On a result of Imin Chen.

Bas Edixhoven

March 19, 2022

1 Introduction, notation and results.

The aim of this text is to give another proof of a recent result of Imin Chen, concerning certain identities among zeta functions of modular curves, or, equivalently, isogenies between products of jacobians of these curves. I want to thank Imin Chen for pointing out a mistake in an earlier version of this text.

For \( n \geq 1 \) an integer, let \( X(n)_{\mathbb{Q}} \) be the modular curve which is the compactified moduli space (coarse if \( n < 3 \)) of pairs \( (E/S, \phi) \), where \( S \) is a \( \mathbb{Q} \)-scheme, \( E/S \) is an elliptic curve and \( \phi: (\mathbb{Z}/n\mathbb{Z})_{S}^{2} \to E[n] \) an isomorphism of group schemes over \( S \). By construction, the group \( \text{GL}_{2}(\mathbb{Z}/n\mathbb{Z}) \) acts from the right on \( X(n)_{\mathbb{Q}} \): an element \( g \) sends \( (E/S, \phi) \) to \( (E/S, \phi \circ g) \). This action induces a left action of the jacobian \( J(n)_{\mathbb{Q}} \) of \( X(n)_{\mathbb{Q}} \).

Let \( p \) be a prime number. Let \( X \) denote \( X(p)_{\mathbb{Q}} \) and \( G \) the group \( \text{GL}_{2}(\mathbb{F}_{p}) \). We will consider the following subgroups of \( G \): the standard “maximal torus” \( T \) consisting of diagonal matrices, a non-split maximal torus \( T' \) obtained by choosing an \( \mathbb{F}_{p} \)-basis of a field \( \mathbb{F}_{p^2} \) of \( p^2 \) elements, the normalizers \( N \) of \( T \) and \( N' \) of \( T' \). Note that \( N/T \) and \( N'/T' \) are both of order 2. Finally, let \( B_{+} \) and \( B_{-} \) denote the two Borel subgroups containing \( T \); \( B_{+} \) is the subgroup of upper triangular matrices and \( B_{-} \) the one of lower triangular matrices.

The quotients of \( X \) by some of these subgroups have the following interpretations. The quotient \( X/T' \) is usually denoted \( X(p)_{\text{non-split}} \). The constructions

\[
\begin{align*}
(1.0.1) \quad & (E/S, \phi) \mapsto (E/S, \langle \phi(1, 0) \rangle), \quad (E/S, \phi) \mapsto (E/S, \langle \phi(0, 1) \rangle) \\
(1.0.2) \quad & X/B_{+} \xrightarrow{\sim} X_{0}(p)_{\mathbb{Q}}, \quad X/B_{-} \xrightarrow{\sim} X_{0}(p)_{\mathbb{Q}} \\
(1.0.3) \quad & (E/S, \phi) \mapsto (E_{1}/S, \ker(\phi_{2} \circ \phi_{1}^{*})),
\end{align*}
\]

induce isomorphisms

where \( \phi_{1}: E \to E_{1} \) (resp. \( \phi_{2}: E \to E_{2} \)) is the isogeny whose kernel is the subgroup scheme generated by \( \phi(1, 0) \) (resp. \( \phi(0, 1) \)), induces an isomorphism

\[
(1.0.4) \quad X/T \xrightarrow{\sim} X_{0}(p^{2})_{\mathbb{Q}}
\]
Under this isomorphism the Atkin-Lehner involution \( w_{p^2} \) of \( X_0(p^2)_\mathbb{Q} \) corresponds to the non-trivial element of \( N/T \); the two maps \( X/T \to X/B_+ \) and \( X/T \to X/B_- \) correspond to the two standard degeneracy maps from \( X_0(p^2)_\mathbb{Q} \) to \( X_0(p)_\mathbb{Q} \).

The result of Chen is the following, see [2, Theorem 1 and §10].

1.1 Theorem. (Chen) The jacobian of \( X_0(p^2)_\mathbb{Q} \) is isogeneous to the product of the jacobian of \( X(p) \) \( \text{non-split} \) by the square of the jacobian of \( X_0(p)_\mathbb{Q} \). The jacobian of \( X_0(p^2)_\mathbb{Q}/\langle w_{p^2} \rangle \) is isogeneous to the product of the jacobian of \( X/N' \) by the jacobian of \( X_0(p)_\mathbb{Q} \).

The proof given by Chen is to show that the traces of the Hecke operators \( T_n \) (\( n \) prime to \( p \)) on the jacobians in the theorem satisfy the identities required to conclude by the Eichler–Shimura relations and Faltings’s isogeny theorem that one has the desired isogenies. We will prove a generalization of Theorem 1.1 using only the representation theory of \( G \) and some elementary properties of abelian varieties.

For a field \( k \), let \( \text{AV}(k) \) denote the category of abelian varieties over \( k \). Let \( \mathbb{Q} \otimes \text{AV}(k) \) denote the category of abelian varieties over \( k \) “up to isogeny”, i.e., its objects are those of \( \text{AV}(k) \) and for two objects \( A \) and \( B \) one has \( \text{Hom}_{\mathbb{Q} \otimes \text{AV}(k)}(A,B) = \mathbb{Q} \otimes \text{Hom}_{\text{AV}(k)}(A,B) \). For \( A \) an abelian variety over \( k \) we denote by \( \mathbb{Q} \otimes A \) the corresponding object of \( \mathbb{Q} \otimes \text{AV}(k) \). By construction, \( A \) and \( B \) are isogeneous if and only if \( \mathbb{Q} \otimes A \) and \( \mathbb{Q} \otimes B \) are isomorphic. The categories \( \mathbb{Q} \otimes \text{AV}(k) \) are \( \mathbb{Q} \)-linear, semi-simple and abelian.

Recall (e.g., see [3, §1]), that an additive category \( C \) is called pseudoabelian if for every object \( M \) of \( C \) every idempotent \( f \) in \( \text{End}(M) \) has a kernel (or, equivalently, an image). If \( C \) is additive, pseudoabelian and \( f \) in \( \text{End}(M) \) is an idempotent in \( C \), then the natural morphism from \( \text{im}(f) \oplus \ker(f) \) to \( M \) is an isomorphism. The categories \( \mathbb{Q} \otimes \text{AV}(k) \) are clearly additive and pseudoabelian.

For each subgroup \( H \) of \( G \) we define

\[
\text{pr}_H := \frac{1}{|H|} \sum_{h \in H} h \in \mathbb{Q}[G]
\]

Hence \( \text{pr}_H \) is the idempotent of \( \mathbb{Q}[G] \) that projects on the \( H \)-invariants. For two subgroups \( H_1 \) and \( H_2 \) of \( G \) such that \( \langle H_1 \cup H_2 \rangle = H_1 H_2 \), one has \( \text{pr}_{H_1} \text{pr}_{H_2} = \text{pr}_{\langle H_1 \cup H_2 \rangle} \). For \( H \) a subgroup and \( g \) in \( G \) one has \( g \text{pr}_H g^{-1} = \text{pr}_{gHg^{-1}} \), hence \( \text{pr}_H \) is a central idempotent if and only if \( H \) is a normal subgroup.

For each irreducible representation \( V \) of \( G \) over \( \mathbb{Q} \) let \( e_V \) be the corresponding central idempotent in \( \mathbb{Q}[G] \) which projects on the \( V \)-isotypical part. If \( V \) is absolutely irreducible, of dimension \( d \) and with character \( \chi \), one has:

\[
e_V := \frac{d}{|G|} \sum_{g \in G} \chi(g^{-1})g
\]

We will use only one idempotent of the form \( e_V \), namely, with \( V \) the representation with character \( \pi^-(1) \) (see Table 2.1). This representation is the \( p \)-dimensional irreducible subrepresentation
of the induction of the trivial representation from $B_+$ to $G$. It is clearly absolutely irreducible and it exists over $\mathbb{Q}$.

Let us for the moment admit the following proposition, whose proof will be given in the next section.

1.2 Proposition. Suppose that $p \neq 2$. The elements $\text{pr}_T(1-\text{pr}_G)$ and $\text{pr}_T(1-e^{-\pi-1})(1-\text{pr}_G)$ of the ring $\mathbb{Q}[G]$ are conjugate idempotents. Likewise, the elements $(\text{pr}_N + \text{pr}_{B_+})(1-\text{pr}_G)$ and $\text{pr}_N(1-\text{pr}_G)$ are conjugate idempotents.

Our generalization of Chen’s result is simply the following direct consequence of Proposition 1.2.

1.3 Theorem. Suppose that $p \neq 2$. Take elements $u$ and $v$ of $\mathbb{Q}[G]^*$ such that

\[ u\text{pr}_T(1-\text{pr}_G)u^{-1} = \text{pr}_T(1-e^{-\pi-1})(1-\text{pr}_G) \]
\[ v(\text{pr}_N + \text{pr}_{B_+})(1-\text{pr}_G)v^{-1} = \text{pr}_N(1-\text{pr}_G) \]

Let $\mathcal{C}$ be a $\mathbb{Q}$-linear pseudoabelian additive category. Let $M$ be an object of $\mathcal{C}$ with an action by the group $G$; this gives a morphism of rings $\mathbb{Q}[G] \to \text{End}(M)$. Then $u$ induces an isomorphism

\[ \text{pr}_T(1-\text{pr}_G)M \xrightarrow{\sim} \text{pr}_T(1-e^{-\pi-1})(1-\text{pr}_G)M \]

Likewise, $v$ induces an isomorphism

\[ \text{pr}_N(1-\text{pr}_G)M \oplus \text{pr}_{B_+}(1-\text{pr}_G)M \xrightarrow{\sim} \text{pr}_N(1-\text{pr}_G)M \]

To see that Theorem 1.2 is a special case, apply Theorem 1.3 to $\mathcal{C} := \mathbb{Q} \otimes \text{AV}(\mathbb{Q})$ and take $M = \mathbb{Q} \otimes \text{jac}(X)$, with $\text{jac}(X)$ the jacobian of $X$. For any subgroup $H$ of $G$ one then has $\text{pr}_H M = \mathbb{Q} \otimes \text{jac}(X/H)$. In this case $\text{pr}_G$ acts as zero on $M$, since $X/G$ has genus zero. The idempotent $e^{-\pi-1}$, acting on $\mathbb{Q} \otimes \text{jac}(X/T) = \mathbb{Q} \otimes J_0(p^2)$, projects on the old part, which is a product of two copies of $\mathbb{Q} \otimes J_0(p)$ (one way to see this is to note that the space of $T$-invariants in the representation corresponding to $\pi^{-1}$ is the direct sum of the two 1-dimensional spaces of $B_+$ and $B_-$-invariants). One also has to use the interpretations of the $X/H$ as explained in the beginning of this section. For the case $p = 2$, note that $X(2)_\mathbb{Q}$ has genus zero.

2 The proof of Proposition 1.2.

The notation is as in the previous section, in particular, $G = \text{GL}_2(F_p)$. We suppose that $p \neq 2$. We will need to do some calculations involving the irreducible characters of $G$, so for convenience of the reader and to fix the notation, we include its character table, taken from [1]:
2.1 Table. The character table of $G$.

| conjugacy class of $\begin{pmatrix} x & 0 \\ 0 & z \end{pmatrix}$ | $x \in \mathbb{F}_p^*$ | $(p+1)x \beta(x)$ | $(p-1)x \Lambda(x)$ | $x \alpha \det$ | $x \Lambda(x)$ |
|---|---|---|---|---|---|
| $(\begin{pmatrix} x & 0 \\ 0 & z \end{pmatrix})$ | $x \notin \mathbb{F}_p^*$ | $x \beta(y) + x \beta(y)$ | $0$ | $x \alpha \det$ | $x \Lambda(x)$ |
| $(\begin{pmatrix} x & 1 \\ 0 & z \end{pmatrix})$ | $x \notin \mathbb{F}_p^*$ | $x \alpha \beta(x)$ | $-\Lambda(x)$ | $x \alpha \det$ | $x \Lambda(x)$ |
| $(\begin{pmatrix} z \alpha & 0 \\ 0 & z \end{pmatrix})$ | $x \notin \mathbb{F}_p^*$ | $0$ | $-\Lambda(z) - \Lambda(z^p)$ | $x \alpha \det$ | $x \Lambda(z^p)$ |

In this table $\alpha$ and $\beta$ denote characters $\mathbb{F}_p^* \rightarrow \overline{\mathbb{Q}}^*$ and $\Lambda$ denotes a character $\mathbb{F}_p^{*2} \rightarrow \overline{\mathbb{Q}}^*$. For each effective character $\chi$ of $G$ we denote by $V_\chi$ some $\overline{\mathbb{Q}}[G]$-module with character $\chi$. For each irreducible $\chi$ and each of the subgroups $H \subset G$ mentioned at the beginning of §4, we will need to know the dimension $\dim(V_\chi^H)$ of the set of $H$-invariants in $V_\chi$. These dimensions are given in the following table, in which $\delta(x, y)$ denotes the Kronecker symbol, i.e., $\delta(x, y) = 1$ if $x = y$ and $\delta(x, y) = 0$ otherwise.

2.2 Table. The dimensions of the spaces $V_\chi^H$.

| $\chi$ | $\pi(\alpha, \beta)$ | $\pi(-\alpha)$ | $\alpha \det$ | $\pi(\Lambda)$ |
|---|---|---|---|---|
| $T$ | $\delta(\alpha \beta, 1)$ | $\delta(\alpha, 1) + \delta(\alpha^2, 1)$ | $\delta(\alpha, 1)$ | $\delta(\Lambda^p + 1, 1)$ |
| $N$ | $\delta(\alpha(-1), 1) \delta(\alpha \beta, 1)$ | $\delta(\alpha(-1), 1) \delta(\alpha^2, 1)$ | $\delta(\alpha, 1)$ | $\delta(\Lambda^p + 1, 1) - \delta(\Lambda^{(p+1)/2}, 1)$ |
| $T'$ | $\delta(\alpha \beta, 1)$ | $-\delta(\alpha, 1) + \delta(\alpha^2, 1)$ | $\delta(\alpha, 1)$ | $\delta(\Lambda^p + 1, 1)$ |
| $N'$ | $\delta(\alpha(-1), 1) \delta(\alpha \beta, 1)$ | $-\delta(\alpha, 1) + \delta(\alpha(-1), 1) \delta(\alpha^2, 1)$ | $\delta(\alpha, 1)$ | $\delta(\Lambda^p + 1, 1) - \delta(\Lambda^{(p+1)/2}, 1)$ |
| $B$ | 0 | $\delta(\alpha, 1)$ | $\delta(\alpha, 1)$ | 0 |

We will not give the computation of this table in detail, since it is a straightforward application of the theory of representations of finite groups, see for example [4]. As an example, let us do the case $\chi = \pi(\Lambda)$ and $H = N$ (the other computations are in fact easier). The group $N'$ can be identified with the subgroup of $\text{GL}_{\mathbb{F}_p}(\mathbb{F}_p^2)$ generated by $\mathbb{F}_p^{*2}$ and $\sigma$, where $\sigma$ is the automorphism of order two of $\mathbb{F}_p^2$. Then $N'$ is the disjoint union of $T' = \mathbb{F}_p^{*2}$ and $T' \sigma$. The conjugacy class in $G$ of $z \in T'$ is the conjugacy class of $\begin{pmatrix} z & 0 \\ 0 & z \end{pmatrix}$. The conjugacy class of $z \sigma$ is the one of $\begin{pmatrix} z^{(p+1)/2} & 0 \\ 0 & z^{-(p+1)/2} \end{pmatrix}$. One has:

\begin{equation}
\text{(2.2.1)} \quad \dim(V_\chi^H) = \dim \text{Hom}_H(\text{Res}_H^G(V_\chi), \overline{\mathbb{Q}}) = \frac{1}{|H|} \sum_{g \in H} \chi(g)
\end{equation}

The sum over the elements of $T'$ can be written as:

\begin{equation}
\text{(2.2.2)} \quad - \sum_z (\Lambda(z) + \Lambda(z^p)) + (p+1) \sum_x \Lambda(x)
\end{equation}
In this sum, $z$ runs through $\mathbb{F}_p^*$ and $x$ through $\mathbb{F}_p^*$. The first of the two terms of \((2.2.2)\) gives zero, the second contributes $\frac{1}{2}\delta(\Lambda^{p+1}, 1)$ to $\dim(\mathcal{V}_{\chi}^H)$. The sum over the elements of $T'\sigma$ can be written as
\[
(2.2.3) \sum_{z \in \mathbb{F}_p} \left( \Lambda\left(\frac{z(p+1)}{2}\right) + \Lambda\left(-\frac{z(p+1)}{2}\right) \right) - \sum_{z} \left( \Lambda\left(\frac{z(p+1)}{2}\right) + \Lambda\left(-\frac{z(p+1)}{2}\right) \right)
\]
The first of the two terms of \((2.2.3)\) contributes $\frac{1}{2}\delta(\Lambda^{p+1}, 1)$ to $\dim(\mathcal{V}_{\chi}^H)$ and the second term contributes $-\delta(\Lambda^{(p+1)/2}, 1)$. This completes the computation of $\dim(\mathcal{V}_{\chi}^H)$.

As promised, we will now give a proof of Proposition 1.2. In fact, that proposition is a direct consequence of the following one.

2.3 Proposition. Define $\mathbb{Q}[G] := \mathbb{Q}[G]/(pr_G)$ and denote the projection $\mathbb{Q}[G] \to \mathbb{Q}[G]$ by $u \mapsto \bar{u}$. Then the elements $pr_T$ and $pr_T(1 - e_{\pi(1)})$ of the ring $\mathbb{Q}[G]$ are conjugate idempotents. Likewise, the elements $pr_{N'} + pr_{B'}$ and $pr_N'$ are conjugate idempotents.

Proof. Consider the first statement. Both elements are clearly idempotents. The $\mathbb{Q}$-algebra $\mathbb{Q}[G]$ is a product of matrix algebras over division rings. Using Table 2.2, one verifies that the two elements in question generate, in each factor, two left ideals of the same dimension over $\mathbb{Q}$ (actually, one verifies this after extension of scalars to $\mathbb{Q}$). Lemma 2.4 then implies that the two elements are conjugates.

The proof of the second statement is almost the same. The element $pr_{N'} + pr_{B'}$ is an idempotent because $T'B_+ = G$. The rest of the proof runs as before. \(\square\)

2.4 Lemma. Let $\Delta$ be a division ring. Let $0 \leq k \leq n$ be integers. Then the group $\text{GL}_n(\Delta)$ acts transitively (by conjugation) on the set of idempotents of rank $k$ in $M_n(\Delta)$.

Proof. Consider the right $\Delta$-module $\Delta^n$. Then $M_n(\Delta)$ can be viewed as $\text{End}_{\Delta}(\Delta^n)$. The map that associates to an idempotent of rank $k$ its kernel and image is a bijection between the set of such idempotents and the set of pairs of $\Delta$-submodules $(V_1, V_2)$ such that $\dim_{\Delta}(V_2) = k$ and $\Delta^n = V_1 \oplus V_2$. One verifies easily that $\text{Aut}_{\Delta}(\Delta^n)$ acts transitively on the set of such pairs. \(\square\)

References

[1] P. Cartier. Détermination des caractères des groupes finis simples: travaux de Lusztig. Séminaire Bourbaki, Exp. 658 (1986).

[2] Imin Chen. The jacobian of the modular curve $X_{\text{non-split}}^+(p)$. Oxford, 1994.

[3] A.J. Scholl. Classical motives. Proceedings of Symposia in Pure Mathematics 55 (1994), Part 1, pp. 163–187.

[4] J-P. Serre. Représentations linéaires des groupes finis. Hermann, Paris 1978 (3ème édition corrigée).