PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 146, Number 8, August 2018, Pages 3307–3320
http://dx.doi.org/10.1090/proc/14019
Article electronically published on February 28, 2018

ON RIBET'S ISOGENY FOR $J_0(65)$

KRZYSZTOF KLOSIN AND MIHRAN PAPIKIAN

(Communicated by Matthew A. Papanikolas)

Abstract. Let J^{65} be the Jacobian of the Shimura curve attached to the indefinite quaternion algebra over $\mathbb{Q}$ of discriminant 65. We study the isogenies $J_0(65) \to J^{65}$ defined over $\mathbb{Q}$, whose existence was proved by Ribet. We prove that there is an isogeny whose kernel is supported on the Eisenstein maximal ideals of the Hecke algebra acting on $J_0(65)$, and, moreover, the odd part of the kernel is generated by a cuspidal divisor of order 7, as is predicted by a conjecture of Ogg.

1. Introduction

Let N be a product of an even number of distinct primes. Let $J_0(N)$ be the Jacobian of the modular curve $X_0(N)$. In [20], Ribet proved the existence of an isogeny defined over $\mathbb{Q}$ between the "new" part $J_0(N)^{\mathrm{new}}$ of $J_0(N)$ and the Jacobian J^N of the Shimura curve X^N attached to a maximal order in the indefinite quaternion algebra over $\mathbb{Q}$ of discriminant N. Although there are no morphisms $X_0(N) \to X^N$ defined over $\mathbb{Q}$, Ribet showed that the $\mathbb{Q}_\ell$-adic Tate modules of $J_0(N)^{\mathrm{new}}$ and J^N are isomorphic as $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-modules, where ℓ is an arbitrary prime number; this is a consequence of a correspondence between automorphic forms on GL(2) and automorphic forms on the multiplicative group of a quaternion algebra. The existence of the isogeny $J_0(N)^{\mathrm{new}} \to J^N$ defined over $\mathbb{Q}$ then follows from a special case of Tate's isogeny conjecture for abelian varieties over number fields, also proved in [20] (the general case of Tate's conjecture was proved a few years later by Faltings). Unfortunately, Ribet's argument provides no information about the isogenies $J_0(N)^{\mathrm{new}} \to J^N$ beyond their existence.

In [16], Ogg made an explicit conjecture about the kernel of Ribet's isogeny when $N = pq$ is a product of two distinct primes and $p = 2, 3, 5, 7, 13$: the conjecture predicts that there is an isogeny $J_0(N)^{\mathrm{new}} \to J^N$ of minimal degree whose kernel is a specific group arising from the cuspidal divisor subgroup of $J_0(N)$. Note that $p = 2, 3, 5, 7, 13$ are exactly the primes for which $J_0(pq)$ has purely toric reduction at q. This fact is crucial for the calculations used by Ogg to come up with his conjecture; the underlying idea is that the knowledge of the group of connected

Received by the editors July 19, 2017, and, in revised form, November 13, 2017.

2010 *Mathematics Subject Classification.* Primary 11G18.

Key words and phrases. Modular curves, Ribet's isogeny, Eisenstein ideal, cuspidal divisor group.

The first author was supported by the Young Investigator Grant #H98230-16-1-0129 from the National Security Agency, and by a PSC-CUNY award jointly funded by the Professional Staff Congress and the City University of New York.

The second author was partially supported by grants from the Simons Foundation (245676) and the National Security Agency (H98230-15-1-0008).

components of the Néron models of $J_0(N)^{\mathrm{new}}$ and J^N at q yields restrictions on the isogenies between them. Ogg's conjecture remains open except for the special cases when J^N has dimension ≤ 3.

When $\dim(J^N) = 1$, equiv. $N = 2\cdot 7,\ 3\cdot 5,\ 3\cdot 7,\ 3\cdot 11,\ 2\cdot 17$, J^N is an elliptic curve over $\mathbb{Q}$ which is uniquely determined by its component groups at p and q, and $J_0(N)^{\mathrm{new}}$ is the optimal elliptic curve of conductor N. Then one easily checks Ogg's conjecture using Cremona's tables [5]. In general, the orders of component groups of J^N can be computed using Brandt matrices [10], which is relatively easy to do with the help of a computer program such as `Magma`.

When $\dim(J^N) = 2$, equiv. $N = 2\cdot 13,\ 2\cdot 19,\ 2\cdot 29$, Ogg's conjecture is verified in [7]. In this case, the proof is based on the fact that X^N is bielliptic and the lattices of $J_0(N)^{\mathrm{new}}$ and J^N can be computed through their elliptic quotients.

When $\dim(J^N) = 3$, equiv. $N = 2\cdot 31,\ 2\cdot 41,\ 2\cdot 47,\ 3\cdot 13,\ 3\cdot 17,\ 3\cdot 19,\ 3\cdot 23,\ 5\cdot 7,\ 5\cdot 11$, Ogg's conjecture is verified in [6]. In this case, X^N is always hyperelliptic. By utilizing this fact, González and Molina explicitly compute the equation for each X^N. Then they obtain a basis of regular differentials for X^N from these equations to produce a period matrix for J^N. The period matrix of $J_0(N)^{\mathrm{new}}$ can be computed using cusp forms with rational q-expansions. The problem then reduces to comparing the period matrices of appropriate quotients of $J_0(N)^{\mathrm{new}}$ with the period matrix of J^N.

The goal of this paper is to study Ribet's isogeny for $N = 5\cdot 13 = 65$. In this case, $\dim(J^N) = 5$ and X^N is *not* hyperelliptic; cf. [14]. Our approach to the study of Ribet isogenies is completely different from that in [7] and [6], and crucially relies on the Hecke equivariance of such isogenies. In this approach we need to know very little about X^N or J^N; we only need to know the orders of component groups of J^N, which, as we mentioned, are easy to compute, and in fact were already computed in [16]. The difficulty shifts to the study of the structure of the Hecke algebra and its action on $J_0(N)$.

Let $\mathbb{T}(N) := \mathbb{Z}[T_2, T_3, \dots]$ be the $\mathbb{Z}$-algebra generated by the Hecke operators T_n acting on be the space $S_2(N)$ of weight 2 cups forms on $\Gamma_0(N)$. This algebra is isomorphic to the subalgebra of $\mathrm{End}(J_0(N))$ generated by T_n acting as correspondences on $X_0(N)$. When $N = 65$, we have $J_0(N)^{\mathrm{new}} = J_0(N)$, so there is a Ribet isogeny

$$\pi : J_0(N) \to J^N.$$

$\mathbb{T}(N)$ also naturally acts on J^N and π is $\mathbb{T}(N)$-equivariant. This equivariance is implicit in Ribet's proof [20]; see also [9, Cor. 2.4].

From now on we assume $N = 65$. To simplify the notation, we denote $\mathbb{T} := \mathbb{T}(N)$, $J := J_0(N)$, $J' := J^N$, $G_{\mathbb{Q}} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Given a finite abelian group H, we denote by H_p its p-primary component (p is a prime number), and by H_{odd} its maximal subgroup of odd order, so that $H \cong H_2 \times H_{\mathrm{odd}}$. Since the endomorphisms of J induced by Hecke operators are defined over $\mathbb{Q}$, the actions of $\mathbb{T}$ and $G_{\mathbb{Q}}$ on J commute with each other. Thus, $\ker(\pi)$ is a $\mathbb{T}[G_{\mathbb{Q}}]$-submodule of J. We show that if the kernel of an isogeny from J to another abelian variety is a $\mathbb{T}[G_{\mathbb{Q}}]$-module, then, up to endomorphisms of J, the kernel is supported on the Eisenstein maximal ideals of $\mathbb{T}$. We then classify all $\mathbb{T}[G_{\mathbb{Q}}]$-submodules of J of odd order supported on the Eisenstein maximal ideals. This leads to the following theorem, which is the main result of the paper.

Theorem 1.1. *There is a Ribet isogeny* $\pi : J \to J'$ *such that* $\ker(\pi)_{\mathrm{odd}} \cong \mathbb{Z}/7\mathbb{Z}$ *is the* 7*-primary component of the cuspidal divisor group of* J*.*

Ogg's conjecture in this case predicts that in fact $\ker(\pi) = \mathbb{Z}/7\mathbb{Z}$. There is a unique Eisenstein maximal ideal $\mathfrak{m}_2 \lhd \mathbb{T}$ of residue characteristic 2. In principle, it should be possible to extend our analysis to finite $\mathbb{T}[G_{\mathbb{Q}}]$-submodules of J supported on $\mathfrak{m}_2$ to show that $\ker(\pi)_2 = 0$. But there are several technical difficulties which at present we are not able to overcome: these stem from the fact that $\mathfrak{m}_2$ is a prime of fusion, $\mathbb{T}_{\mathfrak{m}_2}$ is not Gorenstein, and the groups of rational points of reductions of J usually have large 2-primary components.

Our strategy can be applied also to cases when $\dim(J^N) = 3$, which leads to results similar to Theorem 1.1, at least when $J_0(N)^{\mathrm{new}} = J_0(N)$ (equiv. $N = 3 \cdot 13, 5 \cdot 7$); see Remarks 4.9 and 4.10.

Remark 1.2. Given a prime ℓ, if $H := (J_0(N)^{\mathrm{new}}(\mathbb{Q})_{\mathrm{tor}})_\ell \neq 0$ but $(J^N(\mathbb{Q})_{\mathrm{tor}})_\ell = 0$, then obviously $H \subset \ker(\pi)$ for any Ribet isogeny $\pi : J_0(N)^{\mathrm{new}} \to J^N$. For an odd prime ℓ, in [24], Yoo gives sufficient conditions for the non-existence of rational points of order ℓ on J^N, when $N = pq$ is a product of two distinct primes. This then can be used to find non-trivial subgroups of the kernels of Ribet isogenies; see [24, Thm. 1.3]. In the case when $N = 65$, Yoo's theorem implies that $\mathbb{Z}/7\mathbb{Z} \subset \ker(\pi)$.

2. Néron models

In this section we recall some terminology and facts from the theory of Néron models. Let R be a complete discrete valuation ring, with fraction field K and residue field k. Let A be an abelian variety over K. Denote by $\mathcal{A}$ its Néron model over R and denote by $\mathcal{A}_k^0$ the connected component of the identity of the special fiber $\mathcal{A}_k$ of A. There is an exact sequence

$$0 \to \mathcal{A}_k^0 \to \mathcal{A}_k \to \Phi_A \to 0,$$

where Φ_A is a finite (abelian) group called the *component group of* A. We say that A has *semi-abelian reduction* if $\mathcal{A}_k^0$ is an extension of an abelian variety A'_k by an affine algebraic torus T_A over k (cf. [1, p. 181]):

$$0 \to T_A \to \mathcal{A}_k^0 \to A'_k \to 0.$$

We say that A has *good reduction*, if $\mathcal{A}_k^0 = A'_k$ (in this case, we also have $\mathcal{A}_k = \mathcal{A}_k^0$); we say that A has (purely) *toric reduction* if $\mathcal{A}_k^0 = T_A$. The *character group*

$$M_A := \mathrm{Hom}((T_A)_{\bar{k}}, \mathbb{G}_{m,\bar{k}}) \tag{2.1}$$

is a free abelian group contravariantly associated to A.

Let K' be a finite unramified extension of K, with ring of integers R' and residue field k'. By the fundamental property of Néron models, we have an isomorphism of groups $A(K') \cong \mathcal{A}(R')$, which defines a canonical reduction map

$$A(K') \to \mathcal{A}_k(k'). \tag{2.2}$$

Composing (2.2) with $\mathcal{A}_k \to \Phi_A$, we get a homomorphism

$$A(K') \to \Phi_A. \tag{2.3}$$

Proposition 2.1. *Let K' be a finite unramified extension of K. Let $H \subset A(K')$ be a finite subgroup. Assume that either $\#H$ is coprime to the characteristic p of k, or that K has characteristic 0 and its absolute ramification index is $< p-1$. Then (2.2) defines an injection $H \hookrightarrow \mathcal{A}_k(k')$.*

Proof. See [11, p. 502] and [1, Prop. 7.3/3]. $\square$

Let $\varphi : A \to B$ be an isogeny defined over K. By the Néron mapping property, φ extends to a morphism $\varphi : \mathcal{A} \to \mathcal{B}$ of the Néron models. On the special fibers we get a homomorphism $\varphi_k : \mathcal{A}_k \to \mathcal{B}_k$, which induces an isogeny $\varphi_k^0 : \mathcal{A}_k^0 \to \mathcal{B}_k^0$; [1, Cor. 7.3/7]. This implies that B has semi-abelian (resp. toric) reduction if A has semi-abelian (resp. toric) reduction. The isogeny φ_k^0 restricts to an isogeny $\varphi_t : T_A \to T_B$, which corresponds to an injective homomorphism of character groups $\varphi^* : M_B \to M_A$ with finite cokernel. We also get a natural homomorphism $\varphi_\Phi : \Phi_A \to \Phi_B$.

Denote by $\hat{A}$ the dual abelian variety of A. Let $\hat{\varphi} : \hat{B} \to \hat{A}$ be the isogeny dual to φ. Assume A has semi-abelian reduction. In [8], Grothendieck defined a non-degenerate pairing $u_A : M_A \times M_{\hat{A}} \to \mathbb{Z}$ (called *monodromy pairing*) with nice functorial properties, which induces an exact sequence

$$0 \to M_{\hat{A}} \xrightarrow{u_A} \mathrm{Hom}(M_A, \mathbb{Z}) \to \Phi_A \to 0. \tag{2.4}$$

Using (2.4), one obtains a commutative diagram with exact rows (cf. [21, p. 8]):

$$\begin{tikzcd}
0 \arrow[r] & M_{\hat{A}} \arrow[r] \arrow[d, "\hat{\varphi}^*"] & \mathrm{Hom}(M_A, \mathbb{Z}) \arrow[r] \arrow[d, "\mathrm{Hom}(\varphi^*, \mathbb{Z})"] & \Phi_A \arrow[r] \arrow[d, "\varphi_\Phi"] & 0 \\
0 \arrow[r] & M_{\hat{B}} \arrow[r] & \mathrm{Hom}(M_B, \mathbb{Z}) \arrow[r] & \Phi_B \arrow[r] & 0.
\end{tikzcd}$$

From this diagram we get the exact sequence

$$0 \to \ker(\varphi_\Phi) \to M_{\hat{B}}/\hat{\varphi}^*(M_{\hat{A}}) \to \mathrm{Ext}^1_{\mathbb{Z}}(M_A/\varphi^*(M_B), \mathbb{Z}) \to \mathrm{coker}(\varphi_\Phi) \to 0. \tag{2.5}$$

Since

$$\mathrm{Ext}^1_{\mathbb{Z}}(M_A/\varphi^*(M_B), \mathbb{Z}) \cong \mathrm{Hom}(M_A/\varphi^*(M_B), \mathbb{Q}/\mathbb{Z}) =: (M_A/\varphi^*(M_B))^\vee,$$

we can rewrite (2.5) as

$$0 \to \ker(\varphi_\Phi) \to M_{\hat{B}}/\hat{\varphi}^*(M_{\hat{A}}) \to (M_A/\varphi^*(M_B))^\vee \to \mathrm{coker}(\varphi_\Phi) \to 0. \tag{2.6}$$

Note that $M_A/\varphi^*(M_B) \cong \mathrm{Hom}(\ker(\varphi_t), \mathbb{G}_{m,k})$. On the other hand, $\ker(\varphi_t)$ can be canonically identified with a subgroup scheme of $H := \ker(\varphi)$; cf. [3, p. 762]. Therefore, $\#M_A/\varphi^*(M_B)$ divides $\#H$. Similarly, $\#M_{\hat{B}}/\hat{\varphi}^*(M_{\hat{A}})$ divides $\#\ker(\hat{\varphi})$. Since $\ker(\hat{\varphi}) \cong \mathrm{Hom}(\ker(\phi), \mathbb{G}_{m,K})$ (see [15, Thm.1, p. 143]), we conclude that $\#M_{\hat{B}}/\hat{\varphi}^*(M_{\hat{A}})$ also divides $\#H$. Now one easily deduces from (2.6) the following:

Lemma 2.2. *Assume A has semi-abelian reduction, and $\varphi : A \to B$ is an isogeny defined over K. If ℓ is a prime number which does not divide $\#\ker(\varphi)$, then φ_Φ induces an isomorphism $(\Phi_A)_\ell \cong (\Phi_B)_\ell$.*

Lemma 2.3. *Let K' be a finite unramified extension of K. Let $\varphi : A \to B$ be an isogeny defined over K such that $H = \ker(\varphi) \subset A(K')$, i.e., H becomes a constant group-scheme over K'. Let H_0 (resp. H_1) be the kernel (resp. image) of the homomorphism $H \to \Phi_A$ defined by (2.3). Assume A has toric reduction. Assume* *that either $\#H$ is coprime to the characteristic p of k, or that K has characteristic 0 and its absolute ramification index is $< p-1$. Then there is an exact sequence*

$$0 \to H_1 \to \Phi_A \xrightarrow{\varphi_\Phi} \Phi_B \to H_0 \to 0.$$

Proof. Under these assumptions, we have $H \hookrightarrow \mathcal{A}_k(k')$ and $H_0 = \ker(\varphi_t)$. This implies $(M_A/\varphi^*(M_B))^\vee \cong H_0$. Next, [3, Thm. 8.6] implies that $M_{\hat{B}}/\hat{\varphi}^*(M_{\hat{A}}) \cong H_1$. Thus, we can rewrite (2.6) as

$$0 \to \ker(\varphi_\Phi) \to H_1 \to H_0 \to \operatorname{coker}(\varphi_\Phi) \to 0.$$

Since $\ker(\varphi_\Phi) = H_1$, we conclude from this exact sequence that $\operatorname{coker}(\varphi_\Phi) \cong H_0$. □

3. Hecke algebra

Since the $\mathbb{Z}$-algebra $\mathbb{T}$ is free of finite rank as a $\mathbb{Z}$-module, we can define the discriminant $\operatorname{disc}(\mathbb{T})$ of $\mathbb{T}$ with respect to the trace pairing; cf. [19, p. 66]. An algorithm for computing the discriminants of Hecke algebras is implemented in `Magma`; it gives $\operatorname{disc}(\mathbb{T}) = 2^{11} \cdot 3$. We then obtain

$$\mathbb{T} = \mathbb{Z}T_1 + \mathbb{Z}T_2 + \mathbb{Z}T_3 + \mathbb{Z}T_5 + \mathbb{Z}T_{11}$$

as a free $\mathbb{Z}$-module by comparing the discriminants. We have $\mathbb{T} \otimes_{\mathbb{Z}} \mathbb{Q} \cong \mathbb{Q} \times \mathbb{Q}(\sqrt{2}) \times \mathbb{Q}(\sqrt{3})$. Let

$$\widetilde{\mathbb{T}} = \mathbb{Z} \times \mathbb{Z}[\sqrt{2}] \times \mathbb{Z}[\sqrt{3}]$$

be the integral closure of $\mathbb{T}$ in $\mathbb{T} \otimes \mathbb{Q}$. Viewing $\mathbb{T}$ as an order in $\widetilde{\mathbb{T}}$, we have

$$\begin{aligned} T_1 &= (1,1,1), \\ T_2 &= (-1,-1+\sqrt{2},\sqrt{3}), \\ T_3 &= (-2,\sqrt{2},1-\sqrt{3}), \\ T_5 &= (-1,1,-1), \\ T_{11} &= (2,2-\sqrt{2},-3+\sqrt{3}). \end{aligned} \tag{3.1}$$

One then observes that $\mathbb{T} = \mathbb{Z}v_1 + \mathbb{Z}v_2 + \mathbb{Z}v_3 + \mathbb{Z}v_4 + \mathbb{Z}v_5$, where

$$v_1 = (1,1,1), \quad v_2 = (0,2,0), \quad v_3 = (0,0,2), \quad v_4 = (0,2\sqrt{2},0),$$

$$v_5 = (-1,-1+\sqrt{2},2-\sqrt{3}),$$

which implies

$$\mathbb{T} \cong \left\{ (a, b_1 + b_2\sqrt{2}, c_1 + c_2\sqrt{3}) \;\middle|\; \begin{array}{c} a, b_1, b_2, c_1, c_2 \in \mathbb{Z}, \\ a \equiv b_1 \equiv (c_1 + c_2) \bmod 2, \\ b_2 \equiv c_2 \bmod 2 \end{array} \right\}. \tag{3.2}$$

Given a maximal ideal $\mathfrak{m} \lhd \mathbb{T}$, let $\mathbb{T}_\mathfrak{m} = \varprojlim_n \mathbb{T}/\mathfrak{m}^n$ denote the completion of $\mathbb{T}$ at $\mathfrak{m}$.

Proposition 3.1. *Every maximal ideal in $\mathbb{T}$ of odd residue characteristic is principal. In particular, $\mathbb{T}_\mathfrak{m}$ is Gorenstein for any maximal ideal $\mathfrak{m} \lhd \mathbb{T}$ of odd residue characteristic; cf.* [23, p. 329].

Proof. Since
$$\mathrm{disc}(\mathbb{T}) = [\widetilde{\mathbb{T}} : \mathbb{T}]^2 \cdot \mathrm{disc}(\widetilde{\mathbb{T}}) = [\widetilde{\mathbb{T}} : \mathbb{T}]^2 \cdot 2^5 \cdot 3,$$
we get $[\widetilde{\mathbb{T}} : \mathbb{T}] = 2^3$. Let $I_{\widetilde{\mathbb{T}},2'}$ be the set of ideals $I \lhd \widetilde{\mathbb{T}}$ such that $\widetilde{\mathbb{T}}/I$ is a finite ring of odd order. Let $I_{\mathbb{T},2'}$ be the set of ideals $I \lhd \mathbb{T}$ such that $\mathbb{T}/I$ is a finite ring of odd order. The argument of the proof of Proposition 7.20 in [4] shows that the map $I \mapsto I \cap \mathbb{T}$ gives a bijection from $I_{\widetilde{\mathbb{T}},2'}$ to $I_{\mathbb{T},2'}$, with the inverse given by $I \mapsto I\widetilde{\mathbb{T}}$. Moreover, the proof of that proposition shows that for $I \in I_{\widetilde{\mathbb{T}},2'}$ we have $\widetilde{\mathbb{T}}/I \cong \mathbb{T}/I \cap \mathbb{T}$, so that this bijection restricts to a bijection between the maximal ideals of $\widetilde{\mathbb{T}}$ and $\mathbb{T}$ of odd residue characteristic.

Since $\widetilde{\mathbb{T}}$ is a direct product of Euclidean domains, every ideal $I \in I_{\widetilde{\mathbb{T}},2'}$ is principal. Write $I = \theta\widetilde{\mathbb{T}}$. If $\theta \in \mathbb{T}$, then $I \cap \mathbb{T} = \theta\mathbb{T}$ is also principal, since $(\theta\mathbb{T})\widetilde{\mathbb{T}} = \theta\widetilde{\mathbb{T}}$. Therefore, to prove the proposition it is enough to show that for every maximal ideal $\mathfrak{m} \in I_{\widetilde{\mathbb{T}},2'}$ we can choose a generator which lies in $\mathbb{T}$. Let $p > 2$ be the residue characteristic of $\mathfrak{m} = \theta\widetilde{\mathbb{T}}$. If we write $\mathfrak{m} = \mathfrak{m}' \times \mathfrak{m}'' \times \mathfrak{m}'''$, where $\mathfrak{m}' \lhd \mathbb{Z}$, $\mathfrak{m}'' \lhd \mathbb{Z}[\sqrt{2}]$, $\mathfrak{m}''' \lhd \mathbb{Z}[\sqrt{3}]$, then one of these ideals is maximal of residue characteristic p, and the other two are equal to the corresponding ring. We consider three cases depending on which of the three ideals is proper.

Case 1: $\mathfrak{m}' = p\mathbb{Z}$. Then $\theta = (p, 1, 1) \in \mathbb{T}$.

Case 2: $\mathfrak{m}''$ is proper. If (p) is inert in $\mathbb{Z}[\sqrt{2}]$, then we can take $\theta = (1, p, 1) \in \mathbb{T}$. Now suppose $p = (\alpha + \beta\sqrt{2})(\alpha - \beta\sqrt{2})$ splits, where $\alpha, \beta \in \mathbb{Z}$. Note that α must be odd. If β is even, then $\theta = (1, \alpha \pm \beta\sqrt{2}, 1) \in \mathbb{T}$. If β is odd, then $\theta = (1, \alpha \pm \beta\sqrt{2}, 2 + \sqrt{3}) \in \mathbb{T}$, as $2 + \sqrt{3}$ is a unit in $\mathbb{Z}[\sqrt{3}]$.

Case 3: $\mathfrak{m}'''$ is proper. If (p) is inert in $\mathbb{Z}[\sqrt{3}]$, then we can take $\theta = (1, 1, p) \in \mathbb{T}$. If $p = 3$, then $\theta = (1, 1 + \sqrt{2}, \sqrt{3}) \in \mathbb{T}$, since $1 + \sqrt{2}$ is a unit in $\mathbb{Z}[\sqrt{2}]$. Finally, suppose $p = (\alpha + \beta\sqrt{3})(\alpha - \beta\sqrt{3})$, where $\alpha, \beta \in \mathbb{Z}$. Considering $p = \alpha^2 - 3\beta^2$ modulo 2, we get $1 \equiv (\alpha + \beta)^2 \bmod 2$, so that α and β have different parity. If α is odd and β is even, then $\theta = (1, 1, \alpha \pm \beta\sqrt{3}) \in \mathbb{T}$. If α is even and β is odd, then $\theta = (1, 1 + \sqrt{2}, \alpha \pm \beta\sqrt{3}) \in \mathbb{T}$.

$\square$

Remark 3.2. Let $\mathcal{O} = \mathbb{Z}[i]$ be the Gaussian integers. Let $\mathcal{O}' = \mathbb{Z} + 3\mathcal{O} = \mathbb{Z} + 3i\mathbb{Z}$ be an order in $\mathcal{O}$. We have $[\mathcal{O} : \mathcal{O}'] = 3$. The ideal $\mathfrak{m} = (2 + i)\mathcal{O}$ is maximal and $\mathcal{O}/\mathfrak{m} \cong \mathbb{F}_5$. On the other hand, $\mathfrak{m} \cap \mathcal{O}' = (5, 1 + 3i)\mathcal{O}'$ is not principal, although $(5, 1 + 3i)\mathcal{O} = \mathfrak{m}$. This indicates that Proposition 3.1 is not a special case of a general fact about orders.

Definition 3.3. The *Eisenstein ideal* of $\mathbb{T}$ is the ideal $\mathcal{E} \lhd \mathbb{T}$ generated by $T_\ell - (\ell + 1)$ for all primes $\ell \nmid 65$. A maximal ideal $\mathfrak{m} \lhd \mathbb{T}$ in the support of the Eisenstein ideal is called an *Eisenstein maximal ideal*.

Proposition 3.4. *We have*
$$\mathbb{T}/\mathcal{E} \cong \mathbb{Z}/84\mathbb{Z} \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}.$$

Proof. First, we explain how to compute the expansion of an arbitrary Hecke operator $T_m \in \mathbb{T}$ in terms of the $\mathbb{Z}$-basis $\{T_1, T_2, T_3, T_5, T_{11}\}$ of $\mathbb{T}$. Up to Galois conjugacy, there are three normalized $\mathbb{T}$-eigenforms in $S_2(65)$. The three coordinates of T_m in the ring on the right-hand side of (3.2) are the eigenvalues with which T_m acts on these eigenforms. Once we have this representation of T_m, thanks to (3.1), finding the expansion of T_m in terms of our basis amounts to solving a system of five linear equations in five variables. This strategy yields

$$\begin{aligned} T_7 &= 2T_1 - T_2 - 6T_3 + 9T_5 - 5T_{11}, \\ T_{19} &= 2T_1 + 2T_2 - 4T_3 + 8T_5 - 3T_{11}, \\ T_{29} &= -4T_1 + T_2 + 12T_3 - 13T_5 + 9T_{11}. \end{aligned}$$

The Hecke operators T_ℓ for primes $\ell \nmid 65$ are all congruent to integers modulo $\mathcal{E}$. Since $T_5 = (T_7 - T_{19}) + 3T_2 + 2T_3 + 2T_{11}$, we conclude that all Hecke operators are congruent to integers. Hence the natural map $\mathbb{Z} \to \mathbb{T}/\mathcal{E}$ is surjective. We cannot have $\mathbb{T}/\mathcal{E} = \mathbb{Z}$, for then there would exist a cusp form $f \in S_2(65)$ such that $T_\ell f = (\ell+1)f$, which would contradict the Ramanujan-Petersson bound. Therefore, $\mathbb{T}/\mathcal{E} \cong \mathbb{Z}/n\mathbb{Z}$ for some integer n. Note that $T_5 \equiv 29 \pmod{\mathcal{E}}$. From the expansion of T_7, we obtain $168 = 2^3 \cdot 3 \cdot 7 \equiv 0 \pmod{\mathcal{E}}$; from the expansion of T_{29}, we obtain $252 = 2^2 \cdot 3^2 \cdot 7 \equiv 0 \pmod{\mathcal{E}}$; thus, n divides $4 \cdot 3 \cdot 7 = 84$. On the other hand, the Eichler-Shimura congruence [13, p. 89] implies that $\mathcal{E}$ annihilates $J(\mathbb{Q})_{\mathrm{tor}} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$; see Proposition 4.2. Hence n is divisible by the exponent of this group, which is 84. ☐

Lemma 3.5. *The Hecke operators T_5 and T_{13} act on $\mathbb{T}/\mathcal{E} \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$ as $(1,-1,1)$ and $(1,1,-1)$, respectively.*

Proof. In the proof of Proposition 3.4 we computed that $T_5 \equiv 29 \pmod{\mathcal{E}}$. Similarly, $T_{13} = -T_3 + T_5 - T_{11} \equiv 13 \pmod{\mathcal{E}}$. From this the claim of the lemma immediately follows since, for example, $29 \equiv 1 \pmod 4$, $29 \equiv -1 \pmod 3$, and $29 \equiv 1 \pmod 7$. ☐

Remark 3.6. We note that T_5 and T_{13} are actually equal to the negatives of the Atkin-Lehner involutions W_5 and W_{13} acting on $S_2(65)$. The conclusion $(\mathbb{T}/\mathcal{E})_{\mathrm{odd}} \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$ then can be deduced from Theorem 3.1.3 in [17].

Proposition 3.4 implies that there are three Eisenstein maximal ideals in $\mathbb{T}$:

$$\begin{aligned} \mathfrak{m}_2 &:= (\mathcal{E}, 2) = (\mathcal{E}, 2, T_5 - 1, T_{13} - 1), \\ \mathfrak{m}_3 &:= (\mathcal{E}, 3) = (\mathcal{E}, 3, T_5 + 1, T_{13} - 1), \\ \mathfrak{m}_7 &:= (\mathcal{E}, 7) = (\mathcal{E}, 7, T_5 - 1, T_{13} + 1). \end{aligned}$$

Proposition 3.7. *We have:*

(i) *The ideal $\mathfrak{m}_2 \lhd \mathbb{T}$ is equal to the ideal*

$$\left((2,1,1)\widetilde{\mathbb{T}}\right) \cap \mathbb{T} = \left\{(a, b_1 + b_2\sqrt{2}, c_1 + c_2\sqrt{3}) \in \mathbb{T} \;\middle|\; a \in 2\mathbb{Z}\right\},$$

which is the unique maximal ideal of $\mathbb{T}$ of residue characteristic 2.

(ii) *$\mathfrak{m}_2^n$ is not principal for any $n \geq 1$.*

(iii) *$\mathbb{T}_{\mathfrak{m}_2}$ is not Gorenstein.*

Proof. (i) The uniqueness of the maximal ideal of residue characteristic 2 implies that it must be the Eisenstein maximal ideal $\mathfrak{m}_2$. To prove the uniqueness, note that each of the rings $\mathbb{Z}$, $\mathbb{Z}[\sqrt{2}]$, $\mathbb{Z}[\sqrt{3}]$ has a unique maximal ideal of residue

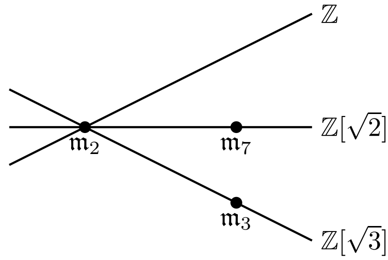

FIGURE 1. Spec($\mathbb{T}$)

characteristic 2; these are generated by 2, $\sqrt{2}$, and $1+\sqrt{3}$, respectively. One easily checks that

$$\mathfrak{m} := ((2,1,1)\widetilde{\mathbb{T}}) \cap \mathbb{T} = ((1,\sqrt{2},1)\widetilde{\mathbb{T}}) \cap \mathbb{T} = ((1,1,1+\sqrt{3})\widetilde{\mathbb{T}}) \cap \mathbb{T},$$

and $\mathbb{T}/\mathfrak{m} \cong \mathbb{F}_2$.

(ii) To prove this statement it is enough to observe that $(1,0,0) \in \widetilde{\mathbb{T}}$ is in $\mathrm{End}_{\mathbb{T}}(\mathfrak{m}_2^n)$ but $(1,0,0) \notin \mathbb{T}$.

(iii) We apply [23, Prop. 1.4 (iii)]: Let $\overline{\mathfrak{m}}_2$ denote the image of $\mathfrak{m}_2$ in $\mathbb{T}/2\mathbb{T}$. Then $\mathbb{T}_{\mathfrak{m}_2}$ is Gorenstein if and only if $\dim_{\mathbb{F}_2}(\mathbb{T}/2\mathbb{T})[\overline{\mathfrak{m}}_2] = 1$. Note that $(2,0,0)$ and $(0,2,0)$ have distinct non-zero images in $\mathbb{T}/2\mathbb{T}$, since otherwise $(2,2,0) \in 2\mathbb{T}$, which would imply $(1,1,0) \in \mathbb{T}$. On the other hand, for any $\theta \in \mathfrak{m}_2$ we have $\theta(2,0,0) = (4a,0,0) = 2(2a,0,0) \in 2\mathbb{T}$ for some $a \in \mathbb{Z}$. Therefore, $\overline{\mathfrak{m}}_2$ annihilates $(2,0,0)$, and similarly $\overline{\mathfrak{m}}_2$ annihilates $(0,2,0)$; thus, $\dim_{\mathbb{F}_2}(\mathbb{T}/2\mathbb{T})[\overline{\mathfrak{m}}_2] \geq 2$. $\square$

Spec($\mathbb{T}$) can be sketched as in Figure 1. It has three irreducible components intersecting at $\mathfrak{m}_2$. The irreducible components containing the closed points $\mathfrak{m}_3$ and $\mathfrak{m}_7$ are determined by observing that $T_5+1 = (0,2,0)$ and $T_5-1 = (-2,0,-2)$, so T_5 acts as -1 (resp., 1) on the component $\mathrm{Spec}(\mathbb{Z}[\sqrt{3}])$ (resp., $\mathrm{Spec}(\mathbb{Z}[\sqrt{2}])$). Finally, note that $\mathbb{T}_{\mathfrak{m}_7} \cong \mathbb{Z}_7$ and $\mathbb{T}_{\mathfrak{m}_3} \cong \mathbb{Z}_3[\sqrt{3}]$.

4. MODULAR JACOBIAN

There are exactly four cusps, denoted [1], [p], [q], and [pq], on $X_0(pq)$, where p and q are two distinct prime numbers. Let $\mathcal{C}(pq)$ be the subgroup of $J_0(pq)$ generated by all cuspidal divisors. Since all cusps are $\mathbb{Q}$-rational, we have $\mathcal{C}(pq) \subset J_0(pq)(\mathbb{Q})$. Let $\Phi(p)$ and $\Phi(q)$ denote the component groups of $J_0(pq)$ at p and q, and $\wp_p, \wp_q : \mathcal{C}(pq) \to \Phi(p), \Phi(q)$ be the homomorphisms induced by (2.3).

Proposition 4.1. *Let $p=5$ and $q=13$. Let c_p and c_q be the divisor classes of $[1]-[p]$ and $[1]-[q]$ in $J_0(pq)$. Denote $\mathcal{C} := \mathcal{C}(pq)$.*

(i) *$\mathcal{C}$ is generated by c_p and c_q. The order of c_p is 28; the order of c_q is 12; the only relation between c_p and c_q in $\mathcal{C}$ is $14c_p = 6c_q$. This implies*

$$\mathcal{C} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}.$$

(ii) *$\Phi(p) \cong \mathbb{Z}/42\mathbb{Z}$ and $\Phi(q) \cong \mathbb{Z}/6\mathbb{Z}$.*

(iii) *The order of $\wp_p(c_p)$ is 14, and $\wp_p(c_q) = 0$; this implies that there is an exact sequence*

$$0 \to \langle c_q \rangle \to \mathcal{C} \xrightarrow{\wp_p} \Phi(p) \to \mathbb{Z}/3\mathbb{Z} \to 0.$$

The order of $\wp_q(c_q)$ *is* 6*, and* $\wp_q(c_p) = 0$*; this implies that there is an exact sequence*

$$0 \to \langle c_p \rangle \to \mathcal{C} \xrightarrow{\wp_q} \Phi(q) \to 0.$$

Proof. (i) follows from [2]. The groups $\Phi(p)$ and $\Phi(q)$ can be computed from the structure of special fibers of $X_0(pq)$ using a well-known method of Raynaud; see [16, p. 214] or the appendix in [13]. Finally, by considering the reductions of the cusps in the special fiber of the minimal regular model of $X_0(pq)$ over $\mathbb{Z}_p$, one can determine the homomorphism $\wp_p$ and $\wp_q$; cf. [18, p. 1161]. □

Proposition 4.2. *We have* $\mathcal{C} = J(\mathbb{Q})_{\mathrm{tor}}$.

Proof. Obviously $\mathcal{C} \subseteq J(\mathbb{Q})_{\mathrm{tor}}$. On the other hand, J has good reduction at any odd prime $p \nmid 65$, so by Proposition 2.1 we have an injective homomorphism $J(\mathbb{Q})_{\mathrm{tor}} \hookrightarrow J(\mathbb{F}_p)$, where $J(\mathbb{F}_p)$ denotes the group of $\mathbb{F}_p$-rational points on the reduction of J at p. The order of $J(\mathbb{F}_p)$ can be computed using `Magma`. We have $\#J(\mathbb{F}_3) = 2^3 \cdot 3^2 \cdot 7$ and $\#J(\mathbb{F}_{11}) = 2^3 \cdot 3 \cdot 5 \cdot 7^2 \cdot 37$. Since the greatest common divisor of these numbers is $2^3 \cdot 3 \cdot 7 = \#\mathcal{C}$, the claim follows. □

The Hecke ring $\mathbb{T}$ is isomorphic to a subring of endomorphisms of J generated by the Hecke operators T_n acting as correspondences on X. In fact, in our case $\mathbb{T}$ is the full ring of endomorphisms of J (this can be proved as in [13, Prop. 9.5]). For a maximal ideal $\mathfrak{m} \lhd \mathbb{T}$, we denote

$$J[\mathfrak{m}] = \bigcap_{\alpha \in \mathfrak{m}} \ker(J \xrightarrow{\alpha} J).$$

Then $J[\mathfrak{m}] \subset J[p]$, where p is the characteristic of $\mathbb{T}/\mathfrak{m}$. By a theorem of Mazur [23, p. 341], $\mathbb{T}_\mathfrak{m}$ is Gorenstein if and only if $\dim_{\mathbb{T}/\mathfrak{m}} J[\mathfrak{m}] = 2$. Therefore, using Proposition 3.1, we conclude that $\dim_{\mathbb{T}/\mathfrak{m}} J[\mathfrak{m}] = 2$ for any maximal ideal $\mathfrak{m}$ of odd residue characteristic.

Let $p = 3, 7$ and $\mathfrak{m}_p$ be the corresponding Eisenstein maximal ideal. The Eichler-Shimura congruence relation implies that $\mathcal{E}$ annihilates $J(\mathbb{Q})_{\mathrm{tor}} = \mathcal{C}$. Hence $\mathbb{Z}/p\mathbb{Z} \cong \mathcal{C}_p \subset J[\mathfrak{m}_p]$. We have

$$0 \longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow J[\mathfrak{m}_p] \longrightarrow \mu_p \longrightarrow 0, \tag{4.1}$$

since $G_\mathbb{Q}$ acts on $\wedge^2 J[\mathfrak{m}_p]$ by the mod p cyclotomic character; cf. [22, p. 465]. By [12], the Shimura subgroup Σ (= kernel of the functorial homomorphims $J_0(65) \to J_1(65)$) is

$$\Sigma \cong \mu_2 \times \mu_3, \tag{4.2}$$

and the Eisenstein ideal $\mathcal{E}$ annihilates Σ. Therefore, (4.1) splits for $p = 3$:

$$J[\mathfrak{m}_3] = \mathcal{C}_3 \times \Sigma_3 \cong \mathbb{Z}/3\mathbb{Z} \times \mu_3.$$

Lemma 4.3. *The sequence* (4.1) *does not split for* $p = 7$.

Proof. If (4.1) splits, then $\mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} \subset J(\mathbb{Q}(\mu_7))_{\mathrm{tor}}$. Since $\ell = 29$ splits completely in $\mathbb{Q}(\mu_7)$, by Proposition 2.1 we must have $7^2 \mid \#J(\mathbb{F}_\ell) = 2^3 \cdot 3^2 \cdot 7 \cdot 13 \cdot 23^2$. □

Remark 4.4. Let E be the elliptic curve defined by $y^2 + xy = x^3 - x$. It is easy to check that E has a rational 2-torsion point and $E[2]$ as a Galois module is a non-split extension

$$0 \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow E[2] \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 0.$$

By Table 1 in [5], E is isomorphic to a subvariety of J. We claim that $E[2] \subset J[\mathfrak{m}_2]$. To see this, consider a Hecke operator $T_p = (a_p, b_p + \sqrt{2}c_p, d_p + \sqrt{3}e_p)$ for prime $p \nmid 65$, given as in (3.2). T_p acts on E by multiplication by a_p. The fact that $\mathfrak{m}_2$ is Eisenstein implies that $a_p - (p+1)$ is even; thus, $T_p - (p+1)$ annihilates $E[2]$; thus $\mathfrak{m}_2 = (2, \mathcal{E})$ annihilates $E[2]$. On the other hand, clearly $E[2] \not\subset \mathcal{C}[2]$, as $\mathcal{C}[2]$ is constant. Therefore, $\dim_{\mathbb{T}/\mathfrak{m}_2} J[\mathfrak{m}_2] \geq \dim_{\mathbb{F}_2} \mathcal{C}[2] + 1 = 3$. This gives a geometric proof of the fact that $\mathbb{T}_{\mathfrak{m}_2}$ is not Gorenstein. Note that Proposition 4.2 implies that $\Sigma[2] \subset \mathcal{C}[2]$, since $\mu_2 \cong \mathbb{Z}/2\mathbb{Z}$ is constant over $\mathbb{Q}$.

Proposition 4.5. *Let $\mathfrak{m} \lhd \mathbb{T}$ be an Eisenstein maximal ideal of odd residue characteristic p. Let $H \subset J[\mathfrak{m}^s]$, $s \geq 1$, be a $\mathbb{T}[G_{\mathbb{Q}}]$-module. If $J[\mathfrak{m}] \not\subset H$, then $H \subsetneq J[\mathfrak{m}]$.*

Proof. We will assume that $J[\mathfrak{m}] \not\subset H$ and $H \not\subset J[\mathfrak{m}]$, and reach a contradiction. First, we make some simplifications. Since $H[\mathfrak{m}^2] \subset J[\mathfrak{m}^2]$ is a $\mathbb{T}[G_{\mathbb{Q}}]$-module satisfying the same assumptions, if we want to show that H does not exist, it is enough to prove the non-existence under the additional assumption that $H \subset J[\mathfrak{m}^2]$.

Lemma 4.6. *We have $H \cong \mathbb{T}/\mathfrak{m}^2$.*

Proof. We can consider H as a finite $\mathbb{T}_{\mathfrak{m}}$-module. Since $\mathbb{T}_{\mathfrak{m}}$ is a DVR, we have

$$H \cong \mathbb{T}_{\mathfrak{m}}/\mathfrak{m}^{s_1} \times \cdots \times \mathbb{T}_{\mathfrak{m}}/\mathfrak{m}^{s_r} \cong \mathbb{T}/\mathfrak{m}^{s_1} \times \cdots \times \mathbb{T}/\mathfrak{m}^{s_r}$$

for some $1 \leq s_1 \leq s_2 \leq \cdots \leq s_r \leq 2$. Since $\dim_{\mathbb{T}/\mathfrak{m}} J[\mathfrak{m}] = 2$, and $H[\mathfrak{m}] \cong (\mathbb{T}/\mathfrak{m})^r \subsetneq J[\mathfrak{m}]$, we must have $r = 1$, i.e., $H \cong \mathbb{T}/\mathfrak{m}^s$ for $s = 1$ or $s = 2$. If $s = 1$, then $H \subset J[\mathfrak{m}]$, contrary to our assumption, so $s = 2$. $\square$

Note that

$$\mathbb{T}/\mathfrak{m}^2 \cong \begin{cases} \mathbb{Z}/p^2\mathbb{Z} & \text{if } p = 7; \\ \mathbb{F}_p[x]/(x^2) & \text{if } p = 3. \end{cases}$$

Let $K := \mathbb{Q}(H)$. If $K = \mathbb{Q}$, then $p^2 = \#H$ divides $\#J(\mathbb{Q})_{\mathrm{tor}}$. This contradicts Proposition 4.2, so we will assume from now on that $K \neq \mathbb{Q}$. Let η be a generator of $\mathfrak{m}$. Note that $\eta H = H[\eta] \subset J[\mathfrak{m}]$ is a proper non-trivial Galois invariant subgroup. On the other hand, the $G_{\mathbb{Q}}$-invariant subgroups of $J[\mathfrak{m}]$ are $\mathbb{Z}/p\mathbb{Z}$ and μ_p, so either

$$0 \to \mathbb{Z}/p\mathbb{Z} \to H \xrightarrow{\eta} \mathbb{Z}/p\mathbb{Z} \to 0, \tag{4.3}$$

or

$$0 \to \mu_p \to H \xrightarrow{\eta} \mu_p \to 0. \tag{4.4}$$

Moreover, the second possibility does not occur for $p = 7$, since (4.1) does not split.

Lemma 4.7. *Let K_p denote the unique degree p extension of $\mathbb{Q}$ contained in $\mathbb{Q}(\mu_{p^2})$.*

1. *If $p = 7$, then $K = K_p$.*
2. *Assume $p = 3$. In case of (4.3), we have $[K : \mathbb{Q}] = p$ and $K \subset K_p\mathbb{Q}(\mu_{13})$. In case of (4.4), we have $\mathbb{Q}(\mu_p) \subseteq K \subset \mathbb{Q}(\mu_{p^2}, \mu_{13})$.*

Proof. Since the actions of $\mathbb{T}$ and $G_{\mathbb{Q}}$ on H commute, we have

$$\mathrm{Gal}(K/\mathbb{Q}) \subset \mathrm{Aut}_{\mathbb{T}}(\mathbb{T}/\mathfrak{m}^2) \cong (\mathbb{T}/\mathfrak{m}^2)^{\times} \cong \mathbb{Z}/(p-1)p\mathbb{Z}.$$

Hence $K/\mathbb{Q}$ is an abelian extension. Since J has good reduction away from 5 and 13, the extension $K/\mathbb{Q}$ is unramified away from $p, 5, 13$. By class field theory, K is a subfield of a cyclotomic extension $\mathbb{Q}(\mu_{p^{n_1}}, \mu_{5^{n_2}}, \mu_{13^{n_3}})$, for some $n_1, n_2, n_3 \geq 1$. We have

$$\begin{aligned}
&\mathrm{Gal}(\mathbb{Q}(\mu_{p^{n_1}}, \mu_{5^{n_2}}, \mu_{13^{n_3}})/\mathbb{Q}) \\
&\cong \mathrm{Gal}(\mathbb{Q}(\mu_{p^{n_1}}/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(\mu_{5^{n_2}}/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(\mu_{13^{n_3}}/\mathbb{Q}) \\
&\cong \mathbb{Z}/p^{n_1-1}(p-1)\mathbb{Z} \times \mathbb{Z}/5^{n_2-1}(5-1)\mathbb{Z} \times \mathbb{Z}/13^{n_3-1}(13-1)\mathbb{Z}.
\end{aligned}$$

Assume $p = 7$. Since in this case H is as in (4.3), $G_\mathbb{Q}$ acts trivially on pH, so $\mathrm{Gal}(K/\mathbb{Q})$ is in the subgroup of units $(\mathbb{Z}/p^2\mathbb{Z})^\times$ which satisfy $ap \equiv p \pmod{p^2}$, or equivalently, $a \equiv 1 \pmod{p}$. The units with this property form the cyclic subgroup of order p in $(\mathbb{Z}/p^2\mathbb{Z})^\times$. Hence $K/\mathbb{Q}$ is an abelian extension of degree p. Since p does not divide $(5-1)5^{n_2-1}$ or $(13-1)13^{n_3-1}$, the field K is fixed by $\mathrm{Gal}(\mathbb{Q}(\mu_{5^{n_2}})/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(\mu_{13^{n_3}})/\mathbb{Q})$. Therefore, $K \subset \mathbb{Q}(\mu_{p^{n_1}})$ is a subfield of degree p over $\mathbb{Q}$. There is a unique such field (as $\mathrm{Gal}(\mathbb{Q}(\mu_{p^{n_1}}/\mathbb{Q})$ is cyclic), and it is contained in $\mathbb{Q}(\mu_{p^2})$.

Assume $p = 3$ and H fits into an exact sequence (4.3). By the argument in the previous paragraph, $[K : \mathbb{Q}] = p$. Let $F := \mathbb{Q}(\mu_{13})$ and $K' = F(H)$. We know that $[K' : F] = 1$ or p. Note that

$$\mathrm{Gal}(\mathbb{Q}(\mu_{p^{n_1}}, \mu_{5^{n_2}}, \mu_{13^{n_3}})/F) \cong \mathbb{Z}/(p-1)p^{n_1-1} \times \mathbb{Z}(5-1)5^{n_2-1} \times \mathbb{Z}/13^{n_3-1}\mathbb{Z},$$

so as in the case of $p = 7$, we get $F(H) \subset K_pF$.

Finally, assume $p = 3$ and H fits into an exact sequence (4.4). Then obviously $\mathbb{Q}(\mu_p) \subset K$. Over $L := \mathbb{Q}(\mu_p)$, the group scheme H fits into an exact sequence (4.3), so, as in the earlier cases, $L(H)/L$ is cyclic of order 1 or p. If H is not constant over FL, then $[FL(H) : FL] = p$. On the other hand,

$$\mathrm{Gal}(\mathbb{Q}(\mu_{p^{n_1}}, \mu_{5^{n_2}}, \mu_{13^{n_3}})/FL) \cong \mathbb{Z}/p^{n_1-1} \times \mathbb{Z}(5-1)5^{n_2-1} \times \mathbb{Z}/13^{n_3-1}\mathbb{Z}.$$

As in the earlier cases, this implies that $FL(H) \subset K_pFL = \mathbb{Q}(\mu_{p^2}, \mu_{13})$. Overall, we see that K is always a subfield of $\mathbb{Q}(\mu_{p^2}, \mu_{13})$. $\square$

Assume $p = 7$. By Lemma 4.7, we have $K = K_p$. Let ℓ be a prime which splits completely in K_p. Then H is constant over $\mathbb{Q}_\ell$, so $H \subset J(\mathbb{Q}_\ell)_{\mathrm{tor}}$. On the other hand, under the canonical reduction map, we have an injection $J(\mathbb{Q}_\ell)_{\mathrm{tor}} \hookrightarrow J(\mathbb{F}_\ell)$; see Proposition 2.1. Therefore, we must have $p^2 \mid \#J(\mathbb{F}_\ell)$. It is easy to show that a prime ℓ splits completely in K_p if and only if its order in $(\mathbb{Z}/p^2\mathbb{Z})^\times$ is coprime to p. We can take 3 as a generator of $(\mathbb{Z}/p^2\mathbb{Z})^\times$. The elements of orders coprime to p are the powers of $3^7 \equiv 31$. These are $\{31, 30, 48, 18, 19, 1\}$. Thus, the smallest prime that splits completely in K_7 is 19, and $\#J(\mathbb{F}_{19}) = 2^3 \cdot 3^2 \cdot 7 \cdot 13 \cdot 23^2$. As 7^2 does not divide this number, we get a contradiction.

Assume $p = 3$. By Lemma 4.7, we have $\mathbb{Q}(H) \subset \mathbb{Q}(\mu_{13}, \mu_{p^2})$. Since μ_p is constant over K', we have $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \cong J(K')[\mathfrak{m}] \subset J(K')_{\mathrm{tor}} \subset J(\mathbb{Q}_\ell)$. Since H is also constant over K', we also have $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \cong H \subset J(\mathbb{Q}_\ell)$. Since $J[\mathfrak{m}] \not\subset H$, we see that $J(\mathbb{Q}_\ell)$ contains a subgroup isomorphic to $(\mathbb{Z}/p\mathbb{Z})^3$. As earlier, this implies that $p^3 \mid \#J(\mathbb{F}_\ell)$. A prime ℓ splits completely in $K' := \mathbb{Q}(\mu_{13}, \mu_{p^2})$ if and only if $\ell \equiv 1 \pmod{9}$ and $\ell \equiv 1 \pmod{13}$. The smallest such prime is $\ell = 937$, and $\#J(\mathbb{F}_{937}) = 2^{13} \cdot 3^2 \cdot 7 \cdot 11^2 \cdot 41 \cdot 97 \cdot 2963$. As 3^3 does not divide this number, we get a contradiction. This concludes the proof of Proposition 4.5. $\square$

Let A be an abelian variety over $\mathbb{Q}$ and $\pi : J \to A$ an isogeny defined over $\mathbb{Q}$. Assume $\ker(\pi)$ is invariant under the action of $\mathbb{T}$, i.e., $\ker(\pi)$ is a finite $\mathbb{T}[G_\mathbb{Q}]$-module.

We can decompose $\ker(\pi) = \ker(\pi)_2 \times \ker(\pi)_{\mathrm{odd}}$; each of these subgroups is also a $\mathbb{T}[G_{\mathbb{Q}}]$-module. Let the maximal ideal $\mathfrak{m} \lhd \mathbb{T}$ be in the support of $H := \ker(\pi)_{\mathrm{odd}}$. Since $\mathfrak{m}$ has odd residue characteristic, $\mathfrak{m} = \eta\mathbb{T}$ is principal by Proposition 3.1. If $\ker(\eta) = J[\mathfrak{m}] \subset H$, then we can decompose $\pi = \pi' \circ \eta$, where $\pi' : J \to A$ is another isogeny whose kernel is a $\mathbb{T}[G_{\mathbb{Q}}]$-module but with smaller odd component than π. We can apply the same argument to π' and continue this process until we obtain an isogeny whose kernel does not contain any $J[\mathfrak{m}]$ with $\mathfrak{m}$ having odd residue characteristic. From now on we assume that π itself has this property.

Since $\mathfrak{m}$ has odd residue characteristic, the $\mathbb{T}[G_{\mathbb{Q}}]$-module $J[\mathfrak{m}]$ is 2-dimensional over $\mathbb{T}/\mathfrak{m}$. By [13, Prop. 14.2] and [22, Thm. 5.2], if $\mathfrak{m}$ is not Eisenstein, then $J[\mathfrak{m}]$ is irreducible. Since $J[\mathfrak{m}] \cap H \neq 0$, we must have $J[\mathfrak{m}] \subset H$, which contradicts our assumption on π. Hence H is supported on the Eisenstein maximal ideals $\mathfrak{m}_3$ and $\mathfrak{m}_7$. We decompose $H = H_3 \times H_7$ into 3-primary and 7-primary components, which themselves are $\mathbb{T}[G_{\mathbb{Q}}]$-modules. Now $H_p \subset J[\mathfrak{m}_p^s]$ for some $s \geq 1$, $p = 3, 7$, and $J[\mathfrak{m}_p] \not\subset H_p$. Applying Proposition 4.5, we conclude that $H_p \subsetneq J[\mathfrak{m}_p]$. Thus $H_7 = 0$ or $\mathcal{C}_7$, and $H_3 = 0$ or Σ_3 or $\mathcal{C}_3$. Overall, H can be one of the following subgroups of J:

$$0, \quad \mathcal{C}_3, \quad \Sigma_3, \quad \mathcal{C}_7, \quad \mathcal{C}_3 \times \mathcal{C}_7, \quad \Sigma_3 \times \mathcal{C}_7. \tag{4.5}$$

Theorem 4.8. *If $A = J'$, then for $\pi : J \to J'$ chosen with the minimality condition discussed above, we must have $H = \mathcal{C}_7$.*

Proof. The reductions of J and J' at $p = 5$ or 13 are purely toric; cf. [16], [22]. Let $\Phi(5)'$ and $\Phi(13)'$ be the component groups of J' at 5 and 13. We have (see [16, p. 214]):

$$\Phi(5)' \cong \mathbb{Z}/6\mathbb{Z}, \qquad \Phi(13)' \cong \mathbb{Z}/42\mathbb{Z}.$$

We decompose $\pi : J \to J'$ as $J \to J/H \xrightarrow{\pi'} J'$, where $\ker(\pi')$ is isomorphic to the 2-primary part of $\ker(\pi)$. Let $\Phi(p)''$ be the component group of J/H at p. By Lemma 2.2 we must have $(\Phi(p)'')_{\mathrm{odd}} \cong (\Phi(p)')_{\mathrm{odd}}$. On the other hand, since we know the image and kernel of $\wp_p : \mathcal{C} \to \Phi(p)$, we can compute $\#(\Phi(p)'')_{\mathrm{odd}}$ for each possible H from the list (4.5) using Lemma 2.3. This simple calculation shows that the only possible H is $\mathcal{C}_7$. (Note that the group-scheme Σ_3 becomes constant over an unramified extension of $\mathbb{Q}_p$, but it is not important to know whether $\wp_p : \Sigma_3 \to \Phi(p)$ is injective or trivial; neither of these possibilities gives the correct $\Phi(p)''$ if $\Sigma_3 \subset H$.) $\square$

Remark 4.9. Let $N = 5 \cdot 7$. In this case,

$$\begin{aligned} \mathbb{T} = \mathbb{Z}[T_3] &\cong \mathbb{Z}[x]/(x-1)(x^2+x-4) \\ &\cong \{(a, b + c\alpha) \in \mathbb{Z} \times \mathbb{Z}[\alpha] \mid a, b, c \in \mathbb{Z},\ a \equiv b + c \pmod 2\}, \end{aligned}$$

where $\alpha := -\frac{1+\sqrt{17}}{2}$. Note that $\mathbb{Z}[\alpha]$ is the ring of integers in $\mathbb{Q}(\sqrt{17})$, and $\mathbb{Z}[\alpha]$ is a Euclidean domain with respect to the usual norm. We have

$$\mathcal{C} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}, \qquad \Sigma \cong \mu_4 \times \mu_3.$$

There is a unique Eisenstein maximal ideal $\mathfrak{m}_3 \lhd \mathbb{T}$ of odd residue characteristic. There is a unique $\mathbb{Q}$-isogeny class of elliptic curves of level 35. The optimal curve is [5, p. 112]

$$E : y^2 + y = x^3 + x^2 + 9x + 1.$$

We have $E[3] \cong \mu_3 \times \mathbb{Z}/3\mathbb{Z}$. Since $\mathbb{T}_\mathfrak{m}$ is Gorenstein for any maximal ideal $\mathfrak{m} \lhd \mathbb{T}$ (as $\mathbb{T}$ is monogenic), $J[\mathfrak{m}]$ is 2-dimensional over $\mathbb{T}/\mathfrak{m}$, so $J[\mathfrak{m}_3] = E[3] = \mathcal{C}_3 \times \Sigma_3$. Now it is easy to analyze all $\mathbb{T}[G_\mathbb{Q}]$-submodules of J supported on $\mathfrak{m}_3$. An argument similar to the argument of the proof of Theorem 4.8 then implies that there is a Ribet isogeny $\pi : J \to J'$ with $\ker(\pi)_{\mathrm{odd}} = 0$. Ogg's conjecture in this case predicts that $\ker(\pi) \cong \mathbb{Z}/2\mathbb{Z} \subset \mathcal{C}_2$.

Remark 4.10. Let $N = 3 \cdot 13$. In this case,

$$\begin{aligned}\mathbb{T} = \mathbb{Z}[T_2] &\cong \mathbb{Z}[x]/(x-1)(x^2+2x-1)\\ &\cong \{(a, b + c\sqrt{2}) \in \mathbb{Z} \times \mathbb{Z}[\sqrt{2}] \mid a, b, c \in \mathbb{Z},\ a \equiv b \pmod 2\}.\end{aligned}$$

We have

$$\mathcal{C} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}, \qquad \Sigma \cong \mu_4.$$

There is a unique Eisenstein maximal ideal $\mathfrak{m}_7 \lhd \mathbb{T}$ of odd residue characteristic. $J[\mathfrak{m}]$ fits into the exact sequence (4.1), which is non-split in this case. One can classify $\mathbb{T}[G_\mathbb{Q}]$-submodules of J supported on $\mathfrak{m}_7$ using an argument similar to the argument we used in Proposition 4.5. Finally, one deduces as in Theorem 4.8 that there is a Ribet isogeny $\pi : J \to J'$ with $\ker(\pi)_{\mathrm{odd}} = \mathcal{C}_7 \cong \mathbb{Z}/7\mathbb{Z}$. Ogg's conjecture in this case predicts that $\ker(\pi) = \mathcal{C}_7$.

Acknowledgments

This work was carried out in part while the second author was visiting the Taida Institute for Mathematical Sciences in Taipei and the Max Planck Institute for Mathematics in Bonn in 2016. He thanks these institutes for their hospitality, excellent working conditions, and financial support. He is also grateful to Fu-Tsun Wei for very useful discussions related to the topic of this paper.

References

[1] Siegfried Bosch, Werner Lütkebohmert, and Michel Raynaud, *Néron models*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], vol. 21, Springer-Verlag, Berlin, 1990. MR1045822

[2] Seng-Kiat Chua and San Ling, *On the rational cuspidal subgroup and the rational torsion points of $J_0(pq)$*, Proc. Amer. Math. Soc. **125** (1997), no. 8, 2255–2263. MR1396972

[3] Brian Conrad and William A. Stein, *Component groups of purely toric quotients*, Math. Res. Lett. **8** (2001), no. 5-6, 745–766. MR1879817

[4] David A. Cox, *Primes of the form $x^2 + ny^2$*, 2nd ed., Pure and Applied Mathematics (Hoboken), John Wiley & Sons, Inc., Hoboken, NJ, 2013. Fermat, class field theory, and complex multiplication. MR3236783

[5] J. E. Cremona, *Algorithms for modular elliptic curves*, 2nd ed., Cambridge University Press, Cambridge, 1997. MR1628193

[6] Josep González and Santiago Molina, *The kernel of Ribet's isogeny for genus three Shimura curves*, J. Math. Soc. Japan **68** (2016), no. 2, 609–635. MR3488137

[7] Josep González and Victor Rotger, *Equations of Shimura curves of genus two*, Int. Math. Res. Not. **14** (2004), 661–674. MR2038166

[8] A. Grothendieck, *Modèles de Néron et monodromie*, SGA 7, Exposé IX, 1972.

[9] David Helm, *On maps between modular Jacobians and Jacobians of Shimura curves*, Israel J. Math. **160** (2007), 61–117. MR2342491

[10] Bruce W. Jordan and Ron A. Livné, *On the Néron model of Jacobians of Shimura curves*, Compositio Math. **60** (1986), no. 2, 227–236. MR868139

[11] Nicholas M. Katz, *Galois properties of torsion points on abelian varieties*, Invent. Math. **62** (1981), no. 3, 481–502. MR604840

[12] San Ling and Joseph Oesterlé, *The Shimura subgroup of $J_0(N)$* (English, with French summary), Astérisque **196-197** (1991), 6, 171–203 (1992). Courbes modulaires et courbes de Shimura (Orsay, 1987/1988). MR1141458

[13] B. Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. **47** (1977), 33–186 (1978). MR488287

[14] Jean-Francis Michon, *Courbes de Shimura hyperelliptiques* (French), Bull. Soc. Math. France **109** (1981), no. 2, 217–225. MR623790

[15] David Mumford, *Abelian varieties*, Tata Institute of Fundamental Research Studies in Mathematics, No. 5, Published for the Tata Institute of Fundamental Research, Bombay; Oxford University Press, London, 1970. MR0282985

[16] A. P. Ogg, *Mauvaise réduction des courbes de Shimura* (French), Séminaire de théorie des nombres, Paris 1983–84, Progr. Math., vol. 59, Birkhäuser Boston, Boston, MA, 1985, pp. 199–217. MR902833

[17] Masami Ohta, *Eisenstein ideals and the rational torsion subgroups of modular Jacobian varieties II*, Tokyo J. Math. **37** (2014), no. 2, 273–318. MR3304683

[18] Mihran Papikian, *On Jacquet-Langlands isogeny over function fields*, J. Number Theory **131** (2011), no. 7, 1149–1175. MR2782835

[19] I. Reiner, *Maximal orders*, London Mathematical Society Monographs. New Series, vol. 28, The Clarendon Press, Oxford University Press, Oxford, 2003. Corrected reprint of the 1975 original; With a foreword by M. J. Taylor. MR1972204

[20] Kenneth Ribet, *Sur les variétés abéliennes à multiplications réelles* (French, with English summary), C. R. Acad. Sci. Paris Sér. A-B **291** (1980), no. 2, A121–A123. MR604997

[21] Kenneth A. Ribet, *On the component groups and the Shimura subgroup of $J_0(N)$*, Séminaire de Théorie des Nombres, 1987–1988 (Talence, 1987), Univ. Bordeaux I, Talence, [1988?], pp. Exp. No. 6, 10. MR993107

[22] K. A. Ribet, *On modular representations of $Gal(\overline{\boldsymbol{Q}}/\boldsymbol{Q})$ arising from modular forms*, Invent. Math. **100** (1990), no. 2, 431–476. MR1047143

[23] Jacques Tilouine, *Hecke algebras and the Gorenstein property*, Modular forms and Fermat's last theorem (Boston, MA, 1995), Springer, New York, 1997, pp. 327–342. MR1638483

[24] Hwajong Yoo, *Rational torsion points on Jacobians of Shimura curves*, Bull. Lond. Math. Soc. **48** (2016), no. 1, 163–171. MR3455760

Department of Mathematics, Queens College, City University of New York, 65-30 Kissena Boulevard Flushing, New York 11367

Email address: kklosin@qc.cuny.edu

Department of Mathematics, Pennsylvania State University, University Park, Pennsylvania 16802

Email address: papikian@psu.edu