ANOTHER LOOK AT RATIONAL TORSION OF MODULAR JACOBIANS

KENNETH A. RIBET AND PRESTON WAKE

Abstract. We study the rational torsion subgroup of the modular Jacobian $J_0(N)$ for N a square-free integer. We give a new proof of a result of Ohta on a generalization of Ogg's conjecture: for a prime number $p \nmid 6N$, the p-primary part of the rational torsion subgroup equals that of the cuspidal subgroup. Whereas previous proofs of this result used explicit computations of the cardinalities of these groups, we instead use their structure as modules for the Hecke algebra.

1. Introduction

Let N be a square-free integer and let $J_0(N)$ be the Jacobian of the modular curve $X_0(N)$. In the case where N is prime, Ogg computed the order of the cuspidal subgroup (the subgroup of $J_0(N)$ generated by linear equivalence classes of differences of cusps) [Ogg73] and conjectured that the cuspidal subgroup is the whole rational torsion subgroup [Ogg75]. Mazur's proof of Ogg's conjecture was one of the principal results of [Maz77].

Ogg's computation of the order of the cuspidal subgroup has been generalized to other modular curves by Kubert and Lang (see [KL81] for example). The order of the cuspidal subgroup for $X_0(N)$ with square-free N has been computed by Takagi [Tak97] using Kubert–Lang theory.

A number of authors have considered the generalization of Ogg's conjecture to $J_0(N)$ where N is a positive integer that is not necessarily prime. Since the cuspidal subgroup of $J_0(N)$ may not consist entirely of rational points, the generalization states that the rational torsion subgroup of $J_0(N)$ is *contained in* the cuspidal subgroup of this Jacobian. See Lorenzini [Lor95], Conrad–Edixhoven–Stein [CES03], Ohta [Oht13, Oht14], Yoo [Yoo16], and Ren [Ren18] for details. In particular, Ohta [Oht14] has proven the generalization of Ogg's conjecture to square-free N. That is, he proved that the p-primary parts of $J_0(N)(\mathbb{Q})_{\mathrm{tor}}$ and of the cuspidal subgroup are equal for $p \geq 5$ (and $p = 3$ if $3 \nmid N$). The computation of the order of the class group by Takagi was a key input in Ohta's proof.

In this article, we give a new proof that, for a prime $p \nmid 6N$, the p-primary parts of $J_0(N)(\mathbb{Q})_{\mathrm{tor}}$ and of the cuspidal subgroup are equal. Our proof is by "pure thought" — we do not compute the order of either group but instead analyze their structure as modules for the Hecke algebra.

(Ribet) Department of Mathematics, University of California, Berkeley, CA 94720-3840

(Wake) Department of Mathematics, Michigan State University, East Lansing, MI 48824

E-mail address: ribet@math.berkeley.edu, wakepres@msu.edu.

Because we do not consider the p-primary parts for primes p dividing $6N$, our results do not completely recover Ohta's. We have not investigated the possibility of adapting our method to handle these primes. See the PhD thesis of Lui [Lui19] for some computational evidence for the generalized Ogg conjecture for 2- and 3-primary parts.

1.1. **Structure of the proof.** Fix a prime $p \nmid 6N$. Let C denote the p-primary part of cuspidal subgroup and T denote the p-primary part of the rational torsion subgroup $J_0(N)(\mathbb{Q})_{\mathrm{tor}}$. Our proof of the following theorem is based on the structure of C and T as Hecke modules. See Section 2.1 for precise definitions of the Hecke operators we use.

Theorem 1.1. *The rational torsion subgroup T coincides with its subgroup C.*

Let $\mathbb{T}$ be the Hecke algebra acting on $J_0(N)$ and let $I \subset \mathbb{T}$ be the Eisenstein ideal (see Section 2.3 for the precise definitions). The following result is the essential contribution of this article.

Theorem 1.2. *The annihilators of T and C as $\mathbb{T}$-modules satisfy*

$$\mathrm{Ann}_{\mathbb{T}}(C) \subseteq I \subseteq \mathrm{Ann}_{\mathbb{T}}(T).$$

Because the annihilator of T is contained in the annihilator of its submodule C, the two inclusions of Theorem 1.2 imply the equalities

$$\mathrm{Ann}_{\mathbb{T}}(C) = I = \mathrm{Ann}_{\mathbb{T}}(T). \tag{1.3}$$

We deduce Theorem 1.1 from (1.3) at the end of Section 2.5, using an argument of Mazur to show that the Pontryagin dual of T is cyclic as a $\mathbb{T}$-module.

Corollary 1.4. *The index of I in $\mathbb{T}$ is the order of $C = T$.*

Proof. Indeed, the Pontryagin dual of T is isomorphic to $\mathbb{T}/I$ because it is a cyclic $\mathbb{T}$-module by Theorem 2.5 and has annihilator I by (1.3). □

We prove the inclusions $I \subseteq \mathrm{Ann}_{\mathbb{T}}(T)$ and $\mathrm{Ann}_{\mathbb{T}}(C) \subseteq I$ separately, by independent arguments. The Eichler–Shimura relation implies T is annihilated by $T_q - q - 1$ for almost all primes q (see Lemma 2.4). So, to prove the inclusion $I \subseteq \mathrm{Ann}_{\mathbb{T}}(T)$, it is enough to show that elements of this type generate I. That is the content of the following theorem, which we prove in Section 3 using Galois representations.

Theorem 1.5. *Let S be a finite set of prime numbers that contains all primes dividing $6Np$. The Eisenstein ideal I is generated by the set of all $T_q - q - 1$ with $q \notin S$.*

Let $\tilde{\mathbb{T}}$ be the Hecke algebra acting on the full space of modular forms (not just cusp forms) of weight 2 and level $\Gamma_0(N)$. Let $\tilde{I} \subset \tilde{\mathbb{T}}$ be the Eisenstein ideal and $J \subset \tilde{\mathbb{T}}$ be the ideal generated by the set of all $T_q - q - 1$ for all $q \notin S$. Let

$$\alpha : \tilde{\mathbb{T}}/J \twoheadrightarrow \tilde{\mathbb{T}}/\tilde{I}$$

be the quotient map arising from the inclusion $J \subseteq \tilde{I}$. The content of Theorem 1.5 is that $J = \tilde{I}$, or, in other words, that α is an isomorphism. To give the flavor of the proof of Theorem 1.5, we now explain informally why $\tilde{\mathbb{T}}/J$ and $\tilde{\mathbb{T}}/\tilde{I}$ have the same minimal primes: Think of $\mathrm{Spec}(\tilde{\mathbb{T}}/\tilde{I})$ as the set of normalized Eisenstein eigenforms and $\mathrm{Spec}(\tilde{\mathbb{T}}/J)$ as the set of those normalized eigenforms whose associated Galois

pseudorepresentation is $\epsilon + 1$, where $\epsilon : G_{\mathbb{Q}} \to \mathbb{Z}_p^\times$ is the p-adic cyclotomic character. Because of oldforms, the map sending an normalized eigenform to its Galois pseudorepresentation is not necessarily injective. However, for each $\ell \mid N$, the U_ℓ-eigenvalue singles out a root of the characteristic polynomial of Frobenius at ℓ, and the map sending an normalized eigenform to its pseudorepresentation plus this additional data *is* injective. We show that the normalized Eisenstein eigenforms fill out all the possibilities for roots of the characteristic polynomial of Frobenius at ℓ with pseudorepresentation $\epsilon + 1$. This shows that $\mathrm{Spec}(\tilde{\mathbb{T}}/\tilde{I}) \subseteq \mathrm{Spec}(\tilde{\mathbb{T}}/J)$ is an equality. In Section 3, we give a more precise version of this argument to establish that α is an isomorphism.

Our proof of the inclusion $\mathrm{Ann}_{\mathbb{T}}(C) \subseteq I$ is given in Section 5. It is based on an interpretation, due to Stevens [Ste85], of C in terms of the lattice of Eisenstein series that have *integral periods*. We use an integrality result about modular units to show that this lattice is contained in the lattice of Eisenstein series with integral q-expansion and thereby exhibit a subquotient of C that has annihilator I.

Remark 1.6. An alternate proof of the inclusion $\mathrm{Ann}_{\mathbb{T}}(C) \subseteq I$ will be given in forthcoming work of Jordan, Ribet, and Scholl related to [JRS22]. This proof uses p-adic Hodge theory to show that the Hecke algebra $\tilde{\mathbb{T}}$ is p-saturated in the endomorphism ring of the generalized Jacobian of $X_0(N)$ relative to the cusps, and then proceeds along the lines of the proof of [Rib83, (1.7)].

Remark 1.7. In Section 4, we prove an integrality result about modular units (Proposition 4.4) using arithmetic geometry techniques. This integrality also follows from an explicit description of the modular units given by Takagi [Tak97] using Kubert–Lang theory. We avoid invoking Takagi's result both in accordance with our desire for a 'pure thought' proof and to show that our method can be used to give alternate proofs of some of his results (see Corollary 6.1).

2. Preliminaries

In this section we set up notation for modular forms and Hecke algebras, recall a duality result, and employ arguments from [Maz77] used to reduce the proof of Theorem 1.1 to Theorem 1.2.

2.1. **Modular forms.** Let $M_2(N)$ denote the $\mathbb{C}$-vector space of modular forms of weight 2 and level $\Gamma_0(N)$ and let $S_2(N)$ and $E_2(N)$ be the subspaces of $M_2(N)$ consisting of cusp forms and Eisenstein series, respectively. For a subring $R \subset \mathbb{C}$, let $M_2(N, R) \subset M_2(N)$ denote the R-module of modular forms whose q-expansion (at the cusp ∞) is in $R[\![q]\!]$. Let $S_2(N, R) = S_2(N) \cap M_2(N, R)$ and $E_2(N, R) = E_2(N) \cap M_2(N, R)$.

The dimension of $E_2(N)$ is $2^r - 1$, where r is the number of prime divisors of N (see [DS05, Theorem 4.6.2, pg. 133], for example). For each $d \mid N$ with $d > 1$, let E_d be the element of $E_2(N)$ such that for prime numbers ℓ,

$$a_\ell(E_d) = \begin{cases} 1 & \text{if } \ell \mid d \\ \ell & \text{if } \ell \nmid d \end{cases},$$

if $\ell \mid N$, and $a_\ell(E_d) = 1 + \ell$ if $\ell \nmid N$. These eigenforms form a basis of $E_2(N)$. Since each E_d is in $E_2(N, \mathbb{Z}_{(p)})$, we infer that $E_2(N, \mathbb{Z}_{(p)})$ is a free $\mathbb{Z}_{(p)}$-module of rank $2^r - 1$ (although not necessarily with $\{E_d\}$ as basis).

2.2. **Hecke operators.** The spaces of modular forms just introduced are equipped with actions of the classical Hecke operators T_n for $n \geq 1$. These operators arise from correspondences on modular curves (see, for example, [Shi71, Chapter 7]). As such, they also act on geometric objects such as $J_0(N)$ and the divisor group of cusps, but there is some ambiguity as to how a correspondence acts (using either the "Picard" or the "Albanese" functoriality — see the discussion in [Rib90, pg. 443–444]). A summary of our conventions is:

- The endomorphism of $J_0(N)$ denoted T_ℓ here is the same as the one in [Rib90, pg. 444] defined using Picard functoriality. It satisfies $T_\ell = \xi_\ell^*$, where ξ_ℓ is the endomorphism defined by Shimura in [Shi71, Chapter 7].
- The action of T_ℓ on the cusps is the *dual* of the "standard" action (for example, our action of T_ℓ on the cusps is the same as the the action of ${}^tT_\ell$ on the cusps described in [Ste82, pg. 15]).

To avoid any ambiguity, we now spell this out in more detail.

We use the following notation for modular curves: $Y_0(N)^{\mathrm{an}}$ is the quotient of the upper half-plane by $\Gamma_0(N)$, thought of as a complex analytic manifold, and $Y_0(N)$ is the smooth model of $Y_0(N)^{\mathrm{an}}$ over $\mathbb{Z}_{(p)}$ (recall that $p \nmid N$, so such a smooth model exists). We use analogous notations $X_0(N)^{\mathrm{an}}$ and $X_0(N)$ for the closed modular curve. Let $C_0(N) = X_0(N) - Y_0(N)$ denote the set of cusps. Let $J_0(N)$ denote the Jacobian variety of $X_0(N)$.

For a prime number ℓ, let $t_\ell = \left(\begin{smallmatrix} 1 & 0 \\ 0 & \ell \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Q})^+$ and consider the subgroup $\Gamma_0(N;\ell) = \Gamma_0(N) \cap t_\ell^{-1}\Gamma_0(N)t_\ell$. Let $Y_0(N;\ell)^{\mathrm{an}}$ be the quotient of the upper half-plane by $\Gamma_0(N;\ell)$. There is a correspondence

$$\begin{array}{ccc} & Y_0(N;\ell)^{\mathrm{an}} & \\ {\scriptstyle \pi}\swarrow & & \searrow{\scriptstyle t_\ell} \\ Y_0(N)^{\mathrm{an}} & & Y_0(N)^{\mathrm{an}} \end{array}$$

where π is the quotient map and t_ℓ is the map induced by $x \mapsto t_\ell x$. This correspondence extends uniquely to give a correspondence on $X_0(N)$ that preserves the cusps; we use the same names π and t_ℓ for the maps in this correspondence. Define the element $T_\ell \in \mathrm{End}(J_0(N))$ by

$$T_\ell = (t_\ell)_* \pi^*.$$

The same formula defines an endomorphism T_ℓ of the group $\mathrm{Div}^0(C_0(N))$ of degree-zero divisors on the cusps. The map

$$\mathrm{Div}^0(C_0(N)) \to J_0(N)$$

sending a divisor to its class is equivariant for these actions of T_ℓ.

By identifying $M_2(N)$ with the space of differential forms on $Y_0(N)^{\mathrm{an}}$, the formula $T_\ell = (t_\ell)_*\pi^*$ gives an action of T_ℓ on $M_2(N)$. This action preserves the subspaces $S_2(N)$ and $E_2(N)$, and preserves the R-submodule $M_2(N,R)$ if R is a $\mathbb{Z}[1/N]$-algebra.

2.3. **Hecke algebras.** Let $\tilde{\mathbb{T}} \subset \mathrm{End}(M_2(N))$ be the $\mathbb{Z}_{(p)}$-algebra generated by the Hecke operators T_ℓ for all primes $\ell \geq 1$. Let $\tilde{I} \subset \tilde{\mathbb{T}}$ be the annihilator of the space of Eisenstein series. Let $\mathbb{T}$ be the image of $\tilde{\mathbb{T}}$ in $\mathrm{End}(S_2(N))$ and let $I \subset \mathbb{T}$ be the

image of $\tilde{I}$. As is customary, for a prime divisor ℓ of N, we denote the operator T_ℓ by U_ℓ.

2.4. **Duality.** The following duality is well known. The duality result for cuspforms (see, for example, [Rib83, Theorem 2.2]) extends to all modular forms because there is no nonzero mod p modular form of weight 2 and level $\Gamma_0(N)$ with constant q-expansion when $p > 3$. This fact can be proven using a mod p Atkin–Lehner-type result (see [Maz77, Lemma II.5.9, pg. 83] for the prime-level version; the proof generalizes to higher levels as in [Aga18, Lemma 3.5] or [Oht14, Lemma (2.1.1)]) together with the fact that there are no nonzero mod p modular forms of weight 2 and level 1 [Maz77, Proposition II.5.6, pg. 81]. Alternatively, a nonzero constant is the q-expansion of a modular form of weight 0, but, by [Kat77, Some Corollaries (2), pg. 55], a nonzero mod p modular form of weight 2 cannot have the same q-expansion as a modular form of smaller weight.

Lemma 2.1. *Let $M = M_2(N, \mathbb{Z}_{(p)})$.*

(1) The pairing

$$M \times \tilde{\mathbb{T}} \to \mathbb{Z}_{(p)}, \ (f, T) \mapsto a_1(Tf) \tag{2.2}$$

is a perfect pairing of free $\mathbb{Z}_{(p)}$-modules of finite rank.

(2) Let $X \subset M$ be a $\tilde{\mathbb{T}}$-submodule. The pairing (2.2) induces an isomorphism

$$\mathrm{Hom}(M/X, \mathbb{Z}_{(p)}) \cong \mathrm{Ann}_{\tilde{\mathbb{T}}}(X).$$

Moreover, if M/X is torsion free, then (2.2) induces an isomorphism

$$\mathrm{Hom}(X, \mathbb{Z}_{(p)}) \cong \tilde{\mathbb{T}}/\mathrm{Ann}_{\tilde{\mathbb{T}}}(X).$$

Proof. The analogue of (1) with $\mathbb{Q}$-coefficients is easy and standard. This analogue implies that the map

$$\Psi : M_2(N, \mathbb{Z}_{(p)}) \to \mathrm{Hom}_{\mathbb{Z}_{(p)}}(\tilde{\mathbb{T}}, \mathbb{Z}_{(p)}), \ \Psi(f)(T) = a_1(Tf)$$

is injective and that $\mathrm{coker}\,\Psi$ is a finite abelian p-group. To show that Ψ is an isomorphism, it suffices to show that $\mathrm{coker}\,\Psi$ is p-torsion free. Let $\phi \in \mathrm{Hom}_{\mathbb{Z}_{(p)}}(\tilde{\mathbb{T}}, \mathbb{Z}_{(p)})$ be such that $p\phi = \Psi(f)$ for some $f \in M_2(N, \mathbb{Z}_{(p)})$; we will show that ϕ is in the image of Ψ, and hence that $\mathrm{coker}\,\Psi$ is p-torsion free. Note that for all $n \geq 1$,

$$a_n(f) = \Psi(f)(T_n) = p\phi(T_n).$$

Since $\phi(T_n) \in \mathbb{Z}_{(p)}$ for all $n \geq 1$, this implies that $f \pmod p$ is a constant and thus it is 0, as was recalled in the sentences before the statement of the lemma. Hence $g := p^{-1}f$ is in $M_2(N, \mathbb{Z}_{(p)})$ and $\phi = \Psi(g)$ is in the image of Ψ. This shows that Ψ is an isomorphism, completing the proof of (1). Statement (2) follows immediately from (1). □

Lemma 2.3. *The $\mathbb{Z}_{(p)}$-module $\tilde{\mathbb{T}}/\tilde{I}$ is free of rank $2^r - 1$, where r is the number of prime divisors of N.*

Proof. Lemma 2.1(2) applied to $X = E_2(N, \mathbb{Z}_{(p)})$ gives an isomorphism

$$\tilde{\mathbb{T}}/\tilde{I} \cong \mathrm{Hom}_{\mathbb{Z}_{(p)}}(E_2(N, \mathbb{Z}_{(p)}), \mathbb{Z}_{(p)}).$$

In particular, $\tilde{\mathbb{T}}/\tilde{I}$ is a free $\mathbb{Z}_{(p)}$-module of the same rank as $E_2(N, \mathbb{Z}_{(p)})$, which is $2^r - 1$ as discussed in Section 2.1. □

2.5. **The Eichler–Shimura relation.** The following lemma, which is well known, shows that many of the elements of I annihilate T. In Section 3, we will prove the inclusion $I \subseteq \mathrm{Ann}_{\mathbb{T}}(T)$ by showing that these elements generate I.

Lemma 2.4. *For every prime $q \notin S$, the group T is annihilated by $T_q - q - 1$.*

Proof. Let q be a prime that is not in S. The Eichler–Shimura relation states that $T_q = \mathrm{Fr}_q + V_q$ on $J_0(N)_{/\mathbb{F}_q}$ [Maz77, pg. 89], where Fr_q is the Frobenius endomorphism of the group scheme $J_0(N)_{/\mathbb{F}_q}$ and V_q is the Verschiebung. Since Fr_q is the identity on $J_0(N)(\mathbb{F}_q)$, this implies that $T_q = 1+q$ on $J_0(N)(\mathbb{F}_q)$. But, since $q \nmid 2N$, the reduction modulo q map induces an injection $T \to J_0(N)(\mathbb{F}_q)$ of $\mathbb{T}$-modules (see [Kat81, Appendix], for example), so $T_q = 1 + q$ on T as well. □

2.6. **Cyclicity of the dual of T.** Theorem 1.1 follows from Theorem 1.2 together with the following mild generalization of a theorem Mazur [Maz77, Corollary II.14.8 pg. 199], which appears in the work of Ohta [Oht14, Proposition (3.5.4)].

Theorem 2.5 (Mazur, Ohta)**.** *The Pontryagin dual of T is cyclic as a $\mathbb{T}$-module.*

Proof. It is equivalent to show that, for all maximal ideals $\mathfrak{m}$ of $\mathbb{T}$, the $\mathfrak{m}$-torsion subgroup of T, which we denote by $T[\mathfrak{m}]$, has dimension at most 1 as a $\mathbb{T}/\mathfrak{m}$-vector space. Since, as was noted in the proof of Lemma 2.4, the reduction map $T \to J_0(N)(\mathbb{F}_p)$ is injective, $T[\mathfrak{m}]$ is contained in the $\mathfrak{m}$-torsion subgroup of $J_0(N)[p](\bar{\mathbb{F}}_p)$. Furthermore, as in [Maz77, Proposition II.14.7 pg. 119], the Cartier–Serre isomorphism induces an injective homomorphism

$$J_0(N)[p](\bar{\mathbb{F}}_p) \otimes_{\mathbb{F}_p} \bar{\mathbb{F}}_p \;\hookrightarrow\; H^0(X_0(N)_{/\bar{\mathbb{F}}_p}, \Omega^1).$$

Note that, as in Mazur's proof, the Cartier–Serre isomorphism is Hecke-equivariant with respect to the our chosen Hecke action on $J_0(N)$ (see also [Wil80, Proposition 6.5]), so this is a homomorphism of $\mathbb{T}$-modules. The $\mathfrak{m}$-torsion subgroup of the right-hand side has dimension at most 1 as a $\mathbb{T}/\mathfrak{m}$-vector space by the q-expansion principle. Hence $T[\mathfrak{m}]$ has dimension at most 1 as a $\mathbb{T}/\mathfrak{m}$-vector space. □

2.7. **Equality of annihilators implies equality.** The cyclicity proven in Theorem 2.5 implies that the equality $T = C$ of $\mathbb{T}$-modules follows from the equality $\mathrm{Ann}_{\mathbb{T}}(T) = \mathrm{Ann}_{\mathbb{T}}(C)$ of annilhilators:

Proof of Theorem 1.1 assuming Theorem 1.2. The inclusion $C \subseteq T$ induces a surjection $T^\vee \twoheadrightarrow C^\vee$ of Pontryagin duals. By Theorem 1.2 and (1.3), this surjection is a map of $\mathbb{T}/I$-modules and $C^\vee$ is a faithful $\mathbb{T}/I$-module. Then the map $T^\vee \twoheadrightarrow C^\vee$ is an isomorphism because, by Theorem 2.5, $T^\vee$ is a cyclic $\mathbb{T}$-module. □

3. Galois representations and the annihilator of T

In this section, we prove Theorem 1.5 and the inclusion $\mathrm{Ann}_{\mathbb{T}}(T) \supseteq I$ of Theorem 1.2. Fix a finite set S of prime numbers containing all primes dividing $6Np$.

3.1. **Galois representations.** Let $J \subset \tilde{\mathbb{T}}$ be the ideal generated by $T_q - q - 1$ for all $q \notin S$.

Lemma 3.1. *The ideal J contains the following elements:*

(a) $T_q - q - 1$ for each prime $q \nmid N$,
(b) $(U_\ell - 1)(U_\ell - \ell)$ for each prime $\ell \mid N$, and
(c) $\prod_{\ell \mid N}(U_\ell - 1)$, where the product is over the set of prime divisors of N.

We will prove Lemma 3.1 using properties of Galois representations associated to eigenforms. Before continuing with the proof, we review the required properties. To this end, fix a maximal ideal $\mathfrak{m} \subset \tilde{\mathbb{T}}$ and assume that $\mathfrak{m} \supseteq J$.

For each minimal prime ideal $\mathfrak{p} \subset \mathfrak{m}$, there is a corresponding (not necessarily cuspidal) eigenform $f_\mathfrak{p}$ with coefficients in $\mathcal{O}_\mathfrak{p} = \tilde{\mathbb{T}}_\mathfrak{m}/\mathfrak{p}$ (which is a finite extension of $\mathbb{Z}_p$), defined by $a_n(f_\mathfrak{p}) = T_n \pmod{\mathfrak{p}}$. Let $K_\mathfrak{p}$ be the field of fractions of $\mathcal{O}_\mathfrak{p}$. To each $f_\mathfrak{p}$, there is an associated two-dimensional semisimple Galois representation $\rho_\mathfrak{p}$ with coefficients in $K_\mathfrak{p}$, contructed by Shimura. See [DDT97, Theorem 3.1] for a list the properties of $\rho_\mathfrak{p}$, which have been established by the work of many mathematicians; we will rewrite these properties in terms of a representation $\rho_\mathfrak{m}$ that we now define.

Since $\mathbb{T}_\mathfrak{m}$ is reduced (see [CE98]), there is an injective homomorphism

$$\tilde{\mathbb{T}}_\mathfrak{m} \hookrightarrow \tilde{\mathbb{T}}_\mathfrak{m} \otimes \mathbb{Q} = \prod_{\mathfrak{p}|\mathfrak{m}} K_\mathfrak{p}. \tag{3.2}$$

The product of the Galois representations $\rho_\mathfrak{p}$ is a continuous representation

$$\rho_\mathfrak{m} : G_\mathbb{Q} \to \mathrm{GL}_2(\tilde{\mathbb{T}}_\mathfrak{m} \otimes \mathbb{Q})$$

with the following properties:

(1) $\rho_\mathfrak{m}$ is unramified outside Np,
(2) $\det(\rho_\mathfrak{m}) = \kappa_{\mathrm{cyc}}$, the p-adic cyclotomic character,
(3) $\mathrm{tr}(\rho_\mathfrak{m})(\mathrm{Fr}_q) = T_q$ for each prime $q \nmid Np$, where Fr_q is an arithmetic Frobenius.

Since $\mathfrak{m} \supseteq J$, the Chebotarev density theorem implies that $\mathrm{tr}(\rho_\mathfrak{m})(\sigma) \equiv \kappa_{\mathrm{cyc}}(\sigma) + 1 \pmod{\mathfrak{m}}$ for every $\sigma \in G_\mathbb{Q}$. This implies that $\mathfrak{m}$ is ordinary in the sense that T_p is invertible modulo $\mathfrak{m}$. Indeed, a theorem of Fontaine (see [Edi92, Theorem 2.6]) implies that the restriction of $\mathrm{tr}(\rho_\mathfrak{m}) \pmod{\mathfrak{m}}$ to the inertia group at p is the sum of two non-trivial characters in the non-ordinary case. Let $u_p \in \tilde{\mathbb{T}}_\mathfrak{m}^\times$ denote the unit root of $x^2 - T_p x + p$, which exists by Hensel's lemma.

The restrictions of $\rho_\mathfrak{m}$ to decomposition groups at primes dividing Np can be described as follows:

(4) For every prime $\ell \nmid N$ and every choice of arithmetic Frobenius $\mathrm{Fr}_\ell \in G_\mathbb{Q}$ the trace of $\rho_\mathfrak{m}(\mathrm{Fr}_\ell)$ is given by
$$\mathrm{tr}(\rho_\mathfrak{m})(\mathrm{Fr}_\ell) = U_\ell + \ell U_\ell^{-1}.$$
(5) For every σ in a decomposition group at p, the trace of $\rho_\mathfrak{m}(\sigma)$ is given by
$$\mathrm{tr}(\rho_\mathfrak{m})(\sigma) = \kappa_{\mathrm{cyc}}(\sigma)\lambda^{-1}(\sigma) + \lambda(\sigma)$$
where λ is the unramified character sending Frobenius to u_p

Proof of Lemma 3.1. It is enough to show the containment after completion at all maximal ideals $\mathfrak{m} \subset \tilde{\mathbb{T}}$. We can and do assume $\mathfrak{m} \supseteq J$ because the statement is clear if $J_\mathfrak{m} = \tilde{\mathbb{T}}_\mathfrak{m}$.

The Chebotarev density implies that the image of $\mathrm{tr}(\rho_\mathfrak{m})$ is contained in $\tilde{\mathbb{T}}_\mathfrak{m}$ and that $J_\mathfrak{m}$ is the ideal generated by

$$\mathrm{tr}(\rho_\mathfrak{m})(\sigma) - \kappa_{\mathrm{cyc}}(\sigma) - 1$$

for all $\sigma \in G_\mathbb{Q}$. It follows from (3) that $T_q - q - 1 \in J_\mathfrak{m}$ for all $q \nmid N$.

To prove part (a), it remains to show that $T_p - p - 1 \in J_{\mathfrak{m}}$, or, equivalently, that $u_p - 1 \in J_{\mathfrak{m}}$. Let σ be an element of the inertia group at p such that $\kappa_{\mathrm{cyc}}(\sigma) \not\equiv 1 \bmod p$. Then (5) implies

$$\mathrm{tr}(\rho_{\mathfrak{m}})(\mathrm{Fr}_p) - \kappa_{\mathrm{cyc}}(\mathrm{Fr}_p) - 1 = \kappa_{\mathrm{cyc}}(\mathrm{Fr}_p)(u_p^{-1} - 1) + u_p - 1 \in J_{\mathfrak{m}},$$
$$\mathrm{tr}(\rho_{\mathfrak{m}})(\sigma\mathrm{Fr}_p) - \kappa_{\mathrm{cyc}}(\sigma\mathrm{Fr}_p) - 1 = \kappa_{\mathrm{cyc}}(\sigma)\kappa_{\mathrm{cyc}}(\mathrm{Fr}_p)(u_p^{-1} - 1) + u_p - 1 \in J_{\mathfrak{m}}.$$

Subtracting these equations, we find that $(\kappa_{\mathrm{cyc}}(\sigma) - 1)\kappa_{\mathrm{cyc}}(\mathrm{Fr}_p)(u_p^{-1} - 1) \in J_{\mathfrak{m}}$. By the assumption on σ, the element $(\kappa_{\mathrm{cyc}}(\sigma) - 1)\kappa_{\mathrm{cyc}}(\mathrm{Fr}_p) \in \mathbb{Z}_p$ is a unit, so $(u_p^{-1} - 1) \in J_{\mathfrak{m}}$. Hence $T_p - p - 1 \in J_{\mathfrak{m}}$, completing the proof of (a).

For part (b), note that by (4)

$$\mathrm{tr}(\rho_{\mathfrak{m}})(\mathrm{Fr}_\ell) - \ell - 1 = U_\ell + \ell U_\ell^{-1} - \ell - 1 \in J_{\mathfrak{m}}.$$

Since $(U_\ell - 1)(U_\ell - \ell) = U_\ell(U_\ell + \ell U_\ell^{-1} - \ell - 1)$, this implies $(U_\ell - 1)(U_\ell - \ell) \in J_{\mathfrak{m}}$.

For part (c), let $x = \prod_{\ell | N}(U_\ell - 1)$. We will show that $x = 0$ in $\tilde{\mathbb{T}}_{\mathfrak{m}}$ by showing that x maps to zero in each factor $K_{\mathfrak{p}}$ under the injective map (3.2). First suppose that $f_{\mathfrak{p}}$ is an Eisenstein series. The only eigenforms in $E_2(N)$ are the forms E_d defined in Section 2.1, hence $f_{\mathfrak{p}} = E_d$ for some $d \mid N$ with $d > 1$. In particular, $a_\ell(f_{\mathfrak{p}}) = 1$ for every prime $\ell \mid d$, so x maps to zero in that factor. Next suppose that $f_{\mathfrak{p}}$ is a cuspform. Then $a_\ell(f_{\mathfrak{p}}) = 1$ for some $\ell \mid N$ by the following lemma of Ribet and Yoo. Hence $x = 0$ in $\tilde{\mathbb{T}}_{\mathfrak{m}}$. □

Lemma 3.3 (Ribet, Yoo)**.** *Let M be a square-free integer and let $p \nmid 6M$. Suppose that f is a newform of weight 2 and level M such that $a_q(f) \equiv q + 1 \pmod{\mathfrak{p}}$ for all $q \nmid Mp$. Then $a_\ell(f) = 1$ for some $\ell \mid M$.*

Proof. See [Yoo19]. □

3.2. **Proof that $J = \tilde{I}$.** We now prove Theorem 1.5, which is the claim that $J = \tilde{I}$, by showing that the elements of J listed in Lemma 3.1 generate $\tilde{I}$.

Proof of Theorem 1.5. We will show that the natural surjection $\alpha : \tilde{\mathbb{T}}/J \twoheadrightarrow \tilde{\mathbb{T}}/\tilde{I}$ is an isomorphism. This will imply that the elements $T_q - q - 1$ for $q \notin S$ generate $\tilde{I}$ and hence also generate I.

Let $N = \ell_1 \cdots \ell_r$ be the prime factorization of N and let $R = \mathbb{Z}_{(p)}[x_1, \ldots, x_r]$. By Lemma 3.1 part (a), the $\mathbb{Z}_{(p)}$-algebra homomorphism

$$s : R \to \tilde{\mathbb{T}}/J, \ x_i \mapsto U_i - 1$$

is surjective. Let $\mathcal{I} \subset R$ be the ideal generated by $x_1 x_2 \cdots x_r$ and $x_i(x_i + 1 - \ell_i)$ for $i = 1, \ldots, r$. The map s induces a surjection $\bar{s} : R/\mathcal{I} \twoheadrightarrow \tilde{\mathbb{T}}/J$ because $s(\mathcal{I}) = 0$ by Lemma 3.1 parts (b) and (c). We claim that $R/\mathcal{I}$ is a free $\mathbb{Z}_{(p)}$-module of rank $2^r - 1$, which is the same as the rank of $\tilde{\mathbb{T}}/\tilde{I}$ by Lemma 2.3. Indeed, consider the ideal $\mathcal{I}' \subset \mathcal{I}$ generated by $x_i(x_i + 1 - \ell_i)$ for $i = 1, \ldots, r$. Then $R/\mathcal{I}'$ is freely generated by the 2^r monomials of degree at most 1 in each x_i. The ideal generated by $x_1 x_2 \cdots x_r$ in $R/\mathcal{I}'$ is equal to its $\mathbb{Z}_{(p)}$-span, which is a direct summand of $R/\mathcal{I}'$ as $\mathbb{Z}_{(p)}$-modules. Since $\mathcal{I} = \mathcal{I}' + x_1 x_2 \cdots x_r R$, this implies that $R/\mathcal{I}$ is free of rank $2^r - 1$.

The composition

$$\alpha \circ \bar{s} : R/\mathcal{I} \twoheadrightarrow \tilde{\mathbb{T}}/\tilde{I}$$

is a surjective homomorphism of free $\mathbb{Z}_{(p)}$-modules of the same finite rank and is therefore an isomorphism. Since $\bar{s}$ is surjective, this implies that α is an isomorphism, which is the content of the theorem. □

Since $\mathrm{Ann}_{\mathbb{T}}(T) \supseteq J$ by Lemma 2.4, Theorem 1.5 implies the inclusion $\mathrm{Ann}_{\mathbb{T}}(T) \supseteq I$, which is one of the two inclusions of Theorem 1.2.

4. The period lattice of Eisenstein series

In this section, we introduce the period lattice in the space of Eisenstein series. This lattice is closely related to the cuspidal subgroup of $J_0(N)$ and to modular units by the work of Stevens [Ste85]. We show that the q-expansions of elements of the period lattice have coefficients in $\mathbb{Z}_{(p)}$ by first proving an analogous integrality property for q-expansions of modular units.

Recall from Section 2.2 the notation $Y_0(N)^{\mathrm{an}} \subset X_0(N)^{\mathrm{an}}$ for the analytic modular curves, $Y_0(N) \subset X_0(N)$ for their $\mathbb{Z}_{(p)}$-models, and $C_0(N) = X_0(N) - Y_0(N)$ for the set of cusps. If R is a commutative $\mathbb{Z}_{(p)}$-algebra, let $Y_0(N)_R$ and $X_0(N)_R$ denote the base-changes of $Y_0(N)$ and $X_0(N)$ to R.

4.1. **The period lattice.** For each Eisenstein series $f \in E_2(N)$, consider the period map $\int f : H_1(Y_0(N)^{\mathrm{an}}, \mathbb{Z}) \to \mathbb{C}$, defined by

$$\int f : \gamma \longmapsto \int_\gamma f(z)\, dz.$$

The *period lattice* $\mathcal{E}$ is the $\mathbb{Z}_{(p)}$-module consisting of those Eisenstein series f for which the image of $\int f$ is contained in $\mathbb{Z}_{(p)}$.

Let $U = (\mathcal{O}^\times_{Y_0(N)^{\mathrm{an}}}/\mathbb{C}^\times) \otimes_{\mathbb{Z}} \mathbb{Z}_{(p)}$ be the $\mathbb{Z}_{(p)}$-module of (analytic) modular units modulo scalars. We will refer to elements of U as *scalar classes* of modular units; note that the divisor of a modular unit depends only on its scalar class. Let $\tilde{C} = \mathrm{Div}^0(C_0(N)) \otimes_{\mathbb{Z}} \mathbb{Z}_{(p)}$ be the $\mathbb{Z}_{(p)}$-module of degree-zero divisors with cuspidal support. By definition,

$$C = \tilde{C}/\mathrm{div}(U).$$

Stevens establishes the isomorphism

$$\mathcal{D} : U \xrightarrow{\sim} \mathcal{E}, \quad \mathcal{D}(u)\, d\log(q) = d\log(u), \tag{4.1}$$

where $d\log(q) = 2\pi i\, dz$. He proves that $\mathrm{div}(u) = \mathrm{Res}(2\pi i \mathcal{D}(u))$ for all $u \in U$ [Ste85, pg. 521], where $\mathrm{Res}\colon \mathcal{E} \to \tilde{C}$ is the residue map defined by

$$\mathrm{Res}(f) = \sum_{x \in C_0(N)} \mathrm{Res}_x(f(z)dz)[x].$$

We will use this isomorphism, together with a integrality result for modular units, to study the integrality of q-expansions of elements of the period lattice.

4.2. **$\mathbb{Z}_{(p)}$-integrality of modular units.** We show that every (analytic) modular unit of level $\Gamma_0(N)$ can be written as a complex constant times an *$\mathbb{Z}_{(p)}$-integral modular unit* — that is, a unit in the ring of regular functions of the smooth model of the modular curve over $\mathbb{Z}_{(p)}$. Then we show that $\mathbb{Z}_{(p)}$-integral modular units have q-expansions in $\mathbb{Z}_{(p)}$ using the algebraic description of the infinity cusp.

The following lemmas provide the reduction from analytic modular units to integral modular units in two steps: first from analytic to rational, then from

rational to integral. The second lemma is established using a similar method to that used in the proof of the q-expansion principle.

Lemma 4.2. *The homomorphism*

$$\mathcal{O}^\times_{Y_0(N)_\mathbb{Q}} \to \mathcal{O}^\times_{Y_0(N)^{\mathrm{an}}}/\mathbb{C}^\times$$

sending a unit on $Y_0(N)_\mathbb{Q}$ to the scalar class of its associated analytic modular unit, is surjective.

Proof. Since the divisor map $\mathrm{div} : \mathcal{O}^\times_{Y_0(N)^{\mathrm{an}}}/\mathbb{C}^\times \to \mathrm{Div}^0(C_0(N))$ is injective, the lemma states that for each analytic unit $u^{\mathrm{an}} \in \mathcal{O}^\times_{Y_0(N)^{\mathrm{an}}}$, there is an algebraic unit $u \in \mathcal{O}^\times_{Y_0(N)_\mathbb{Q}}$ with the same divisor.

Let $u^{\mathrm{an}} \in \mathcal{O}^\times_{Y_0(N)^{\mathrm{an}}}$ and let $D = \mathrm{div}(u^{\mathrm{an}})$ in $\tilde{C}$, and consider the divisor class $\bar{D} \in \mathrm{Pic}(X_0(N)_\mathbb{Q})$ of D. Then $\bar{D}$ is in the kernel of the composite map

$$\mathrm{Pic}(X_0(N)_\mathbb{Q}) \to \mathrm{Pic}(X_0(N)_\mathbb{C}) \to \mathrm{Pic}(X_0(N)^{\mathrm{an}}).$$

The first map is injective by [Sta18, Tag 0CC5], and the second map is injective (in fact, an isomorphism) by GAGA (see [Ray71, Théorème 4.4, pg. 329]). This injectivity implies that $\bar{D} = 0$ in $\mathrm{Pic}(X_0(N)_\mathbb{Q})$, so $D = \mathrm{div}(u)$ for some rational function u on $X_0(N)_\mathbb{Q}$. Since D is supported on the cusps, $u \in \mathcal{O}^\times_{Y_0(N)_\mathbb{Q}}$ as desired. □

Lemma 4.3. *Base change induces an surjection*

$$\mathcal{O}^\times_{Y_0(N)} \to \mathcal{O}^\times_{Y_0(N)_\mathbb{Q}}/\mathbb{Q}^\times.$$

Proof. Let $u \in \mathcal{O}^\times_{Y_0(N)_\mathbb{Q}}$, thought of as a rational function on the arithmetic surface $Y_0(N)$ with zeros and poles along the special fiber $Y_0(N)_{\mathbb{F}_p}$. Choose a closed point $x \in Y_0(N)_{\mathbb{F}_p}$ with residue field k, a finite extension of $\mathbb{F}_p$, and identify the the local ring at x with $W(k)[\![T]\!]$, which is possible because $Y_0(N)$ is smooth. Consider the pullback $\tilde{u}$ of u to $W(k)[\![T]\!]$. Since u is a unit on $Y_0(N)_\mathbb{Q}$, the constant term $\tilde{u}(0)$ of $\tilde{u}$ is non-zero, so we can write $\tilde{u}(0) = p^n\alpha$ for some $n \in \mathbb{Z}$ and $\alpha \in W(k)^\times$. We claim that $p^{-n}u$ is a unit in $\mathcal{O}_{Y_0(N)}$. Indeed, the divisor of $p^{-n}u$ is supported on $Y_0(N)_{\mathbb{F}_p}$ by assumption, and, since $Y_0(N)$ is normal, it must be a union of irreducible codimension 1 subvarieties. Since $Y_0(N)$ is smooth, $Y_0(N)_{\mathbb{F}_p}$ itself is irreducible, so the divisor of $p^{-n}u$ is either empty or all of $Y_0(N)_{\mathbb{F}_p}$. But, by the definition of n, x is not in the divisor of $p^{-n}u$, so the divisor is empty and $p^{-n}u$ is a unit. □

Proposition 4.4. *The q-expansion of every element of $\mathcal{O}^\times_{Y_0(N)}$, thought of as an analytic modular unit, is in $\mathbb{Z}_{(p)}[\![q]\!][q^{-1}]^\times$.*

Proof. The q-expansion of a modular unit is given by pulling back to the infinity cusp. The infinity cusp extends to the integral model as a morphism

$$\infty : \mathrm{Spec}(\mathbb{Z}_{(p)}[\![q]\!][q^{-1}]) \to Y_0(N)$$

of schemes (defined using the Tate elliptic curve). Hence there is a commutative diagram

$$\begin{array}{ccc} \mathcal{O}^\times_{Y_0(N)} & \longrightarrow & \mathbb{Z}_{(p)}[\![q]\!][q^{-1}]^\times \\ \downarrow & & \downarrow \\ \mathcal{O}^\times_{Y_0(N)^{\mathrm{an}}} & \longrightarrow & \mathbb{C}[\![q]\!][q^{-1}]^\times, \end{array}$$

where the horizontal arrows are the q-expansions (that is, pullback along ∞). This commutativity implies that the q-expansion of every element in the image of $\mathcal{O}^\times_{Y_0(N)} \to \mathcal{O}^\times_{Y_0(N)^{\mathrm{an}}}$ belongs to $\mathbb{Z}_{(p)}[\![q]\!][q^{-1}]^\times$. □

4.3. **q-expansions of elements of the period lattice.** We note the effect of the isomorphism $\mathcal{D}$ from (4.1) on q-expansions. Let $u \in \mathcal{O}^\times_{Y_0(N)^{\mathrm{an}}}$ and let $u(q)$ be the q-expansion of u and $\mathcal{D}(u)(q)$ be the q-expansion of $\mathcal{D}(u)$. The chain rule and the fact that $dq = 2\pi i q\, dz$ imply

$$\mathcal{D}(u)(q) = q\frac{u'(q)}{u(q)}, \tag{4.5}$$

where $u'(q) = \frac{d}{dq}u(q)$.

Theorem 4.6. *For each $f \in \mathcal{E}$, the q-expansion of f has coefficients in $\mathbb{Z}_{(p)}$. In other words, $\mathcal{E} \subseteq E_2(N, \mathbb{Z}_{(p)})$.*

Proof. Let $S \subset \mathcal{O}^\times_{Y_0(N)^{\mathrm{an}}}$ be the image of the map $\mathcal{O}^\times_{Y_0(N)} \to \mathcal{O}^\times_{Y_0(N)^{\mathrm{an}}}$ sending an integral modular unit to the associated analytic modular unit. By Lemma 4.2 and Lemma 4.3, the composition $S \to \mathcal{O}^\times_{Y_0(N)^{\mathrm{an}}} \to \mathcal{O}^\times_{Y_0(N)^{\mathrm{an}}}/\mathbb{C}^\times$ is surjective. Then, by Steven's theorem (4.1), $\mathcal{D}(S)$ spans $\mathcal{E}$, so it is enough to show that $\mathcal{D}(S) \subset E_2(N, \mathbb{Z}_{(p)})$.

Let $u \in S$ and write the q-expansion of u as $q^n v$ for some $v \in \mathbb{Z}_{(p)}[\![q]\!]^\times$ and $n \in \mathbb{Z}$. By (4.5), the q-expansion of $\mathcal{D}(u)$ is $n + \frac{qv'}{v}$. Since v' is in $\mathbb{Z}_{(p)}[\![q]\!]$, the q-expansion of $\mathcal{D}(u)$ is in $\mathbb{Z}_{(p)}[\![q]\!]$ and $\mathcal{D}(u) \in E_2(N, \mathbb{Z}_{(p)})$. □

5. The annihilator of the cuspidal subgroup

We established the inclusion $\mathrm{Ann}_{\mathbb{T}}(T) \supseteq I$ in Section 3. To complete the proof of Theorem 1.2. we need to show that C is large in the sense that $\mathrm{Ann}_{\mathbb{T}}(C)$ is contained in I. The following result implies this needed fact.

Proposition 5.1. *There is a subquotient of C whose Pontryagin dual is a free $\mathbb{T}/I$-module of rank 1.*

Proof. For this proof, let $M = M_2(N, \mathbb{Z}_{(p)})$, $S = S_2(N, \mathbb{Z}_{(p)})$, and $E = E_2(N, \mathbb{Z}_{(p)})$. Stevens's isomorphism $\mathcal{D} : U \xrightarrow{\sim} \mathcal{E}$ (4.1) and the inclusion $\mathcal{E} \subset E$ of Theorem 4.6 induce a natural surjection

$$C \cong \tilde{C}/\mathrm{Res}(\mathcal{E}) \twoheadrightarrow \tilde{C}/\mathrm{Res}(E).$$

On the other hand, the residue theorem gives an exact sequence

$$0 \to S \to M \xrightarrow{\mathrm{Res}} \tilde{C},$$

so the residue map induces an injective homomorphism

$$\frac{M}{S+E} \to \frac{\tilde{C}}{\mathrm{Res}(E)}.$$

Note that the residue map is Hecke-equivariant with respect to the action of Hecke operators on $\tilde{C}$ by Picard functoriality (see [Ste82, pg. 36], for example), which induces our chosen action of $\mathbb{T}$ on C. Hence C has a subquotient that is isomorphic to $\frac{M}{S+E}$. Let $X = \frac{M}{S+E}$; it remains to show that the Pontryagin dual $X^\vee$ of X is isomorphic to $\mathbb{T}/I$.

Consider the exact sequence

$$0 \to S \to M/E \to X \to 0. \tag{5.2}$$

By Lemma 2.1(2), there are duality isomorphisms

$$\mathrm{Hom}_{\mathbb{Z}_{(p)}}(S, \mathbb{Z}_{(p)}) \cong \mathbb{T}, \qquad \mathrm{Hom}_{\mathbb{Z}_{(p)}}(M/E, \mathbb{Z}_{(p)}) \cong \tilde{I}.$$

Since M/E is torsion free, $\mathrm{Ext}^1_{\mathbb{Z}_{(p)}}(M/E, \mathbb{Z}_{(p)}) = 0$. Because X is finite, there is are isomorphisms $\mathrm{Hom}_{\mathbb{Z}_{(p)}}(X, \mathbb{Z}_{(p)}) = 0$ and $\mathrm{Ext}^1_{\mathbb{Z}_{(p)}}(X, \mathbb{Z}_{(p)}) \cong X^\vee$. Applying $\mathrm{Hom}_{\mathbb{Z}_{(p)}}(-, \mathbb{Z}_{(p)})$ to (5.2), we obtain an exact sequence

$$0 \to \tilde{I} \to \mathbb{T} \to X^\vee \to 0,$$

so $X^\vee \cong \mathbb{T}/I$. □

The proposition implies that C has a subquotient whose annihilator is I. Since any element of $\mathbb{T}$ that annihilates C will annihilate this subquotient, it follows that $\mathrm{Ann}_{\mathbb{T}}(C) \subseteq I$ and this completes the proof of Theorem 1.2. By Corollary 1.4, C has the same cardinality as its subquotient X. We record some implications of this as a corollary.

Corollary 5.3.

(1) *The period lattice $\mathcal{E}$ coincides with the q-expansion lattice $E_2(N, \mathbb{Z}_{(p)})$.*
(2) *There is an isomorphism of $\mathbb{T}$-modules*

$$\frac{M}{S+E} \to C$$

sending $f \in M$ to the class of $\mathrm{Res}(f)$ in C.
(3) *The Pontryagin dual of C is a cyclic $\mathbb{T}$-module generated by the homomorphism $\lambda : C \to \mathbb{Q}_p/\mathbb{Z}_p$ defined as follows: let $x \in C$, choose $f \in M$ such that $\mathrm{Res}(f) \in \tilde{C}$ represents the class of x, and write $f = ae + bg$ for $a, b \in \mathbb{Q}_p$, $e \in E$, and $g \in S$; then define $\lambda(x) = ba_1(g) \bmod \mathbb{Z}_p$.*

Proof. Continue with the notation as in the proof of Proposition 5.1. Recall that $X = \frac{M}{S+E}$ is Pontriagyn dual to $\mathbb{T}/I$, so there is an equality of cardinalities $|X| = |\mathbb{T}/I|$. The module X is a subquotient of C as follows

$$X \xhookrightarrow{\mathrm{Res}} \tilde{C}/\mathrm{Res}(E) \twoheadleftarrow \tilde{C}/\mathrm{Res}(\mathcal{E}) \xrightarrow{\sim} C. \tag{5.4}$$

Moreover, $|C| = |\mathbb{T}/I|$ by Corollary 1.4. The maps in (5.4) imply a string of inequalities of cardinalities

$$|\mathbb{T}/I| = |X| \leq \left|\tilde{C}/\mathrm{Res}(E)\right| \leq \left|\tilde{C}/\mathrm{Res}(\mathcal{E})\right| = |C| = |\mathbb{T}/I|.$$

Since the beginning and end of the string are equal, all the inequalities are in fact equalities. This implies that all the maps in (5.4) are isomorphisms.

The fact that the surjection $\tilde{C}/\mathrm{Res}(\mathcal{E}) \twoheadrightarrow \tilde{C}/\mathrm{Res}(E)$ is an isomorphism implies $\mathrm{Res}(\mathcal{E}) = \mathrm{Res}(E)$. Since Res is injective on $E_2(N)$, this shows that $E = \mathcal{E}$, proving (1). The map described in (2) is the composition of the isomorphisms in (5.4).

The homomorphism λ defined in (3) is the composition of the isomorphism defined in (2) with the map $\lambda' : X \to \mathbb{Q}_p/\mathbb{Z}_p$ defined by $\lambda'(ae+bg) = ba_1(g) \bmod \mathbb{Z}_p$. By (2), it is enough to show that λ' generates the dual of X. First note that λ' is well defined since $M[1/p] = S[1/p] \oplus E[1/p]$ as $\mathbb{Q}$-vector spaces. The element of $\mathrm{Ext}^1_{\mathbb{Z}_p}(X, \mathbb{Z}_p)$ corresponding to λ' is class of the extension

$$0 \to \mathbb{Z}_p \to Z' \to X \to 0$$

where $Z' = \{(x, \alpha) \in X \times \mathbb{Q}_p \mid \lambda'(x) \equiv \alpha \bmod \mathbb{Z}_p\}$. On the other hand, the proof of Proposition 5.1 shows that $\mathrm{Ext}^1_{\mathbb{Z}_p}(X, \mathbb{Z}_p)$ is a free $\mathbb{T}/I$-module generated by the class of the extension

$$0 \to \mathbb{Z}_p \to Z \to X \to 0$$

where $Z = \dfrac{M/E \oplus \mathbb{Z}_p}{\langle (g, -a_1(g)) \ : \ g \in S \rangle}$. There is a map

$$Z \to Z', \quad (f, \alpha) \mapsto (f, \alpha + ba_1(g))$$

where $f = ae + bg \in M$ with $e \in E$, $g \in S$, $a, b \in \mathbb{Q}_p$, and $\alpha \in \mathbb{Z}_p$. A simple computation shows that this map is an isomorphism of extensions. Hence the class of the extension given by Z' generates $\mathrm{Ext}^1_{\mathbb{Z}_p}(X, \mathbb{Z}_p)$ and λ' generates the dual of X. □

6. Complement: explicit bases of Eisenstein series and modular units

We give explicit bases of $\mathcal{E}$ and U as $\mathbb{Z}_{(p)}$-modules. For $d \mid N$ with $d > 1$, let $h_d \in U$ be the scalar class of $\left(\frac{\eta(dz)}{\eta(z)}\right)^{12N}$, where $\eta(z)$ is the Dekekind eta function. Let $f_d = \mathcal{D}(h_d) \in \mathcal{E}$, and note that

$$f_d(z) = 12N(E_2(dz) - E_2(z)).$$

where $E_2(z)$ is the (non-holomorphic) normalized Eisenstein series of weight 2 and level 1.

Corollary 6.1.

(1) The set $\{f_d \ : \ d > 1, \ d \mid N\}$ is a basis for $E_2(N, \mathbb{Z}_{(p)})$ as a $\mathbb{Z}_{(p)}$-module.
(2) The period lattice $\mathcal{E}$ coincides with the q-expansion lattice $E_2(N, \mathbb{Z}_{(p)})$.
(3) The set $\{h_d \ : \ d > 1, \ d \mid N\}$ is a basis for U as a $\mathbb{Z}_{(p)}$-module.

Proof. Note that (2) has already been proven in Corollary 5.3(1); we give an alternate proof here. Since each f_d is in $\mathcal{E}$, (1) implies that $E_2(N, \mathbb{Z}_{(p)}) \subseteq \mathcal{E}$. Together with Theorem 4.6, this inclusion implies (2). Since $f_d = \mathcal{D}(h_d)$ and $\mathcal{D}$ is an isomorphism, (1) and (2) imply (3).

It remains to prove (1). Let $E' \subseteq E_2(N, \mathbb{Z}_{(p)})$ be the $\mathbb{Z}_{(p)}$-submodule generated by $\{f_d \mid d > 1, \ d \mid N\}$. Since the set $\{f_d \mid d > 1, \ d \mid N\}$ is a $\mathbb{Q}$-basis for $E_2(N, \mathbb{Q})$ (see [DS05, Theorem 4.6.2, pg. 133], for example), the index of E' in $E_2(N, \mathbb{Z}_{(p)})$ is finite. To show this index is 1, it is enough to show that the restriction map

$$\mathrm{Hom}_{\mathbb{Z}_{(p)}}(E_2(N, \mathbb{Z}_{(p)}), \mathbb{Z}_{(p)}) \to \mathrm{Hom}_{\mathbb{Z}_{(p)}}(E', \mathbb{Z}_{(p)}) \tag{6.2}$$

is surjective.

For any divisor $d \mid N$, define a functional $l_d : E_2(N, \mathbb{Z}_{(p)}) \to \mathbb{Z}_{(p)}$ by

$$l_d(f) = \sum_{t|d} \mu(d/t)\sigma_{d/t}a_t(f). \tag{6.3}$$

where μ is the Möbius function and σ is the divisor-sum function. In terms of the duality pairing of Lemma 2.1, l_d corresponds to the Hecke operator

$$t_d := \prod_{\{\ell|N:\ell \text{ prime}\}} (U_\ell - \ell - 1),$$

in that $l_d(f) = a_1(t_d f)$. Now let $d, s \mid N$ with $d, s > 1$. An elementary computation, either directly using (6.3) or by computing the action of t_d on f_s, shows

$$l_d(f_s) = \begin{cases} -12Nd & s = d \\ 0 & s \neq d. \end{cases}$$

Since $-12Nd \in \mathbb{Z}_{(p)}^\times$, the elements ℓ_d generate $\mathrm{Hom}_{\mathbb{Z}_{(p)}}(E', \mathbb{Z}_{(p)})$ and the map (6.2) is surjective. □

Corollary 6.1(3) was first proven by Takagi [Tak97, Theorem 4.1] using Kubert–Lang theory.

References

[Aga18] Amod Agashe. Rational torsion in elliptic curves and the cuspidal subgroup. *J. Théor. Nombres Bordeaux*, 30(1):81–91, 2018.

[CE98] Robert F. Coleman and Bas Edixhoven. On the semi-simplicity of the U_p-operator on modular forms. *Math. Ann.*, 310(1):119–127, 1998.

[CES03] Brian Conrad, Bas Edixhoven, and William Stein. $J_1(p)$ has connected fibers. *Doc. Math.*, 8:331–408, 2003.

[DDT97] Henri Darmon, Fred Diamond, and Richard Taylor. Fermat's last theorem. In *Elliptic curves, modular forms & Fermat's last theorem (Hong Kong, 1993)*, pages 2–140. Int. Press, Cambridge, MA, 1997.

[DS05] Fred Diamond and Jerry Shurman. *A first course in modular forms*, volume 228 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2005.

[Edi92] Bas Edixhoven. The weight in Serre's conjectures on modular forms. *Invent. Math.*, 109(3):563–594, 1992.

[Gro71] Alexander Grothendieck. *Revêtements étales et groupe fondamental (SGA 1)*, volume 224 of *Lecture notes in mathematics*. Springer-Verlag, 1971.

[JRS22] Bruce W. Jordan, Kenneth A. Ribet, and Anthony J. Scholl. Modular curves and Néron models of generalized Jacobians. Preprint, arXiv:2207.13203, 2022.

[Kat77] Nicholas M. Katz. A result on modular forms in characteristic p. In *Modular functions of one variable, V (Proc. Second Internat. Conf., Univ. Bonn, Bonn, 1976)*, Lecture Notes in Math., Vol. 601, pages 53–61. Springer, Berlin, 1977.

[Kat81] Nicholas M. Katz. Galois properties of torsion points on abelian varieties. *Invent. Math.*, 62(3):481–502, 1981.

[KL81] Daniel S. Kubert and Serge Lang. *Modular units*, volume 244 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, New York-Berlin, 1981.

[Lor95] Dino J. Lorenzini. Torsion points on the modular Jacobian $J_0(N)$. *Compositio Math.*, 96(2):149–172, 1995.

[Lui19] Kevin Lui. *Arithmetic of Totally Split Modular Jacobians and Enumeration of Isogeny Classes of Prime Level Simple Modular Abelian Varieties*. ProQuest LLC, Ann Arbor, MI, 2019. Thesis (Ph.D.)–University of Washington.

[Maz77] B. Mazur. Modular curves and the Eisenstein ideal. *Inst. Hautes Études Sci. Publ. Math.*, (47):33–186 (1978), 1977.

[Ogg73] A. P. Ogg. Rational points on certain elliptic modular curves. In *Analytic number theory (Proc. Sympos. Pure Math., Vol XXIV, St. Louis Univ., St. Louis, Mo., 1972)*, pages 221–231, 1973.

[Ogg75] A. P. Ogg. Diophantine equations and modular forms. *Bull. Amer. Math. Soc.*, 81:14–27, 1975.

[Oht13] Masami Ohta. Eisenstein ideals and the rational torsion subgroups of modular Jacobian varieties. *J. Math. Soc. Japan*, 65(3):733–772, 2013.

[Oht14] Masami Ohta. Eisenstein ideals and the rational torsion subgroups of modular Jacobian varieties II. *Tokyo J. Math.*, 37(2):273–318, 2014.

[Ray71] Michèle Raynaud. Géométrie algébrique et géométrie analytique. 1971. Exposé XII in [Gro71].

[Ren18] Yuan Ren. Rational torsion subgroups of modular Jacobian varieties. *J. Number Theory*, 190:169–186, 2018.

[Rib83] Kenneth A. Ribet. Mod p Hecke operators and congruences between modular forms. *Invent. Math.*, 71(1):193–205, 1983.

[Rib90] K. A. Ribet. On modular representations of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ arising from modular forms. *Invent. Math.*, 100(2):431–476, 1990.

[Shi71] Goro Shimura. *Introduction to the arithmetic theory of automorphic functions*. Publications of the Mathematical Society of Japan, No. 11. Iwanami Shoten, Publishers, Tokyo; Princeton University Press, Princeton, N.J., 1971. Kanô Memorial Lectures, No. 1.

[Sta18] Stacks Project Authors. *Stacks Project*. https://stacks.math.columbia.edu, 2018.

[Ste82] Glenn Stevens. *Arithmetic on modular curves*, volume 20 of *Progress in Mathematics*. Birkhäuser Boston, Inc., Boston, MA, 1982.

[Ste85] Glenn Stevens. The cuspidal group and special values of L-functions. *Trans. Amer. Math. Soc.*, 291(2):519–550, 1985.

[Tak97] Toshikazu Takagi. The cuspidal class number formula for the modular curves $X_0(M)$ with M square-free. *J. Algebra*, 193(1):180–213, 1997.

[Wil80] Andrew Wiles. Modular curves and the class group of $\mathbf{Q}(\zeta_p)$. *Invent. Math.*, 58(1):1–35, 1980.

[Yoo16] Hwajong Yoo. Rational torsion points on Jacobians of modular curves. *Acta Arith.*, 172(4):299–304, 2016.

[Yoo19] Hwajong Yoo. Non-optimal levels of a reducible mod ℓ modular representation. *Trans. Amer. Math. Soc.*, 371(6):3805–3830, 2019.