p^{a-1}} - y^{p^{b-1}})^{p-1}.$$

Step III. For $x \in X_0(M)(\bar{\mathbf{F}}_p)$ corresponding to $j(E) = 1728$:

(i) if x is supersingular ($p \equiv -1 \bmod 4$), we replace x by one copy of $\mathbf{P}^1$, which meets the j_a's ($a < b$) at a point y_1, meets the j_a's ($a > b$) at a point y_3, and, if r is even, meets j_a ($a = b$) at a point y_2.

This added irreducible component has self-intersection number -2, and it has multiplicity $\begin{cases} \dfrac{p+1}{2} p^{-1+\frac{r}{2}} & \text{if } r \text{ is even} \\ p^{\frac{r-1}{2}} & \text{if } r \text{ is odd}. \end{cases}$

(ii) if x is ordinary ($p \equiv 1 \bmod 4$), then replace each $x_{a,b}$ $(a,b>0)$, where $x_{a,b}$ is the point on j_a lying over x, by a copy of $\mathbf{P}^1$ which meets j_a at w_a.

Each of these $r-1$ copies of $\mathbf{P}^1$ has self-intersection number -2, and the multiplicity of the copy replacing $x_{a,b}$ is $\dfrac{p-1}{2} p^t$.

Step IV. For $x \in X_0(M)(\bar{\mathbf{F}}_p)$ corresponding to $j(E) = 0$:

(i) if x is supersingular ($p \equiv -1 \bmod 3$), then

- if r is even, replace x by a copy of $\mathbf{P}^1$, which meets the j_a's ($a < b$) at a point z_1, meets the j_a's ($a > b$) at a point z_3, and meets j_a ($a = b$) at a point z_2.
  The self-intersection number of the added component is -3, and its multiplicity is $\dfrac{p+1}{3} p^{-1+\frac{r}{2}}$
- if r is odd, replace x by a chain of two copies of $\mathbf{P}^1$. One copy meets the j_a's ($a < b$) at a unique point, while the other meets the j_a's ($a > b$) at another unique point. These two copies of $\mathbf{P}^1$ meet each other at yet another point.

Each of these two copies of $\mathbf{P}^1$ has self-intersection number -2, and multiplicity $p^{\frac{r-1}{2}}$.

(ii) if x is ordinary ($p \equiv 1 \bmod 3$), then replace $x_{a,b}$ by a copy of $\mathbf{P}^1$, for $a, b > 0$.

Each of these $r-1$ copies of $\mathbf{P}^1$ has self-intersection number -3, and the multiplicity of the copy replacing $x_{a,b}$ is $\dfrac{p-1}{3}p^t$.

1.3 Relaxing the regularity condition

In this section, we show that if we carry out the calculations of Sect. 1.1, using $X_0(p^rM) \otimes_{\mathbf{Z}} \bar{\mathbf{F}}_p$ instead of the minimal resolution $\tilde{X}_0(p^rM) \otimes_{\mathbf{Z}} \bar{\mathbf{F}}_p$, the character group thus obtained is isomorphic to that obtained by using the minimal resolution. The idea of the proof is similar to one used by Ribet in [20]. We shall treat carefully the case of *even* r. The proof for the case of *odd* r is essentially the same.

(i) *When r is even*

We already know that $X_0(p^rM) \otimes_{\mathbf{Z}} \bar{\mathbf{F}}_p$ consists of $r+1$ irreducible components, all intersecting at the supersingular points. Let s_2, s_4 and s_6 denote the number of supersingular points x with $\mathrm{Card}(\mathrm{Aut}(x)) = 2, 4$ and 6 respectively, and let s_4' and s_6' denote the corresponding number of ordinary points.

For $\tilde{X}_0(p^rM) \otimes_{\mathbf{Z}} \bar{\mathbf{F}}_p$, using the notation in Sect. 1.1, we see that

$$\oplus \tilde{R}(x) \cong \oplus \mathbf{Z}_0^{\mathscr{Z}(x)} \simeq (\mathbf{Z}^r)^{s_2} \oplus G\,,$$

where

$$G = \mathbf{Z}^{(r-1)s_4'} \oplus \mathbf{Z}^{(r-1)s_6'} \oplus (\mathbf{Z}^{r/2} \oplus \mathbf{Z} \oplus \mathbf{Z}^{r/2})^{s_4} \oplus (\mathbf{Z}^{r/2} \oplus \mathbf{Z} \oplus \mathbf{Z}^{r/2})^{s_6}.$$

Moreover, we have that $\mathbf{Z}_0^{\mathscr{Z}} \simeq \mathbf{Z}^{r+u}$, where

$$u = (s_4' + s_6')(r-1) + s_4 + s_6\,.$$

The character group $\mathscr{X}(T(p^rM))$ of the torus is the kernel of the map $\tilde{\theta} : \oplus \tilde{R}(x) \to \mathbf{Z}^{\mathscr{Z}}$. (The components added in Steps III and IV of Sect. 1.2 have been labelled from j_{r+1} to j_{r+u} in some definite way.)

Applying Sect. 1.1 to $X_0(p^rM) \otimes_{\mathbf{Z}} \bar{\mathbf{F}}_p$, we see that $\oplus R(x) \cong (\mathbf{Z}^r)^{s_2+s_4+s_6}$ and $\mathbf{Z}_0^{\mathscr{Z}} \cong \mathbf{Z}^r$. Let Z denote the kernel of $\theta : \oplus R(x) \to \mathbf{Z}^{\mathscr{Z}}$ defined analogously to $\tilde{\theta}$. (Note that $R(x) \cong \mathbf{Z}_0^{\mathscr{Z}}$ since $\mathscr{Z}(x) = \mathscr{Z}$.)

We have an injective map $\iota : \mathbf{Z}_0^{\mathscr{Z}} \to Z_0^{\mathscr{Z}}$ defined as follows: for $(a_0, \ldots, a_r) \in \mathbf{Z}_0^{\mathscr{Z}}$, we have $\iota(a_0, \ldots, a_r) = (a_0, \ldots, a_r, 0, \ldots, 0)$.

There is another natural injective map $\tau : \oplus R(x) \to \oplus \tilde{R}(x)$, which we shall define by giving its action on each $R(x)$.

If x corresponds to a supersingular point for which the j-invariant is neither 0 nor 1728, then $\tau(x_0, \ldots, x_r) = (x_0, \ldots, x_r, 0, \ldots, 0) \in \tilde{R}(x)$ for the same x.

If x corresponds to $j = 1728$ (the case of Sect. 1.2, Step III (i)), the image of $R(x)$ lies in $\tilde{R}(y_1) \oplus \tilde{R}(y_2) \oplus \tilde{R}(y_3) \subsetneqq \oplus \tilde{R}(x)$. For $(x_0, \ldots, x_r) \in R(x)$, its image in $\tilde{R}(y_1)$ is the element whose entries are: x_i in the i^{th} coordinate $\left(0 \leqq i \leqq \frac{r}{2} - 1\right)$, $-x_0 - \cdots - x_{\frac{r}{2}-1}$ in the coordinate corresponding to the added $\mathbf{P}^1$, and 0 elsewhere. Its image in $\tilde{R}(y_2)$ has as entries: $x_{\frac{r}{2}}$ in the $\frac{r}{2}^{\text{th}}$ coordinate, $-x_{\frac{r}{2}}$ in the coordinate corresponding to the added $\mathbf{P}^1$, and 0 elsewhere. Its image in $\tilde{R}(y_3)$ has as entries: x_i in the i^{th} coordinate $\left(\frac{r}{2} + 1 \leqq i \leqq r\right)$, $-x_{\frac{r}{2}+1} - \cdots - x_r$ in the coordinate corresponding to the added $\mathbf{P}^1$, and 0 elsewhere.

The case where $j = 0$ is similar, with z_1, z_2, z_3 replacing y_1, y_2, y_3.

Now, it is easy to verify that we obtain a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & Z & \longrightarrow & \oplus R(x)_0 & \xrightarrow{\theta} & \mathbf{Z}_0^{\mathscr{Z}} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \kappa} & & \downarrow{\scriptstyle \tau} & & \downarrow{\scriptstyle \iota} & & \\ 0 & \longrightarrow & \mathscr{X}(T(p^r M)) & \longrightarrow & \oplus \tilde{R}(x)_0 & \xrightarrow{\tilde{\theta}} & \mathbf{Z}_0^{\mathscr{Z}} & \longrightarrow & 0\,, \end{array}$$

where κ is induced by τ and ι. Since τ and ι are injective, so is κ. The rank of Z is $r(s_2 + s_4 + s_6 - 1)$ and so is that of $\mathscr{X}(T(p^r M))$; hence the cokernel of κ is a torsion abelian group.

A straight-forward argument using the definition of τ shows that $\operatorname{coker} \tau$ is torsion-free. By the Snake Lemma, $\operatorname{coker} \kappa$ injects into $\operatorname{coker} \tau$. Since $\operatorname{coker} \kappa$ is a torsion abelian group while $\operatorname{coker} \tau$ is torsion-free, we conclude that $\operatorname{coker} \kappa = 0$. Hence the groups Z and $\mathscr{X}(T(p^r M))$ are isomorphic. In other words, when r is even, we can use $X_0(p^r M) \otimes_{\mathbf{Z}} \bar{\mathbf{F}}_p$ rather than $\tilde{X}_0(p^r M) \otimes_{\mathbf{Z}} \bar{\mathbf{F}}_p$ to calculate its character group $\mathscr{X}(T(p^r M))$.

(ii) *When r is odd*

The argument that we use for this case is essentially the same as for the previous case, except that, when r is odd,

$$G = \mathbf{Z}^{(r-1)s_4'} \oplus \mathbf{Z}^{(r-1)s_6'} \oplus (\mathbf{Z}^{\frac{r+1}{2}} \oplus \mathbf{Z}^{\frac{r+1}{2}})^{s_4} \oplus (\mathbf{Z}^{\frac{r+1}{2}} \oplus \mathbf{Z} \oplus \mathbf{Z}^{\frac{r+1}{2}})^{s_6}.$$

and

$$u = (s_4' + s_6')(r-1) + s_4 + 2s_6\,.$$

1.4 Proof of Theorem 1

Let $\mathscr{J}$ (resp. $\mathscr{I}$) denote the set of irreducible components of $X_0(p^r M) \otimes_{\mathbf{Z}} \bar{\mathbf{F}}_p$ (resp. $X_0(pM) \otimes_{\mathbf{Z}} \bar{\mathbf{F}}_p$). Note that $\mathscr{J}$ has $r+1$ elements and $\mathscr{I}$ has 2 elements. We label

the elements of $\mathscr{J}$ as j_a as in Sect. 1.2. Similarly, the elements of $\mathscr{T}$ can be written as i_0 and i_1. From Sect. 1.3, we obtain the two exact sequences

$$0 \longrightarrow \mathscr{K}(T(p^r M)) \longrightarrow (\mathbf{Z}_0^{\mathscr{J}})^{s_2+s_4+s_6} \longrightarrow \mathbf{Z}_0^{\mathscr{T}} \longrightarrow 0\,,$$

and (setting $r = 1$ in Sect. 1.3)

$$0 \longrightarrow \mathscr{K}(T(pM)) \longrightarrow (\mathbf{Z}_0^{\mathscr{J}})^{s_2+s_4+s_6} \longrightarrow \mathbf{Z}_0^{\mathscr{J}} \longrightarrow 0\,.$$

On $X_0(p^r M) \otimes_{\mathbf{Z}} \bar{\mathbf{F}}_p$, an *ordinary* point on j_a can be described by two ordinary elliptic curves E_0, E_r (over $\bar{\mathbf{F}}_p$) and an isogeny $E_0 \xrightarrow{F_o^a} E_0^{(p^a)} \xrightarrow{\simeq} E_r^{(p^b)} \xrightarrow{V_r^b} E_r$, where F_o is the Frobenius for E_0 and V_r is the Verschiebung for E_r. Using this description, we determine the action of the maps $v_1, \ldots, v_{p^{r-1}}$ on $\mathscr{J}$ to be the following:

$$v_{p^h}(j_a) = \begin{cases} i_1 & h+1 \leqq a \leqq r \\ i_0 & 0 \leqq a \leqq h\,. \end{cases}$$

Now we choose the base of $\mathbf{Z}_0^{\mathscr{J}}$ to be $i_0 - i_1$ and that of $\mathbf{Z}_0^{\mathscr{J}}$ to be $j_0 - j_1, j_0 - j_2, \ldots, j_0 - j_r$. The map v_{p^h} then sends $j_0 - j_a$ to 0 if $1 \leqq a \leqq h$, and $i_0 - i_1$ if $h+1 \leqq a \leqq r$. This extends, by linearity, to a map $\mathbf{Z}_0^{\mathscr{J}} \to \mathbf{Z}_0^{\mathscr{J}}$, which shall also be called v_{p^h}. This gives us r commutative diagrams (one for each h: $0 \leqq h \leqq r-1$)

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathscr{K}(T(p^r M)) & \longrightarrow & (\mathbf{Z}_0^{\mathscr{J}})^{s_2+s_4+s_6} & \longrightarrow & \mathbf{Z}_0^{\mathscr{J}} \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & \mathscr{K}(T(pM)) & \longrightarrow & (\mathbf{Z}_0^{\mathscr{J}})^{s_2+s_4+s_6} & \longrightarrow & \mathbf{Z}_0^{\mathscr{J}} \longrightarrow 0\,, \end{array}$$

where the map $\mathbf{Z}_0^{\mathscr{J}} \to \mathbf{Z}_0^{\mathscr{J}}$ is v_{p^h}, and the other two vertical maps are induced by v_{p^h}.

The map $\nu = (v_1, \ldots, v_{p^{r-1}}) : \mathbf{Z}_0^{\mathscr{J}} \to \mathbf{Z}_0^{\mathscr{J}} \oplus \cdots \oplus \mathbf{Z}_0^{\mathscr{J}}$ is then given by the square $r \times r$ matrix (with the same bases as above)

$$\begin{pmatrix} 1 & 1 & \ldots & 1 \\ 0 & 1 & \ldots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & 1 \end{pmatrix},$$

which is clearly invertible.

Hence, the map ν is an isomorphism. The induced map

$$\nu : (\mathbf{Z}_0^{\mathscr{J}})^{s_2+s_4+s_6} \to (\mathbf{Z}_0^{\mathscr{J}})^{s_2+s_4+s_6} \oplus \cdots \oplus (\mathbf{Z}_0^{\mathscr{J}})^{s_2+s_4+s_6}$$

is hence also an isomorphism. This implies that

$$\mathscr{K}(T(p^r M)) \simeq \mathscr{K}(T(pM)) \oplus \cdots \oplus \mathscr{K}(T(pM)) \simeq \mathscr{K}((T(pM))^r)\,.$$

Therefore, we obtain the isomorphism $(T(pM))^r \cong T(p^r M)$.

2 The kernel K

2.1 Group of components and degeneracy maps

As representatives of the cusps of $X_0(N)$, we use as in Ogg [16] the vectors $\begin{pmatrix} x \\ y \end{pmatrix}$, where $y|N$, $y > 0$ and $(x, y) = 1$ with x taken modulo $(y, N/y)$. When $N = p$ a prime, there are only two cusps P_1 and P_p on $X_0(p)$, which are represented by $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$ and $\begin{pmatrix} 1 \\ p \end{pmatrix}$ respectively.

Let $c \in J_0(p)(\mathbf{Q})$ be the class of the cuspidal divisor $P_1 - P_p$. Then c is of finite order $n = \text{num}\left(\frac{p-1}{12}\right)$ [16].

The r degeneracy maps from $X_0(p^r)$ to $X_0(p)$ are denoted $v_1, \ldots, v_{p^{r-1}}$. Recall that these maps induce, via Pic functoriality, the maps $v_{p^\delta}^* : J_0(p) \to J_0(p^r)$. They also induce, via Albanese functoriality, maps $(v_{p^\delta})_* : J_0(p^r) \to J_0(p)$ between the Jacobians. (The Jacobian $J_0(N)$, regarded as an Albanese variety, parametrises the classes, modulo principal divisors, of divisors of degree 0 on $X_0(N)$.)

For $0 \leqq d \leqq r$ and $0 \leqq \delta \leqq r-1$, let

$$a(d, \delta) = \frac{p^{r-\delta-d}(p^d, p^\delta)^2}{(p^d, p^{r-d})}.$$

Information on the ramification behaviour of the cusps in the covering $v_{p^\delta} : X_0(p^r) \to X_0(p)$ may be obtained from the divisor of Δ_δ, where $\Delta_\delta(\tau) = \Delta(\delta\tau)$ and $\Delta(\tau) = q \prod_{n=1}^{\infty}(1-q^n)^{24}$, $q = e^{2\pi i\tau}$ (cf. [16]), and we deduce easily that

$$v_{p^\delta}^*(c) = \text{class of } \frac{1}{p-1}\sum_{d,x}(a(d,\delta) - a(d,\delta+1))\begin{pmatrix} x \\ p^d \end{pmatrix}. \tag{2}$$

Consequently, we obtain

Proposition 2. *With the above notations, we have* $(v_1)_* \circ v_{p^\delta}^*(c) = c$.

Proof. From (2), it follows that

$$\begin{aligned}(v_1)_* \circ v_{p^\delta}^*(c) &= \text{class of } \frac{1}{p-1}(a(0,\delta) - a(0,\delta+1))(P_1 - P_p) \\ &= \frac{1}{p-1}(p^{r-\delta} - p^{r-\delta-1})c \\ &= p^{r-\delta-1}c = c.\end{aligned}$$

□

Let Φ_p denote the group of components of the special fibre of the Néron model of $J_0(p)$. It is known that Φ_p is generated by the cuspidal divisor c (see [12, Appendix]). Therefore, we obtain from Proposition 2

Corollary. *The endomorphism* $(v_1)_* \circ v_{p^\delta}^*$ *of* $J_0(p)$ *induces the identity map on* Φ_p.

2.2 Proof of Theorem 2

Let

$$K_0 \stackrel{\text{def}}{=} \left\{ \begin{pmatrix} x_1 \\ \vdots \\ x_r \end{pmatrix} \;\middle|\; x_i \in \Sigma(p) \quad \text{for all } i, \sum_{i=1}^{r} x_i = 0 \right\}.$$

Since the degeneracy maps from $J_0(p)$ to $J_0(p^r)$ coincide on the Shimura subgroup $\Sigma(p)$ [11, Theorem 4], we have the inclusion $K_0 \subseteq K$.

Considering $J_0(p)^r$ and $J_0(p^r)$ as abelian varieties over $\mathbf{Q}_p$, [8, Sect. 5] and [2] show that the tori $T(p)^r$ and $T(p^r)$ in their reductions mod p have liftings $\underline{T}(p)^r$ and $\underline{T}(p^r)$ to $J_0(p)^r$ and $J_0(p^r)$ respectively.

Since the map $\gamma : J_0(p)^r \to J_0(p^r)$ induces an injection $T(p)^r \hookrightarrow T(p^r)$, it also induces an injection $\underline{T}(p)^r \hookrightarrow \underline{T}(p^r)$. In particular, $K \cap \underline{T}(p)^r = 0$. Consequently, the Galois action on K is trivial. Hence, K extends to a constant (finite, flat) group scheme $\mathbf{K}$ over $\mathbf{Z}_p$, and $\mathbf{K}$ embeds in the Néron model of $J_0(p)^r$. Furthermore, $\mathbf{K}$ has trivial intersection with $T(p)^r$. Since $J_0(p)$, and hence $J_0(p)^r$, has purely toric reduction, the special fibre $\mathbf{K}_s$ injects into the group of components Φ_p^r of $J_0(p)^r$).

Let $\gamma' : J_0(p^r) \to J_0(p)^r$ be the map defined by $\gamma'(x) = \begin{pmatrix} (v_1)_* x \\ \vdots \\ (v_{p^{r-1}})_* x \end{pmatrix}$. Then the composition $\gamma' \circ \gamma : J_0(p)^r \to J_0(p)^r$ can be represented by the matrix

$$\begin{pmatrix} (v_1)_* v_1^* & (v_1)_* v_p^* & \cdots & (v_1)_* v_{p^{r-1}}^* \\ \vdots & \vdots & \vdots & \vdots \\ (v_{p^{r-1}})_* v_1^* & (v_{p^{r-1}})_* v_p^* & \cdots & (v_{p^{r-1}})_* v_{p^{r-1}}^* \end{pmatrix}$$

Clearly, $K \subseteq \ker(\gamma' \circ \gamma)$. Passing to the Néron model, we see that, since $\mathbf{K}$ is flat, the fact that $\gamma' \circ \gamma$ annihilates the generic fibre (of $\mathbf{K}$) implies that it annihilates the special fibre as well. Let $\begin{pmatrix} x_1 \\ \vdots \\ x_r \end{pmatrix} \in \mathbf{K}_s \subseteq \Phi_p^r$. Then we have $(v_1)_* v_1^* x_1 + (v_1)_* v_p^* x_2 + \cdots + (v_1)_* v_{p^{r-1}}^* x_r = 0$. By the corollary to Proposition 2, it follows that $x_1 + \cdots + x_r = 0$. Therefore, $\mathbf{K}_s \subseteq P = \left\{ \begin{pmatrix} x_1 \\ \vdots \\ x_r \end{pmatrix} \in \Phi_p^r \;\middle|\; \sum_{i=1}^{r} x_i = 0 \right\}$. This shows that $\mathrm{card}(\mathbf{K}_s)$ (and hence $\mathrm{card}(K)$) is at most $\left(\mathrm{num}\left(\frac{p-1}{12} \right) \right)^{r-1} = \mathrm{card}(\Sigma(p))^{r-1} = \mathrm{card}(K_0)$. Since $K_0 \subseteq K$, we conclude that $K = K_0$.

3 Congruence relations between cusp forms of level p and p^2

In this section, we shall apply a special case of Theorem 2 to the problem of establishing congruence relations between weight-2 cusp forms of levels p and p^2.

More precisely, in view of Theorem 6 in the introduction, we shall prove Theorems 3, 4 and 5.

The problem of finding congruence relations between cusp forms of different levels has been extensively studied. For example, let p, p' be distinct primes, and let M be prime to pp'. Consider a weight-2 Hecke eigenform $f = \sum a_n q^n$ of level dividing $p'M$ and divisible by p'. Let $\mathcal{O}$ be the ring of integers in some (sufficiently large) finite extension of $\mathbf{Q}(\ldots, a_n, \ldots)$, and let $\lambda \subsetneqq \mathcal{O}$ be a prime ideal such that the characteristic l of $\mathbf{F} = \mathcal{O}/\lambda$ is prime to $pp'M$. Assume that the Galois representation associated to f

$$\varrho_\lambda : \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}) \longrightarrow GL_2(\mathbf{F})$$

is irreducible. Ribet (cf. [19, 20]) showed that, if one of the congruences

$$\mathrm{Tr}(\varrho_\lambda(\mathrm{Frob}_p)) \equiv \pm(p+1) \bmod l \tag{3}$$

holds, then one can find a weight-2 newform $g = \sum b_n q^n$ of level N', where N' divides $pp'M$ and is divisible by pp', such that $a_r \equiv b_r \bmod \lambda$ for almost all primes r. Generalizations to forms of higher weights have been obtained by Diamond [6], Jordan and Livné [9].

A particular case of Ribet's result, with $M = 1$, implies that, if one starts with a weight-2 newform f of level p', and (3) holds, then one can find a weight-2 newform g of level pp' such that $a_r \equiv b_r \bmod \lambda$ for almost all primes r. Here, p and p' are distinct. In this section, we study the complementary problem of what happens when $p = p'$.

Problem. *Given a weight-2 newform $f = \sum a_n q^n$ on $\Gamma_0(p)$ (p a prime), let λ be a prime ideal in the ring of integers $\mathcal{O}$ of a sufficiently large extension of $\mathbf{Q}$ in $\bar{\mathbf{Q}}$ such that the characteristic of the residue field $\mathcal{O}/\lambda$ is* not *p. When is there a weight-2 newform $g = \sum b_n q^n$ of level p^2 such that $a_r \equiv b_r \bmod \lambda$ for all primes $r \neq p$?* [1]

As explained in the introduction, due to Theorem 6, this above problem becomes one of determining whether a given prime in $\mathbf{T}_X$ is a prime of fusion. To achieve this, we borrow ideas from Ribet's proof in [19] and make use of Theorem 2 with $M = 1$ and $r = 2$ (cf. [19, Theorem 4.3]). After some preliminary definitions and notations in Sect. 3.1, we construct in Sect. 3.2 a $\mathbf{T}_X$-module Ω whose support contains only primes of fusion. Then in Sects. 3.3 and 3.4, we study a $\mathbf{T}_X$-module Δ which has a filtration (of $\mathbf{T}_X$-submodules) of the form

$$\Delta = M_0 \supseteq M_1 \supseteq M_2 \supseteq M_3 = 0\,, \tag{4}$$

where M_1/M_2 is isomorphic to Ω and $M_2 = K$. We also show that M_0, M_1, M_2 and Ω are all $\mathbf{T}$-stable.

The proof of Theorem 3 is given in Sect. 3.5, by making use of the fact $\mathrm{Supp}_{\mathbf{T}} \Delta = \mathrm{Supp}_{\mathbf{T}} \Sigma(p) \cup \mathrm{Supp}_{\mathbf{T}} \Omega$ and Proposition 19.2 of [12]. Theorem 3, together with the map $\psi : \mathbf{T}_X \to \mathbf{T}$ alluded to in the introduction, is subsequently used in Sect. 3.6 to deduce Theorem 4. Finally in Sect. 3.7, we give a direct characterization of the primes of fusion, without having to go via the support of Ω in $\mathbf{T}$.

[1] Ribet has informed me that this problem may also be answered using results of Carayol [3]

3.1 Definitions and notations

For the rest of this paper, we let $M = 1$ and $r = 2$ as in the introduction.

Consider the map $\gamma : J_0(p)^2 \to J_0(p^2)$. Let A denote its image, and let $\iota : A \to J_0(p^2)$ be the natural inclusion. Let Θ be the canonical divisor on $J_0(p^2)$ and let ϕ_Θ be the canonical polarization of $J_0(p^2)$. Then Θ and ι induce an invertible sheaf $\mathscr{L}$ on A. Let $\phi_{\mathscr{L}} : A \to A^\vee$ denote the isogeny defined by $\mathscr{L}$, where $A^\vee$ is the abelian variety dual to A. Let $K_{\mathscr{L}}$ denote the kernel of $\phi_{\mathscr{L}}$.

The map γ induces an isogeny $\delta : J_0(p)^2 \to A$, which in turn gives rise to a pullback $\delta^* \mathscr{L}$ of $\mathscr{L}$ on $J_0(p)^2$. Since $\phi_{\delta^* \mathscr{L}} = \delta^\vee \circ \phi_{\mathscr{L}} \circ \delta$, where $\delta^\vee$ is the dual of δ, we have $\deg(\phi_{\delta^* \mathscr{L}}) = \deg(\delta)^2 \deg(\phi_{\mathscr{L}})$. Therefore, the kernel

$$\Delta \stackrel{\text{def}}{=} K_{\delta^* \mathscr{L}}$$

is finite.

Let $\gamma' : J_0(p^2) \to J_0(p)^2$ be the map defined in Sect. 2.2. Its kernel is an extension of a finite group by an abelian subvariety B of $J_0(p^2)$. In fact, B is the kernel of the map $J_0(p^2) \xrightarrow{\phi_\Theta} J_0(p^2) \xrightarrow{\iota^\vee} A^\vee$.

We also define $h : J_0(p) \to J_0(p) \times J_0(p)$ to be the map given by $h(y) = \begin{pmatrix} w_p py \\ y \end{pmatrix}$, where w_p is the Atkin-Lehner involution on $J_0(p)$. Then noting that $w_p py = -y$ for $y \in \Sigma(p)$, we deduce from Theorem 2

Theorem 2′. *The kernel K of γ is isomorphic to $\Sigma(p)$ via h, i.e., $K = h(\Sigma(p))$.*

Corollary. *The kernel K is a* **T***-module.*

This follows from the fact that $\Sigma(p)$ is a **T**-module.

Finally, we fix the following notations:

J: the Jacobian $J_0(p)$,

Σ: the Shimura subgroup $\Sigma(p)$ of J,

C: the cuspidal subgroup of J,

$n = \text{num}\left(\dfrac{p-1}{12}\right)$: the cardinality of Σ and C,

l: a prime other than 2 and 3 that divides n, and l^f the exact power of l dividing n,

$\Sigma_l, C_l, \ldots$: the l-primary parts of $\Sigma, C, \ldots$.

3.2 The $\mathbf{T}_X$-module Ω

Let Ω be the intersection

$$\Omega = A \cap B .$$

It is the kernel of the map $A \xrightarrow{\iota} J_0(p^2) \xrightarrow{\phi_\Theta} J_0(p^2) \xrightarrow{\iota^\vee} A^\vee$, so $K_{\mathscr{L}} = \Omega$. The intersection $\Omega = A \cap B$ is therefore a finite subgroup of $J_0(p^2)$.

To understand the action of $\mathbf{T}_{p^2}$ on Ω, we first describe the action of $\mathbf{T}_{p^2}$ on $J \times J$. For primes $r \nmid p$, the Hecke operator $T_r \in \mathbf{T}_{p^2}$ is simply the Hecke operator T_r on

J, acting diagonally on the product $J \times J$. To show that U_p stabilizes $J \times J$, we need the following lemma.

Lemma 1. *We have the identities $v_1 U_p = T_p v_1$ and $v_p U_p = p v_1$, where each side of both formulae is regarded as a correspondence from $X_0(p^2)$ to $X_0(p)$.*

The lemma follows easily from the definitions of degeneracy maps and Hecke operators.

Lemma 1 shows, in particular, that $U_p \in \mathbf{T}_{p^2}$ acts as the matrix $\begin{pmatrix} T_p & p \\ 0 & 0 \end{pmatrix}$ on $J \times J$, so we have $U_p^2 - T_p U_p = 0$.

Corollary. *The Hecke operator U_p annihilates $H \stackrel{\text{def}}{=} h(J) = \left\{ \begin{pmatrix} w_p p y \\ y \end{pmatrix} \middle| \, y \in J \right\}$.*

Proof. This follows readily from Lemma 1 and the fact that $T_p = -w_p$ on J. □

Lemma 1 also shows that A is stable under the action of $\mathbf{T}_{p^2}$ we just described. Since A corresponds to the old subspace X, the action of $\mathbf{T}_{p^2}$ on A factors through $\mathbf{T}_X$.

Using Lemma 1 again, we see that $\ker \gamma'$ is stabilized by $\mathbf{T}_{p^2}$. Since B is the connected component of $\ker \gamma'$, it is also $\mathbf{T}_{p^2}$-stable. This action factors through $\mathbf{T}_Y$ since B corresponds to Y.

We conclude therefore that the action of $\mathbf{T}_{p^2}$ on Ω factors through both $\mathbf{T}_X$ and $\mathbf{T}_Y$. Hence, any prime in the support of Ω is automatically a prime of fusion.

3.3 The $\mathbf{T}_X$-module Δ

From the definition of Δ, we see readily that Δ contains $\ker \delta = K$, and there is a canonical skew-symmetric $\mathbf{G}_m$-valued pairing $e^{\delta^* \vee}$ on $K_{\delta^* \vee} \times K_{\delta^* \vee}$ that is trivial on $K \times K$. Let $K^\perp$ be the orthogonal complement to K under this pairing. Then $K \subsetneq K^\perp$ and $K^\perp / K \cong K_\vee = \Omega$ (see [15, Sect. 23]).

Proposition 3. *We have the equality $h(J[p^2 - 1]) = \Delta$.*

Proof. Since $\gamma = \iota \circ \delta$ and γ' is the dual of γ, it follows that $\gamma' \circ \gamma = \delta^\vee \circ \iota^\vee \circ \phi_\Theta \circ \iota \circ \delta = \delta^\vee \circ \phi_\vee \circ \delta = \phi_{\delta^* \vee}$. In particular, we have the equality $\Delta = \ker(\gamma' \circ \gamma)$.

The map $\gamma' \circ \gamma$, in matrix form, is $\begin{pmatrix} p & T_p \\ T_p & p \end{pmatrix}$ (cf. Sect. 2.2). If $\begin{pmatrix} x \\ y \end{pmatrix} \in \Delta$, then $py = -T_p x = w_p x$ and $px = w_p y$, where w_p is the Atkin-Lehner involution. In particular, $x = w_p p y$ and $(p^2 - 1)y = 0$. Conversely, if $y \in J_0(p)[p^2 - 1]$, then clearly $\begin{pmatrix} p & T_p \\ T_p & p \end{pmatrix} \begin{pmatrix} w_p p y \\ y \end{pmatrix} = 0$. □

Corollary 1. *The group Δ is a $\mathbf{T}$-module.*

Proof. Since $J[p^2 - 1]$ is $\mathbf{T}$-stable, so is $\Delta = h(J[p^2 - 1])$. □

Corollary 2. *The Hecke operator U_p annihilates Δ, and hence annihilates K and $K^\perp$.*

Proof. This follows immediately from Proposition 3 and the corollary to Lemma 1. □

Corollary 3. *The groups Δ and K are $\mathbf{T}_X$-modules.*

Proof. Since $J[p^2-1]$ and Σ are stable under T_r ($r \neq p$ prime), we see that Δ and K are stable under such T_r. Since U_p annihilates Δ and K (Corollary 2), we see that Δ and K are $\mathbf{T}_X$-stable. □

We shall next analyse $K^\perp$ in the filtration

$$\Delta \supseteq K^\perp \supseteq K \supseteq 0\,. \tag{5}$$

In particular, we shall prove

Proposition 4. *The orthogonal complement $K^\perp$ of K in Δ under the pairing $e^{\delta^*\,\prime}$ is $h(\Sigma^\perp)$, where $\Sigma^\perp$ is the orthogonal complement of Σ in $J[p^2-1]$ under the Weil pairing $\bar{e}_{p^2-1}$.*

3.4 The orthogonal complement $K^\perp$

In this section, we let m be $\dfrac{p^2-1}{n}$, where $n = \text{num}\left(\dfrac{p-1}{12}\right)$.

Recall the Weil pairing $\bar{e}_n$ (see [15, p. 183] for the definition) on $J[n]$:

$$\begin{aligned} \bar{e}_n : J[n] \times J[n] &\to \mu_n \\ (x, y) &\mapsto \bar{e}_n(x, y)\,. \end{aligned} \tag{6}$$

Since $\bar{e}_n$ is a perfect pairing, we obtain the isomorphism

$$\begin{aligned} J[n] &\xrightarrow{\cong} \text{Hom}(J[n], \mu_n) \\ y &\mapsto (y^\sharp : x \mapsto \bar{e}_n(x, y)). \end{aligned} \tag{7}$$

The cuspidal group C is the subgroup of $J(\mathbf{Q})$ generated by c, the class of the divisor $P_1 - P_p$ (cf. Sect. 2.1), and is cyclic of order n. Restricting $c^\sharp$ to Σ, we obtain a homomorphism $c^\sharp \in \Sigma^\wedge = \text{Hom}(\Sigma, \mu_n)$. Proposition 19.2 of [12] says that, for $l \neq 2$, $c^\sharp$ projects onto a generator of $\Sigma_l^\wedge$, the l-primary part of $\Sigma^\wedge$, if and only if $\mathbf{Z}_l = \mathbf{T}_\lambda$.

Next, consider the pairing

$$\begin{aligned} \bar{e}_{mn} = \bar{e}_{p^2-1} : J[p^2-1] \times J[p^2-1] &\to \mu_{p^2-1} \\ (x, y) &\mapsto \bar{e}_{p^2-1}(x, y)\,. \end{aligned}$$

As in the previous pairing $\bar{e}_n$, the generator c of C determines a homomorphism $c^\flat \in \Sigma_l^\wedge = \text{Hom}(\Sigma_l, \mu_{lf})$.

For any $\sigma \in \Sigma$, we have the following relation:

$$(c^\flat(\sigma))^m = \bar{e}_{nm}(\sigma, c)^m = \bar{e}_n(m\sigma, mc) = (mc)^\sharp(m\sigma)\,.$$

Using this relation and the fact $l \nmid m$, we verify readily that $c^\sharp$ projects onto a generator of $\Sigma_l^\wedge$ if and only if so does $c^\flat$.

Proposition 5. *For $x, y \in J[p^2-1]$, we have the identity*

$$e^{\delta^* \not\vee}(h(x), h(y)) = \bar{e}_{p^2-1}(x, py)\,.$$

Proof. We identify J with its dual, and we also identify $J \times J$ with its dual. Then the dual of h is the map $h^\vee : J \times J \to J$, defined by $h^\vee \begin{pmatrix} x \\ y \end{pmatrix} = w_p px + y$. Since $\phi_{\delta^* \not\vee} = \begin{pmatrix} p & T_p \\ T_p & p \end{pmatrix}$ on $J \times J$ with kernel Δ, its pullback $h^* \delta^* \not\vee$ on J via the homomorphism h gives rise to the isogeny $\phi_{h^* \delta^* \not\vee} : J \to J$ defined by $y \mapsto p(p^2-1)y$, i.e., $\phi_{h^* \delta^* \not\vee}$ is the multiplication-by-$p(p^2-1)$ map on J.

For $x, y \in J[p^2-1]$,

$$\begin{aligned} e^{\delta^* \not\vee}(h(x), h(y)) &= (e^{\delta^* \not\vee}(h(x), h(y)))^{p^2} = (e^{h^* \delta^* \not\vee}(x, y))^{p^2} \\ &= (\bar{e}_{p(p^2-1)}(x, y))^{p^2} = (\bar{e}_{(p^2-1)}(px, py))^p = \bar{e}_{nm}(x, py)\,. \end{aligned}$$

□

The multiplication-by-p map acts as an involution on $J[p^2-1]$. It also acts as the identity map on the Shimura subgroup Σ. Hence if we let y run through the elements of Σ, we obtain Proposition 4 stated in Sect. 3.3.

Corollary. *The orthogonal complement $K^\perp$ is a* **T***-module, hence so is Ω.*

Proof. We show that $K^\perp$ is **T**-stable by demonstrating that $\Sigma^\perp$ is **T**-stable. First, we have the identity

$$\bar{e}_{p^2-1}(\eta x, y) = \bar{e}_{p^2-1}(x, \eta^\vee y)\,, \tag{8}$$

where $x, y \in J[p^2-1]$, $\eta \in \mathrm{End}(J)$ and $\eta^\vee$ denotes the dual of η. Next, we observe that $w_p^\vee = w_p = -T_p$, and $T_r^\vee = T_r$ for all primes $r \neq p$. We also know that $\mathrm{End}(J) = \mathbf{T}$. Combining all these observations, and letting x run through the elements of Σ in (8), we see that $\Sigma^\perp$, hence $K^\perp$, is **T**-stable.

Since $\Omega \cong K^\perp / K$, it follows that Ω is also **T**-stable. □

3.5 Proof of Theorem 3

Let λ be in $\mathrm{Supp}_{\mathbf{T}} \Delta$.

3.5.1 Non-Eisenstein primes

The Eisenstein ideal $\mathfrak{I} \subsetneq \mathbf{T}$ is the ideal generated by $w_p + 1$ and $T_r - (1 + r)$ for all primes $r \neq p$. It is well-known that $\mathrm{Ann}_{\mathbf{T}} \Sigma = \mathfrak{I}$ [12, II, Proposition 11.7].

Hence, the support of Σ in $\mathbf{T}$ consists exactly of the Eisenstein primes. Suppose that $\lambda \in \mathrm{Supp}_{\mathbf{T}}\, \Delta$ is non-Eisenstein. In particular, λ is *not* in $\mathrm{Supp}_{\mathbf{T}}\, \Sigma$.

The groups Σ and $\Sigma^\wedge$ are dual to each other, and the annihilator of $\Sigma^\wedge$ in $\mathbf{T}$ is in fact the image of the Eisenstein ideal $\mathfrak{I}$ under the Rosati involution on $\mathrm{End}^o(J)$ with respect to the line bundle defined by the Θ-divisor. However, in this case, this involution turns out to be the identity. Therefore, we have $\mathrm{Ann}_{\mathbf{T}}\, \Sigma^\wedge = \mathfrak{I} = \mathrm{Ann}_{\mathbf{T}}\, \Sigma$, and $\mathrm{Supp}_{\mathbf{T}}\, \Sigma^\wedge = \mathrm{Supp}_{\mathbf{T}}\, \Sigma$. Consequently, we have $\mathrm{Supp}_{\mathbf{T}}\, \Delta = \mathrm{Supp}_{\mathbf{T}}\, \Sigma \cup \mathrm{Supp}_{\mathbf{T}}\, \Omega$. When $\lambda \in \mathrm{Supp}_{\mathbf{T}}\, \Delta$ is non-Eisenstein, we have $\lambda \notin \mathrm{Supp}_{\mathbf{T}}\, \Sigma$, so we conclude that $\lambda \in \mathrm{Supp}_{\mathbf{T}}\, \Omega$ and these are the only non-Eisenstein primes in $\mathrm{Supp}_{\mathbf{T}}\, \Omega$. This proves (i) of Theorem 3.

3.5.2 Eisenstein primes

There is a one-to-one correspondence between the Eisenstein primes in $\mathbf{T}$ and the prime numbers dividing n [12, II, Sect. 9]. In fact, for l a prime dividing n, the Eisenstein prime λ that corresponds to l is the ideal $(\mathfrak{I}, l)$.

In this section, we identify Δ with $J[p^2 - 1]$.

(I) We assume that $\mathbf{T}_\lambda \neq \mathbf{Z}_l$.

By Proposition 19.2 of [12], we see that in this case $c^\sharp$, and hence $c^\flat$, does not project onto a generator of $\Sigma_l^\wedge$. Hence, we see from the exact sequence

$$0 \longrightarrow \Sigma^\perp \longrightarrow \Delta \longrightarrow \Sigma^\wedge \longrightarrow 0 \tag{9}$$

that $C_l \cap \Sigma_l^\perp \neq 0$. In particular, $C[l] \subsetneqq \Sigma_l^\perp$.

Therefore, we have that $\Sigma_l^\perp[\mathfrak{I}] \supsetneqq \Sigma_l \oplus C[l]$, which implies that $0 \neq \Sigma_l^\perp[\mathfrak{I}]/\Sigma_l \subsetneqq \Omega_l[\mathfrak{I}]$. Consequently, $\Omega[\lambda] = \Omega[\mathfrak{I}, l] \neq 0$, which clearly implies that $\Omega_\lambda \neq 0$, i.e. $\lambda \in \mathrm{Supp}_{\mathbf{T}}\, \Omega$.

(II) Next, we treat the case where $\mathbf{T}_\lambda = \mathbf{Z}_l$.

First, note that $\Delta_l = J[l^f]$. Hence, $\mathrm{card}(\Delta_l) = (l^f)^{2g}$ and $\mathrm{card}(\Sigma_l^\perp) = (l^f)^{2g-1}$, where $g = \dim J$.

Proposition 19.2 of [12] and (9) imply that $C_l \cap \Sigma_l^\perp = 0$. Hence $C_l \oplus \Sigma_l^\perp \subsetneqq \Delta_l$. By considering cardinalities, we have the equality $C_l \oplus \Sigma_l^\perp = \Delta_l$.

Lemma 2. *As ideals in* $\mathbf{T}$, $\mathrm{Ann}_{\mathbf{T}}\, \Omega_l = \mathrm{Ann}_{\mathbf{T}}(\mathfrak{I}/(l^f) \cap \mathfrak{I})$.

Proof. Assume first that $T \in \mathbf{T}$ satisfies $T\mathfrak{I} \subsetneqq (l^f)$. Then, T induces a map $T : \Delta_l \to \Delta_l[\mathfrak{I}]$. Since $J_l[\mathfrak{I}] = C_l \oplus \Sigma_l$, we have also $\Delta_l[\mathfrak{I}] = C_l \oplus \Sigma_l$. Composing T with the surjection $\Delta_l[\mathfrak{I}] \to \Delta_l[\mathfrak{I}]/\Sigma_l \cong C_l$, we obtain a map

$$\alpha : \Delta_l \longrightarrow \Delta_l[\mathfrak{I}]/\Sigma_l\,.$$

We want to show that $\Sigma_l^\perp$ is in $\ker \alpha$. By duality, this means that we want to show that the image of $\alpha^\wedge$ is contained in Σ_l, where $\alpha^\wedge$ is the map

$$\alpha^\wedge : (\Delta_l[\mathfrak{I}]/\Sigma_l)^\wedge \to \Delta_l\,.$$

Since $\mathbf{T}$ acts on $\Delta_l[\mathfrak{I}]$ via the quotient $\mathbf{T}/\mathfrak{I}$, the image of $\alpha^\wedge$ is in $\Delta_l[\mathfrak{I}] = C_l \oplus \Sigma_l$. However, when we consider the action of Galois on $(\Delta_l[\mathfrak{I}]/\Sigma_l)^\wedge$, we see that it is a μ-type group (see [12]), so the image of $\alpha^\wedge$ must lie in Σ_l.

Now assume that $T\Sigma_l^\perp \subsetneqq \Sigma_l$. We want to show that $T\mathfrak{I} \subsetneqq (l^f)$. This is equivalent to showing that $T\mathfrak{I}$ annihilates $\Delta_l = J[l^f]$ because $\mathbf{T} = \mathrm{End}(J)$. For $i \in \mathfrak{I}$, we have a map

$$Ti : \Delta_l \to \Delta_l .$$

By considering the $\bar{e}_n$-pairing (6), it follows that the image of Ti lies in Σ_l and Ti kills $\Sigma_l^\perp$. Hence, we deduce a map

$$Ti : \Sigma_l^\wedge \to \Sigma_l .$$

As Galois modules, $\Sigma_l^\wedge$ is $\mathbf{Z}/l^f\mathbf{Z}$ and Σ_l is μ_{lf}. Since $l \neq 2$, Ti is trivial, i.e. $Ti \in (l^f)$. □

Now we return to the proof of Theorem 3. To check if $\lambda \in \mathrm{Supp}_{\mathbf{T}}\, \Omega$, it suffices to check if $\lambda \supsetneqq \mathrm{Ann}_{\mathbf{T}}\, \Omega_l = \mathrm{Ann}_{\mathbf{T}}(\mathfrak{I}/(l^f) \cap \mathfrak{I})$.

To complete the proof of the theorem, we only need to show now that λ does *not* contain $\mathrm{Ann}_{\mathbf{T}}(\mathfrak{I}/(l^f) \cap \mathfrak{I})$.

Since $\mathbf{T}_\lambda = \mathbf{Z}_l$, from $\mathbf{T}/\mathfrak{I} \simeq \mathbf{Z}/n\mathbf{Z}$, we have $\mathfrak{I}\mathbf{T}_\lambda = l^f\mathbf{Z}_l$. In particular, $\mathfrak{I}\mathbf{T}_\lambda = (\mathfrak{I} \cap (l^f))\mathbf{T}_\lambda$. If $\mathrm{Ann}_{\mathbf{T}}(\mathfrak{I}/(l^f) \cap \mathfrak{I}) \subsetneqq \lambda$, then $\mathbf{Z}_l = \mathbf{T}_\lambda = \mathrm{Ann}_{\mathbf{T}_\lambda}(\mathfrak{I}\mathbf{T}_\lambda/((l^f) \cap \mathfrak{I})\mathbf{T}_\lambda) \subsetneqq \lambda\mathbf{T}_\lambda = l\mathbf{Z}_l$.

This is clearly a contradiction. Hence, $\mathrm{Ann}_{\mathbf{T}}(\mathfrak{I}/(l^f) \cap \mathfrak{I}) \not\subseteq \lambda$.

This completes the proof of Theorem 3.

3.6 Primes of fusion

In Sect. 3.2, we observed that any prime in the support of Ω is a prime of fusion. Since $\mathrm{Supp}_{\mathbf{T}_X}\, \Omega$ is contained in $\mathrm{Supp}_{\mathbf{T}_X}\, \Delta$, we shall start with a prime $\mathfrak{m}$ in $\mathrm{Supp}_{\mathbf{T}_X}\, \Delta$ and decide when $\mathfrak{m}$ is in $\mathrm{Supp}_{\mathbf{T}_X}\, \Omega$.

Recall that (corollary to Lemma 1) U_p annihilates $H = h(J)$, and, for every prime $r \neq p$, $T_r \in \mathbf{T}_X$ acts diagonally on H. Therefore, the ring $\mathbf{T}_X$ acts on H. Since H is isomorphic to J, we obtain a map (cf. introduction) $\psi : \mathbf{T}_X \to \mathrm{End}(J) = \mathbf{T}$ that sends T_r to T_r ($r \neq p$ prime) and sends U_p to 0. If we let $R = \mathbf{Z}[\ldots, T_r, \ldots]$ be the ring generated by the T_r's, then ψ induces a surjective map $\psi' : \mathbf{T}_X/(U_p) \to R$.

Proposition 6. *The map $\psi' : \mathbf{T}_X/(U_p) \xrightarrow{\simeq} R$ is an isomorphism.*

Proof. Let $\varrho : R \to \mathbf{T}_X/(U_p)$ be the map that sends T_r to T_r. Then ϱ is clearly surjective. The composition of maps $\psi' \circ \varrho$ is the identity map on R. Consequently, ψ' is injective and is therefore an isomorphism. □

Let $\mathfrak{m} \in \mathrm{Supp}_{\mathbf{T}_X}\, \Delta$. Then, since Δ is finite, $\mathfrak{m}$ is maximal. Since $U_p \in \mathrm{Ann}_{\mathbf{T}_X}\, \Delta$ (Corollary 2 of Proposition 3), $U_p \in \mathfrak{m}$ and, thus, the image $\bar{\mathfrak{m}}$ of $\mathfrak{m}$ in $\mathbf{T}_X/(U_p)$ is also a maximal ideal. By Proposition 6, $\bar{\mathfrak{m}}$ can be regarded as a maximal ideal in

R. Since $\mathbf{T} = R[T_p]$ and $T_p^2 - 1 = 0$, we have that $\mathbf{T}$ is integral over R. By the going-up theorem of Cohen-Seidenberg, there exists a maximal ideal λ of $\mathbf{T}$ such that $\lambda \cap R = \bar{\mathfrak{m}}$. In particular, $\psi^{-1}(\lambda) = \mathfrak{m}$. Since $p^2 - 1 \in \mathrm{Ann}_{\mathbf{T}_X} \Delta \subseteq \mathfrak{m}$, such a λ automatically contains $p^2 - 1$ and is therefore in $\mathrm{Supp}_{\mathbf{T}} \Delta$. This proves the first statement of Theorem 4.

Let λ be such that $\lambda \in \mathrm{Supp}_{\mathbf{T}} \Omega$.

For $x \in \mathbf{T}_X$, we see that

$$x.\omega = \psi(x).\omega \quad \forall \omega \in \Omega\,. \tag{10}$$

If $x \in \mathrm{Ann}_{\mathbf{T}_X} \Omega$, then $\psi(x) \in \mathrm{Ann}_{\mathbf{T}} \Omega \subseteq \lambda$. Hence, $\mathrm{Ann}_{\mathbf{T}_X} \Omega \subseteq \psi^{-1}(\lambda) = \mathfrak{m}$, i.e., $\mathfrak{m} \in \mathrm{Supp}_{\mathbf{T}_X} \Omega$. This proves (i) of Theorem 4.

To prove (ii) of Theorem 4, suppose that $\lambda \notin \mathrm{Supp}_{\mathbf{T}} \Omega$ for all λ such that $\psi^{-1}(\lambda) = \mathfrak{m}$.

For any such λ, since $\lambda \in \mathrm{Supp}_{\mathbf{T}} \Delta$ but $\lambda \notin \mathrm{Supp}_{\mathbf{T}} \Omega$, the argument in Sect. 3.5.1 shows that $\lambda \in \mathrm{Supp}_{\mathbf{T}} \Sigma$ and is hence Eisenstein.

Next suppose $\mathfrak{m} = \psi^{-1}(\lambda_1) = \psi^{-1}(\lambda_2)$, where λ_1 and λ_2 are distinct Eisenstein primes. Let λ_1 be $(\mathfrak{I}, l_1)$ and let λ_2 be $(\mathfrak{I}, l_2)$, where l_1 and l_2 are distinct primes. Then $\mathfrak{m}$ contains l_1 and l_2, and hence $\mathfrak{m}$ contains 1, which contradicts the choice of $\mathfrak{m}$ as a prime ideal. Hence, λ is unique.

Now assume further that $\mathfrak{m} \in \mathrm{Supp}_{\mathbf{T}_X} \Omega$. Then $\Omega_{\mathfrak{m}} \neq 0$, and so, in particular, $\Omega[\mathfrak{m}] \neq 0$. Suppose that $0 \neq \omega_o \in \Omega[\mathfrak{m}]$. Let $\mathfrak{m}'$ be the ideal in $\mathbf{T}$ generated by $\psi(\mathfrak{m})$. In view of (10), we see that $\omega_o \in \Omega[\mathfrak{m}']$. Pick $a \in \mathrm{Ann}_{\mathbf{T}} \Omega$ such that $a \notin \lambda$, then $\omega_o \in \Omega[\mathfrak{m}' + (a)]$.

However, $\mathfrak{m}' + (a)$ is the entire ring $\mathbf{T}$. Otherwise, we have that $\psi(\mathfrak{m}) \subseteq \psi(\mathfrak{m}) + (a) \subseteq \mathfrak{m}' + (a) \subseteq \lambda'$ for some maximal ideal $\lambda' \neq \lambda$ (since $a \notin \lambda$). However, λ is the *unique* ideal containing $\psi(\mathfrak{m})$ in this case, so $\lambda = \lambda'$, which gives a contradiction. Hence, $\mathfrak{m}' + (a) = \mathbf{T}$. But then, $\Omega[\mathfrak{m}' + (a)] = 0$. This is a contradiction since $\omega_o \neq 0$ is in $\Omega[\mathfrak{m}' + (a)]$. Therefore, $\mathfrak{m} \notin \mathrm{Supp}_{\mathbf{T}_X} \Omega$. This completes the proof of Theorem 4.

3.7 $\mathrm{Supp}_{\mathbf{T}_X} \Omega$: *a direct determination*

Let $L(\Theta)$ be the line bundle on J associated with the canonical Θ-divisor (cf. Sect. 3.5.1). For $\zeta \in \mathrm{End}(J \times J)$, an easy calculation shows that the Rosati involution on $\mathrm{End}^0(J \times J)$ with respect to $L = p_1^* L(\Theta) \otimes p_2^* L(\Theta)$ sends $\zeta = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ (with $a, b, c, d \in \mathrm{End}(J)$) to $\zeta' = \begin{pmatrix} a^\dagger & c^\dagger \\ b^\dagger & d^\dagger \end{pmatrix}$, where p_1 and p_2 denote the projections onto J, and $x^\dagger$ denotes the image of x under the Rosati involution on J with respect to $L(\Theta)$.

For $r \neq p$ a prime, let

$$\eta_r = T_r - (1 + r)\,.$$

Then the η_r's act diagonally on $J \times J$. After identification of J with $J^\vee$ via the canonical Θ-divisor, it follows that $\eta_r' = \eta_r \in \mathrm{End}(J \times J)$.

Let $\Delta^\wedge$ be $\mathrm{Hom}(\Delta, \mathbf{G}_m)$. We let $\mathbf{T}_X$ act on $\Delta^\wedge$ in the following way: if $t \in \mathbf{T}_X$, $\phi \in \Delta^\wedge$ and $d \in \Delta$, then $(t\phi)(d) = \phi(td)$. This makes $\Delta^\wedge$ into a $\mathbf{T}_X$-module.

Proposition 7. *There is an isomorphism of $\mathbf{T}_X$-modules $\Delta \cong \Delta^\wedge$.*

Proof. From the pairing $e^{\delta^{*\prime\prime}} : \Delta \times \Delta \to \mu_{p^2-1}$, we deduce a map

$$\begin{aligned} \Delta &\to \Delta^\wedge \\ d &\mapsto [d' \mapsto e^{\delta^{*\prime\prime}}(d, d')]\,. \end{aligned}$$

Since the pairing is non-degenerate, $\Delta \cong \Delta^\wedge$ as groups. To see that it is compatible with the action of $\mathbf{T}_X$, it suffices to show that for $\eta \in \mathbf{T}_X$, we have that $e^{\delta^{*\prime\prime}}(\eta d, d') = e^{\delta^{*\prime\prime}}(d, \eta d')$. Since U_p annihilates Δ, this identity is trivial for $\eta = U_p$. Therefore, it suffices to check this equality for $\eta = T_r$ $(r \nmid p)$. From Proposition 5, we have, for $x, y \in J[p^2 - 1]$,

$$e^{\delta^{*\prime\prime}}(h(x), h(y)) = \bar{e}_{p^2-1}(x, py) = \bar{e}_{p(p^2-1)}(x, y)\,.$$

Let L be a line bundle on an abelian variety V and let $\phi_L : V \to V^\vee$ be the isogeny associated to L. For $\phi \in \mathrm{End}^o(V)$, the Rosati involution on $\mathrm{End}^o(V)$ with respect to L is given by $\phi \mapsto \phi^\dagger = \phi_L^{-1} \circ \phi^\vee \circ \phi_L$. There is a Riemann form E^L of L defined by

$$\begin{aligned} E^L : T_q(V) \times T_q(V) &\to \varprojlim \mu_{q^m} \\ E^L(x, y) &= (\bar{e}_{q^m}(x_m, \phi_L(y_m)))\,, \end{aligned}$$

where $x = (x_m)$, $y = (y_m)$ belong to $T_q(V)$ and q is a prime distinct from the characteristic of the base field of V. A well-known property of E^L is that $E^L(\phi x, y) = E^L(x, \phi^\dagger y)$ for any $\phi \in \mathrm{End}^o(V)$.

When we take $V = J$ and $\phi = \eta_r$, let q be a prime dividing $p^2 - 1$ and write $p(p^2 - 1) = q^e s$, where $(q, s) = 1$, we see that for $x, y \in J[p^2 - 1]$,

$$\bar{e}_{p(p^2-1)}(\eta_r x, y)^s = \bar{e}_{q^e}(\eta_r s x, sy) = \bar{e}_{q^e}(sx, \eta_r sy) = \bar{e}_{p(p^2-1)}(x, \eta_r y)^s\,.$$

This implies that $e^{\delta^{*\prime\prime}}(\eta_r d, d') = e^{\delta^{*\prime\prime}}(d, \eta_r d')$ for $d, d' \in \Delta$. Hence, $\Delta \cong \Delta^\wedge$ as $\mathbf{T}_X$-modules. □

Let $\mathfrak{I}_X$ be the annihilator (in $\mathbf{T}_X$) of the kernel K.

Lemma 3. *The ideal $\mathfrak{I}_X$ is generated by the elements: n, U_p and $\eta_r = T_r - (1 + r)$ for all primes $r \nmid p$.*

Proof. By Theorem 2 and the definition of $\mathfrak{I}_X$, we have that

$$\mathbf{T}_X/\mathfrak{I}_X \cong \mathrm{End}(K) \simeq \mathrm{End}(\Sigma) \cong \mathbf{Z}/n\mathbf{Z}\,.$$

Let $I = \langle n, U_p, \eta_r \ (\forall r \neq p) \rangle$. Since n and η_r (regarded as elements of $\mathbf{T}$) annihilate Σ, they annihilate K as well. Since U_p annihilates Δ, and $K \subseteq \Delta$, it follows that $U_p \in \mathfrak{I}_X$. Hence, $I \subseteq \mathfrak{I}_X$. We therefore have the following commutative diagram

$$\begin{array}{ccc} \mathbf{Z}/n\mathbf{Z} & \longrightarrow & \mathbf{T}_X/I \\ \| & & \downarrow \\ \mathbf{Z}/n\mathbf{Z} & \cong & \mathbf{T}_X/\mathfrak{I}_X \,, \end{array}$$

where the maps $\mathbf{Z}/n\mathbf{Z} \to \mathbf{T}_X/I$ and $\mathbf{T}_X/I \to \mathbf{T}_X/\mathfrak{I}_X$ are surjective.

The lemma follows immediately from this diagram. □

Remark. Observe that $\mathfrak{I}_X = \psi^{-1}(\mathfrak{I})$.

Lemma 4. *The kernel of $\mathfrak{I}_X$ in Δ_l,* i.e., *$\Delta_l[\mathfrak{I}_X]$, is equal to the antidiagonal in $J_l[\mathfrak{I}] \times J_l[\mathfrak{I}]$.*

Proof. We first note that if an element x of J_l is annihilated by η_r for all primes $r \neq p$, then x is also annihilated by $w_p + 1$ (cf. [12, p. 114]). In other words, $J_l[\ldots, \eta_r, \ldots] = J_l[\mathfrak{I}]$.

If $\begin{pmatrix} w_p py \\ y \end{pmatrix} \in \Delta_l[\mathfrak{I}_X]$, then $\eta_r y = 0$ for all primes $r \neq p$, i.e., $y \in J_l[\mathfrak{I}]$. In particular, $w_p py = -y$ and $\Delta_l[\mathfrak{I}_X] \subseteq \left\{ \begin{pmatrix} -y \\ y \end{pmatrix} \middle| y \in J_l[\mathfrak{I}] \right\}$.

Conversely, $y \in J_l[\mathfrak{I}]$ implies that η_r (for all primes $r \neq p$) and n annihilate $\begin{pmatrix} -y \\ y \end{pmatrix}$. Moreover, since $n | p^2 - 1$, we have that $\begin{pmatrix} -y \\ y \end{pmatrix} = \begin{pmatrix} w_p py \\ y \end{pmatrix} \in \Delta_l$. Since U_p annihilates Δ, it follows from the previous lemma that $\begin{pmatrix} -y \\ y \end{pmatrix} \in \Delta_l[\mathfrak{I}_X]$. □

We are now ready to prove Theorem 5.

Assume first that $T \in \mathbf{T}_X$ is such that $T\mathfrak{I}_X \subseteq \mathrm{Ann}_{\mathbf{T}_X} \Delta_l$. Then T induces a map

$$T : \Delta_l \to \Delta_l[\mathfrak{I}_X] \,.$$

Let $D = \left\{ \begin{pmatrix} x \\ -x \end{pmatrix} \middle| x \in C \right\}$. Since $J_l[\mathfrak{I}] = \Sigma_l \oplus C_l$ for $l \neq 2$, it follows from the previous lemma that we have the equality $\Delta_l[\mathfrak{I}_X] = K_l \oplus D_l$. The map $\beta : \Delta_l \to \Delta_l[\mathfrak{I}_X]/K_l \simeq D_l$ composed of T and the canonical map $\Delta_l[\mathfrak{I}_X] \to \Delta_l[\mathfrak{I}_X]/K_l$ induces, by taking duals, a map

$$\beta^\wedge : D_l^\wedge \to \Delta_l^\wedge \cong \Delta_l \,.$$

We want to prove that $K_l^\perp$ is contained in the kernel of β, which, by duality, means that $\beta^\wedge(D_l^\wedge)$ is contained in K_l.

Since D_l is annihilated by η_r for all primes $r \neq p$, so is $\beta^\wedge(D_l^\wedge)$. Moreover, Δ_l is annihilated by n and U_p. Hence,

$$\beta^\wedge(D_l^\wedge) \subseteq \Delta_l[\mathfrak{I}_X] = K_l \oplus D_l \,.$$

Since $C^\wedge$ is a μ-type group (see[12]), so is $D_l^\wedge$. This means that $\beta^\wedge(D_l^\wedge)$ must lie in K_l. Hence we obtain $\mathrm{Ann}_{\mathbf{T}_X}(\mathfrak{I}_X/(\mathrm{Ann}_{\mathbf{T}_X}\,\Delta_l \cap \mathfrak{I}_X)) \subseteqq \mathrm{Ann}_{\mathbf{T}_X}\,\Omega_l$.

Conversely, assume that $TK_l^\perp \subseteqq K_l$.

We have $n\Delta_l = 0 \subseteqq K_l^\perp$ and $U_p\Delta_l = 0 \subseteqq K_l^\perp$.

For all $d \in \Delta$ and $\sigma \in K$,

$$e^{\delta^{*\vee}}(\eta_r d, \sigma) = e^{\delta^{*\vee}}(d, \eta_r \sigma) = 1$$

since $\eta_r\sigma = 0$. Therefore, for $d \in \Delta_l$, we have $\eta_r d \in K_l^\perp$, i.e., $\eta_r\Delta_l \subseteqq K_l^\perp$. Now for $i \in \mathfrak{I}_X$, Ti induces a map

$$Ti : \Delta_l \to K_l$$

whose kernel contains $K_l^\perp$. This gives a map $\Delta_l/K_l^\perp \to K_l$, i.e. $K_l^\wedge \to K_l$. The action of Galois on $K_l^\wedge$ is trivial while that on K_l is given by the cyclotomic character (see [12]), so (since $l \neq 2$) this last map is trivial, which in turn implies that $Ti\Delta_l = 0$. This completes the proof of Theorem 5.

4 The old subvariety and the old quotient of $J_0(p^2)$

In this final section, we apply Theorem 2′, as well as Proposition 3, to a question raised by Mazur [13, Sect. 2b, Remark]. Note that our abelian variety A is by construction the old subvariety of $J_0(p^2)$, and its dual $A^\vee$ is the old quotient of $J_0(p^2)$ (cf. [22]). The question that Mazur raised is to obtain information about the degree of the map

$$\phi_\vee : A \to A^\vee$$

defined in Sect. 3.1.

Since $\deg(\phi_{\delta^{*\vee}}) = \deg(\delta)^2 \deg(\phi_\vee)$, we have $\mathrm{card}(\Delta) = \mathrm{card}(K)^2 \deg(\phi_\vee)$. By Proposition 3, $\mathrm{card}(\Delta) = (p^2-1)^{2g}$, where g is the dimension of $J_0(p)$. By Theorem 2′, $\mathrm{card}(K) = n = \mathrm{num}\left(\dfrac{p-1}{12}\right)$. Therefore, we obtain

Theorem 7. *The isogeny $\phi_\vee$ is of degree $\dfrac{(p^2-1)^{2g}}{n^2}$, where g is the dimension of $J_0(p)$ and n is the numerator of $\dfrac{p-1}{12}$ when the latter is expressed in lowest terms.*

Acknowledgements. I would like to thank my advisor, Ken Ribet, for his guidance and the invaluable discussions we had while I was working on this project. I am also grateful to Bas Edixhoven for enlightening conversations, and to Dino Lorenzini for pointing out some errors in an earlier version. I also owe special thanks to the referee for his very careful and helpful comments. Finally, I would like to thank the National University of Singapore for the Overseas Graduate Scholarship I received while working on my dissertation.

References

1. Atkin, A.O.L., Lehner, J.: Hecke operators on $\Gamma_0(m)$. Math. Ann. **185**, 134–160 (1970)
2. Bosch, S., Lütkebohmert, W.: Stable reduction and uniformization of abelian varieties. II. Invent. Math. **78**, 257–297 (1984)
3. Carayol, H.: Sur les représentations Galoisiennes modulo ℓ attachées aux formes modulaires. Duke Math. J. **59**, 785–801 (1989)
4. Deligne, P., Rapoport, M.: Les schémas de modules de courbes elliptiques. In: Deligne, P., Kuyk, W. (eds.) Modular functions of one variable II. (Lect. Notes Math., vol. **349**, pp. 143–316) Berlin Heidelberg New York: Springer 1973
5. Deligne, P., Serre, J.-P.: Formes modulaires de poids 1. Ann. Sci. Ec. Norm. Supér. **7**, 507–530 (1974)
6. Diamond, F.: Congruence primes for cusp forms of weight $k \geqq 2$. (Astérisque, vols. **196–197**, pp. 205–213) Paris: Soc. Math. Fr. 1991
7. Edixhoven, S.J.: Minimal resolution and stable reduction of $X_0(N)$. Ann. Inst. Fourier **40** (no. 1), 31–67 (1990)
8. Grothendieck, A.: SGA 7 I, exposé IX. In: Grothendieck, A. (ed.) SGA7 (Lect. Notes Math., vol. **288**, pp. 313–523) Berlin Heidelberg New York: Springer 1972
9. Jordan, B., Livné, R.: Conjecture "epsilon" for weight $k > 2$. Bull. Am. Math. Soc. **21**, 51–56 (1989)
10. Katz, N.M., Mazur, B.: Arithmetic moduli of elliptic curves. (Ann. Math. Stud., vol. **108**) Princeton: Princeton University Press 1985
11. Ling, S., Oesterlé, J.: The Shimura subgroup of $J_0(N)$. (Astérisque, vols. **196–197**, pp. 171–203) Paris: Soc. Math. Fr. 1991
12. Mazur, B.: Modular curves and the Eisenstein ideal. Publ. Math., Inst. Hautes Etud. Sci. **47**, 33–186 (1978)
13. Mazur, B.: Rational isogenies of prime degree. Invent. Math. **44**, 129–162 (1978)
14. Milne, J.: Abelian varieties. In: Cornell, G., Silverman, J.H. (eds.) Arithmetic geometry. Berlin Heidelberg New York: Springer 1986
15. Mumford, D.: Abelian varieties. Oxford: Oxford University Press 1970
16. Ogg, A.: Rational points on certain elliptic modular curves. In: Diamond, H.G. (ed.) Analytic number theory. (Proc. Symp. Pure Math., vol. **24**, pp. 221–231) Providence, RI: Am. Math. Soc. 1973
17. Raynaud, M.: Spécialisation du foncteur de Picard. Publ. Math., Inst. Hautes Etud. Sci. **38**, 27–76 (1970)
18. Raynaud, M.: SGA 6, exposé XII (rédigé par S. Kleinman). In: Berthelot, P. et al. (eds.) SGA6 (Lect. Notes Math., vol. 1 **225**, pp. 595–615) Berlin Heidelberg New York: Springer 1971
19. Ribet, K.: Congruence relations between modular forms. In: Ciesielski, Z., Olech, C. (eds.) Proc. International Congress of Mathematicians (1983), pp. 503–514. Warsaw: PMV and Amsterdam: North-Holland 1984
20. Ribet, K.: On modular representations of $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ arising from modular forms. Invent. Math. **100**, 431–476 (1990)
21. Ribet, K.: Raising the levels of modular representations. In: Goldstein, C. (ed.) Sém. Th. Nombres, Paris 1987–88. (Prog. Math., vol. **81**, pp. 259–271) Boston Basel Stuttgart: Birkhäuser 1990
22. Ribet, K.: The old subvariety of $J_0(pq)$ In: van der Geer, G. (ed.) Arithmetic algebraic geometry. (Prog. Math., vol. **89**, pp. 293–307) Boston Basel Stuttgart: Birkhäuser 1991
23. Serre, J.-P.: Sur le représentations modulaires de degré 2 de $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$. Duke Math. J. **54**, 179–230 (1987)
24. Serre, J.-P., Tate, J.: Good reduction of abelian varieties. Ann. Math. **68**, 492–517 (1968)
25. Shimura, G.: Introduction to the arithmetic theory of automorphic functions. Princeton: Princeton University Press 1971
26. Swinnerton-Dyer, H.P.F., Birch, B.J.: Elliptic curves and modular functions. In: Birch, B.J., Kuyk, W. (eds.) Modular functions of one variable IV. (Lect. Notes Math., vol. **476**, pp. 2–32) Berlin Heidelberg New York: Springer 1975