ON RIBET’S ISOGENY FOR $J_0(65)$

KRZYSZTOF KLOSIN AND MIHRAN PAPIKIAN

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 $J_0(N)^{\text{new}}$ 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 $J_0(N)^{\text{new}}$ and $J^N$ are isomorphic as $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-modules, where $\ell$ 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 $J_0(N)^{\text{new}} \to J^N$ 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 $J_0(N)^{\text{new}} \to J^N$ 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 $J_0(N)^{\text{new}} \to J^N$ 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 components of the Néron models of $J_0(N)^{\text{new}}$ and $J^N$ at $q$ yields restrictions on

2010 Mathematics Subject Classification. 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).
the isogenies between them. Ogg’s conjecture remains open except for the special cases when $J^N$ has dimension $\leq 3$.

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 $J_0(N)^{\text{new}}$ 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 \texttt{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 $J_0(N)^{\text{new}}$ 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 $J_0(N)^{\text{new}}$ can be computed using cusp forms with rational $q$-expansions. The problem then reduces to comparing the period matrices of appropriate quotients of $J_0(N)^{\text{new}}$ 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 \[10\]. The difficulty shifts to the study of the structure of the Hecke algebra and its action on $J_0(N)$.

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

$$\pi : J_0(N) \to J^N.$$ $T(N)$ also naturally acts on $J^N$ and $\pi$ is $T(N)$-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 $T := T(N)$, $J := J_0(N)$, $J' := J^N$, $G_\mathbb{Q} := \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Given a finite abelian group $H$, we denote by $H_p$ its $p$-primary component ($p$ is a prime number), and by $H_{\text{odd}}$ its maximal subgroup of odd order, so that $H \cong H_2 \times H_{\text{odd}}$. Since the endomorphisms of $J$ induced by Hecke operators are defined over $\mathbb{Q}$, the actions of $T$ and $G_\mathbb{Q}$ on $J$ commute with each other. Thus, $\ker(\pi)$ is a $T[G_\mathbb{Q}]$-submodule of $J$. We show that if the kernel of an isogeny from $J$ to another abelian variety is a $T[G_\mathbb{Q}]$-module, then, up to endomorphisms of $J$, the kernel is supported on the Eisenstein maximal ideals of $T$. We then classify all $T[G_\mathbb{Q}]$-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 $\ker(\pi)_{\text{odd}} \cong \mathbb{Z}/7^k\mathbb{Z}$ 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 \( m_2 \triangleleft \mathbb{T} \) 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 \( m_2 \) 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 \( m_2 \) is a prime of fusion, \( \mathbb{T}_{m_2} \) 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 \( J_0(N)_{\text{new}} = J_0(N) \) (equiv. \( N = 3 \cdot 13, 5 \cdot 7 \)); see Remarks 4.9 and 4.10

**Remark 1.2.** Given a prime \( \ell \), if \( H := (J_0(N)_{\text{new}}(\mathbb{Q})_{\text{cor}})_\ell \neq 0 \) but \( (J^N(\mathbb{Q})_{\text{cor}})_\ell = 0 \), then obviously \( H \subset \ker(\pi) \) for any Ribet isogeny \( \pi : J_0(N)_{\text{new}} \to J^N \). For an odd prime \( \ell \), in [24], Yoo gives sufficient conditions for the non-existence of rational points of order \( \ell \) 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 \( \mathcal{A}^0 \) the connected component of the identity of the special fiber \( \mathcal{A}_k \) of \( A \). There is an exact sequence

\[
0 \to \mathcal{A}^0 \to \mathcal{A} \to \Phi_A \to 0,
\]

where \( \Phi_A \) 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. [11 p. 181]):

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

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

\[
\text{M}_A := \text{Hom}(\text{(}[T_A]_k, \mathbb{G}_{m,k})
\]

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

\[
A(K') \to \mathcal{A}_k(k').
\]

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

\[
A(K') \to \Phi_A.
\]

**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 \( H \to \mathcal{A}_k(k') \).

**Proof.** See [11 p. 502] and [11 Prop. 7.3/3], \( \square \)
Let \( \varphi : A \to B \) be an isogeny defined over \( K \). By the Néron mapping property, \( \varphi \) extends to a morphism \( \varphi : A \to B \) of the Néron models. On the special fibers we get a homomorphism \( \varphi_k : A_k \to B_k \), which induces an isogeny \( \varphi_k^0 : A_k^0 \to B_k^0 \); \cite[Cor. 7.3/7]{H}. This implies that \( A \) has semi-abelian (resp. toric) reduction if \( A \) has semi-abelian (resp. toric) reduction. The isogeny \( \varphi_k^0 \) restricts to an isogeny \( \varphi_t : T_A \to T_B \), which corresponds to an injective homomorphisms 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 \( \varphi \). Assume \( A \) has semi-abelian reduction. In \cite{G}, Grothendieck defined a non-degenerate pairing \( u_A : M_A \times \hat{M}_A \to \mathbb{Z} \) (called \textit{monodromy pairing}) with nice functorial properties, which induces an exact sequence

\[
0 \to M_A \ni u \to \text{Hom}(M_A, \mathbb{Z}) \to \Phi_A \to 0.
\]

Using \cite[(2.4)]{K}, one obtains a commutative diagram with exact rows (cf. \cite[p. 8]{K}):

\[
\begin{array}{ccccccccc}
0 & \to & M_A & \to & \text{Hom}(M_A, \mathbb{Z}) & \to & \Phi_A & \to & 0 \\
\downarrow \varphi^* & & \downarrow & & \downarrow \varphi_\Phi & & \downarrow \varphi & & \\
0 & \to & M_B & \to & \text{Hom}(M_B, \mathbb{Z}) & \to & \Phi_B & \to & 0.
\end{array}
\]

From this diagram we get the exact sequence

\[
0 \to \ker(\varphi_\Phi) \to M_B/\varphi^*(M_A) \to \text{Ext}^1_B(\text{Hom}(M_A/\varphi^*(M_B), \mathbb{Z}) \to \text{coker}(\varphi_\Phi) \to 0.
\]

Since

\[
\text{Ext}^1_B(M_A/\varphi^*(M_B), \mathbb{Z}) \cong \text{Hom}(M_A/\varphi^*(M_B), \mathbb{Q}/\mathbb{Z}) =: (M_A/\varphi^*(M_B))^{\text{v}},
\]

we can rewrite (2.5) as

\[
0 \to \ker(\varphi_\Phi) \to M_B/\varphi^*(M_A) \to (M_A/\varphi^*(M_B))^{\text{v}} \to \text{coker}(\varphi_\Phi) \to 0.
\]

Note that \( M_A/\varphi^*(M_B) \cong \text{Hom}(\ker(\varphi), G_{m,k}) \). On the other hand, \( \ker(\varphi_1) \) can be canonically identified with a subgroup scheme of \( H := \ker(\varphi) \); cf. \cite[p. 762]{K}. Therefore, \#\( M_A/\varphi^*(M_B) \) divides \#\( H \). Similarly, \#\( M_B/\varphi^*(M_A) \) divides \#\( \ker(\varphi) \). Since \( \ker(\varphi) \cong \text{Hom}(\ker(\varphi), G_{m,k}) \) (see \cite[Thm.1, p. 143]{L}), we conclude that \#\( M_B/\varphi^*(M_A) \) also divides \#\( H \). Now one easily deduces from (2.6) the following:

\textbf{Lemma 2.2.} Assume \( A \) has semi-abelian reduction, and \( \varphi : A \to B \) is an isogeny defined over \( K \). If \( \ell \) is a prime number which does not divide \#\( \ker(\varphi) \), then \( \varphi_\Phi \) induces an isomorphism \( (\Phi_A)^\ell \cong (\Phi_B)^\ell \).

\textbf{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 $H \rightarrow A(k')$ and $H_0 = \ker(\varphi)$. This implies $(M_A/\varphi^*(M_B))^\vee \cong H_0$. Next, [3 Thm. 8.6] implies that $M_B/\varphi^*(M_A) \cong H_1$. Thus, we can rewrite (2.6) as

$$0 \rightarrow \ker(\varphi_\mathfrak{p}) \rightarrow H_1 \rightarrow H_0 \rightarrow \coker(\varphi_\mathfrak{p}) \rightarrow 0.$$ 

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

\[ \Box \]

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 $\text{disc}(\mathbb{T})$ 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 $\text{disc}(\mathbb{T}) = 2^{11} \cdot 3$. We then obtain

$$\mathbb{T} = ZT_1 + ZT_2 + ZT_3 + ZT_5 + ZT_{11}$$

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

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

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

$$T_1 = (1, 1, 1)$$
$$T_2 = (-1, -1 + \sqrt{2}, \sqrt{3})$$
$$T_3 = (-2, \sqrt{2}, 1 - \sqrt{3})$$
$$T_5 = (-1, 1, -1)$$
$$T_{11} = (2, 2 - \sqrt{2}, -3 + \sqrt{3}).$$

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

$$\mathbb{T} \cong \left\{ (a, b_1 + b_2\sqrt{2}, c_1 + c_2\sqrt{3}) \mid a, b_1, b_2, c_1, c_2 \in \mathbb{Z}, \quad a \equiv b_1 \equiv c_1 + c_2 \mod 2, \quad b_2 \equiv c_2 \mod 2 \right\}.$$ 

Given a maximal ideal $\mathfrak{m} \triangleleft \mathbb{T}$, let $\mathbb{T}_\mathfrak{m} = \lim_{\mathfrak{m}} \mathbb{T}/\mathfrak{m}^n$ 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 $\mathfrak{m} \triangleleft \mathbb{T}$ of odd residue characteristic; cf. [23 p. 329].

Proof. Since

$$\text{disc}(\mathbb{T}) = [\tilde{\mathbb{T}} : \mathbb{T}]^2 \cdot \text{disc}(\tilde{\mathbb{T}}) = [\tilde{\mathbb{T}} : \mathbb{T}]^2 \cdot 2^5 \cdot 3,$$

we get $[\tilde{\mathbb{T}} : \mathbb{T}] = 2^3$. Let $I_{\mathbb{T}, 2'}$ be the set of ideals $I \triangleleft \mathbb{T}$ such that $\mathbb{T}/I$ is a finite ring of odd order. Let $I_{\mathbb{T}, 2'}$ be the set of ideals $I \triangleleft \mathbb{T}$ 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 $I_{\mathbb{T}, 2'}$ to $I_{\mathbb{T}, 2'}$, with the inverse given by
Moreover, the proof of that proposition shows that for $I \in I_{\mathbb{T},2'}$, we have $\mathbb{T}/I \cong \mathbb{T}/I \cap \mathbb{T}$, so that this bijection restricts to a bijection between the maximal ideals of $\mathbb{T}$ and $\mathbb{T}$ of odd residue characteristic.

Since $\mathbb{T}$ is a direct product of Euclidean domains, every ideal $I \in I_{\mathbb{T},2'}$ is principal. Write $I = \theta \mathbb{T}$. If $\theta \in \mathbb{T}$, then $I \cap \mathbb{T} = \theta \mathbb{T}$ is also principal, since $(\theta \mathbb{T})\mathbb{T} = \theta \mathbb{T}$. Therefore, to prove the proposition it is enough to show that for every maximal ideal $m \in I_{\mathbb{T},2'}$ we can choose a generator which lies in $\mathbb{T}$. Let $p > 2$ be the residue characteristic of $m = \theta \mathbb{T}$. If we write $m = m' \times m''$, where $m' \triangleleft \mathbb{Z}$, $m'' \triangleleft \mathbb{Z}[\sqrt{2}]$, $m'' \triangleleft \mathbb{Z}[\sqrt{3}]$, 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: $m' = p\mathbb{Z}$. Then $\theta = (p, 1, 1) \in \mathbb{T}$.

Case 2: $m''$ is proper. If $(p)$ is inert in $\mathbb{Z}[\sqrt{2}]$, then we can take $\theta = (1, 1, 1) \in \mathbb{T}$. Now suppose $p = (\alpha + \beta \sqrt{2})(\alpha - \beta \sqrt{2})$ splits, where $\alpha, \beta \in \mathbb{Z}$. Note that $\alpha$ must be odd. If $\beta$ is even, then $\theta = (1, \alpha \pm \beta \sqrt{2}, 1) \in \mathbb{T}$. If $\beta$ 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: $m'''$ is proper. If $(p)$ is inert in $\mathbb{Z}[\sqrt{3}]$, then we can take $\theta = (1, 1, 1) \in \mathbb{T}$. If $p = 3$, then $\theta = (1, 1, 1 + \sqrt{2}, \sqrt{3}) \in \mathbb{T}$, 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 $1 \equiv (\alpha + \beta)^2 \mod 2$, so that $\alpha$ and $\beta$ have different parity. If $\alpha$ is odd and $\beta$ is even, then $\theta = (1, 1, 1, \alpha \pm \beta \sqrt{3}) \in \mathbb{T}$. If $\alpha$ is even and $\beta$ is odd, then $\theta = (1, 1, 1 + \sqrt{2}, \alpha \pm \beta \sqrt{3}) \in \mathbb{T}$. □

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 $\mathcal{I} = (2 + i)\mathcal{O}$ is maximal and $\mathcal{O}/\mathcal{I} \cong \mathbb{F}_5$. On the other hand, $\mathcal{I} \cap \mathcal{O}' = (5, 1 + 3i)\mathcal{O}'$ is not principal, although $(5, 1 + 3i)\mathcal{O} = \mathcal{I}$. 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 $\mathcal{E} \triangleleft \mathbb{T}$ generated by $T_\ell - (\ell + 1)$ for all primes $\ell \nmid 65$. A maximal ideal $\mathfrak{m} \triangleleft \mathbb{T}$ 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

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

The Hecke operators $T_\ell$ 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 \( 3 \cdot 7 = 84 \). On the other hand, the Eichler-Shimura congruence \([13, p. 89]\) implies that \( \mathcal{E} \) annihilates \( J(\mathbb{Q})_{\text{tor}} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} \); see Proposition \([4,2]\). Hence \( n \) is divisible by the exponent of this group, which is 84.

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

\[ \text{Proof.} \quad \text{In the proof of Proposition } [5,4] \text{ we computed that } T_5 \equiv 29 \pmod{\mathcal{E}}. \text{ Similarly, } T_{13} = -T_3 + T_5 - T_{11} \equiv 13 \pmod{\mathcal{E}}. \text{ From this the claim of the lemma immediately follows since, for example, } 29 \equiv 1 \pmod{4}, 29 \equiv -1 \pmod{3}, \text{ and } 29 \equiv 1 \pmod{7}. \]

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

Proposition \([5,4]\) implies that there are three Eisenstein maximal ideals in \( \mathbb{T} \):

\[ m_2 := (\mathcal{E}, 2) = (\mathcal{E}, 2, T_5 - 1, T_{13} - 1), \]

\[ m_3 := (\mathcal{E}, 3) = (\mathcal{E}, 3, T_5 + 1, T_{13} - 1), \]

\[ m_7 := (\mathcal{E}, 7) = (\mathcal{E}, 7, T_5 - 1, T_{13} + 1). \]

\[ \text{Proposition 3.7.} \quad \text{We have:} \]

\[ \text{(i) The ideal } m_2 \triangleleft \mathbb{T} \text{ is equal to the ideal} \]

\[ \left( (2, 1, 1)^\mathbb{Z} \right) \cap \mathbb{T} = \left\{ (a, b_1 + b_2 \sqrt{2}, c_1 + c_2 \sqrt{3}) \in \mathbb{T} \mid a \in 2\mathbb{Z} \right\}, \]

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

\[ \text{(ii) } m_2^n \text{ is not principal for any } n \geq 1. \]

\[ \text{(iii) } T_{m_2} \text{ is not Gorenstein.} \]

\[ \text{Proof.} \quad \text{(i) The uniqueness of the maximal ideal of residue characteristic } 2 \text{ implies that it must be the Eisenstein maximal ideal } m_2. \text{ To prove the uniqueness, note that each of the rings } \mathbb{Z}, \mathbb{Z}[\sqrt{2}], \mathbb{Z}[\sqrt{3}] \text{ has a unique maximal ideal of residue characteristic } 2; \text{ these are generated by } 2, \sqrt{2}, \text{ and } 1 + \sqrt{3}, \text{ respectively. One easily checks that} \]

\[ m := ((2, 1, 1)^\mathbb{Z}) \cap \mathbb{T} = ((1, \sqrt{2}, 1)^\mathbb{Z}) \cap \mathbb{T} = ((1, 1, 1 + \sqrt{3})^\mathbb{Z}) \cap \mathbb{T}, \]

\[ \text{and } \mathbb{T}/m \cong \mathbb{F}_2. \]

\[ \text{(ii) To prove this statement it is enough to observe that } (1, 0, 0) \in (2, 1, 1)^\mathbb{Z} \text{ is in } \text{End}_\mathbb{T}(m_2^2) \text{ but } (1, 0, 0) \not\in \mathbb{T}. \]

\[ \text{(iii) We apply } [23] \text{ Prop. 1.4 (iii): Let } \bar{m}_2 \text{ denote the image of } m_2 \text{ in } \mathbb{T}/2\mathbb{T}. \text{ Then } T_{m_2} \text{ is Gorenstein if and only if } \dim_{\mathbb{F}_2}(\mathbb{T}/2\mathbb{T})[\bar{m}_2] = 1. \text{ Note that } (2, 0, 0) \text{ and } (0, 2, 0) \text{ have distinct non-zero images in } \mathbb{T}/2\mathbb{T}, \text{ since otherwise } (2, 2, 0) \in 2\mathbb{T}, \text{ which would imply } (1, 1, 0) \in \mathbb{T}. \text{ On the other hand, for any } \theta \in m_2 \text{ we have } \theta(2, 0, 0) = (4a, 0, 0) = 2(2a, 0, 0) \in 2\mathbb{T} \text{ for some } a \in \mathbb{Z}. \text{ Therefore, } \bar{m}_2 \text{ annihilates } (2, 0, 0), \text{ and similarly } \bar{m}_2 \text{ annihilates } (0, 2, 0); \text{ thus, } \dim_{\mathbb{F}_2}(\mathbb{T}/2\mathbb{T})[\bar{m}_2] \geq 2. \]

\[ \square \]
Proposition 4.1. Let \( C \subseteq \mathbb{Q} \) and \( q \) be the divisor classes of \([1] - [p] \) and \([1] - [q] \) in \( J_0(pq) \). Denote \( C := C(pq) \).

(i) \( C \) 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 \( C \) is \( 14c_p = 6c_q \). This implies \( C \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} \).

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

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

\[
0 \to (c_q) \to C \xrightarrow{\varphi_p} \Phi(p) \to \mathbb{Z}/3\mathbb{Z} \to 0.
\]

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

\[
0 \to (c_p) \to C \xrightarrow{\varphi_q} \Phi(q) \to 0.
\]

Proof. (i) follows from [2]. The groups \( \Phi(p) \) and \( \Phi(q) \) can be computed from the structure of special fibres 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 fibre of the minimal regular model of \( X_0(pq) \) over \( \mathbb{Z}_p \), one can determine the homomorphism \( \varphi_p \) and \( \varphi_q \); cf. [18] p. 1161.

Proposition 4.2. We have \( C = J(\mathbb{Q})_{\text{tor}} \).

Proof. Obviously \( C \subseteq J(\mathbb{Q})_{\text{tor}} \). On the other hand, \( J \) has good reduction at any odd prime \( p \nmid 65 \), so by Proposition [2, 7] we have an injective homomorphism \( J(\mathbb{Q})_{\text{tor}} \mapsto J(\mathbb{F}_p) \), where \( J(\mathbb{F}_p) \) denotes the group of \( \mathbb{F}_p \)-rational points on the reduction of \( J \) at
The order of \(J(\mathbb{F}_p)\) can be computed using Magma. We have \(#J(\mathbb{F}_3) = 2^4 \cdot 3^2 \cdot 7\) 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 \(T\) 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 \(T\) is the full ring of endomorphisms of \(J\) (this can be proved as in [13, Prop. 9.5]). For a maximal ideal \(m \triangleleft T\), we denote

\[
J[m] = \bigcap_{\alpha \in m} \ker(J \rightarrow \alpha J)
\]

Then \(J[m] \subset J[p]\), where \(p\) is the characteristic of \(T/m\). By a theorem of Mazur [23, p. 341], \(T_m\) is Gorenstein if and only if \(\dim_{T/m} J[m] = 2\). Therefore, using Proposition [4.1] we conclude that \(\dim_{T/m} J[m] = 2\) for any maximal ideal \(m\) of odd residue characteristic.

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

\[
0 \rightarrow \mathbb{Z}/p\mathbb{Z} \rightarrow J[m_p] \rightarrow \mu_p \rightarrow 0,
\]

since \(G_\mathbb{Q}\) acts on \(J[m_p]\) by the mod \(p\) cyclotomic character; cf. [22, p. 465]. By [12], the Shimura subgroup \(\Sigma = (=\text{kernel of the functorial homomorphisms } J_0(65) \rightarrow J_1(65))\) is

\[
\Sigma \cong \mu_2 \times \mu_3,
\]

and the Eisenstein ideal \(E\) annihilates \(\Sigma\). Therefore, (4.1) splits for \(p = 3\):

\[
J[m_3] = \mathcal{C}_3 \times \Sigma_3 \cong \mathbb{Z}/3\mathbb{Z} \times \mu_3.
\]

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

**Proof.** If (4.1) splits then \(\mathbb{Z}/\mathbb{Q} \times \mathbb{Z}/\mathbb{Q} \subset J(\mathbb{Q}(\mu_7))_{\text{tor}}\). Since \(\ell = 29\) splits completely in \(\mathbb{Q}(\mu_7)\), by Proposition [2.1] we must have \(\ell^2 \mid #J(\mathbb{F}_7) = 2^3 \cdot 3 \cdot 7 \cdot 13 \cdot 23^2\).

**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

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

By Table 1 in [5], \(E\) is isomorphic to a subvariety of \(J\). We claim that \(E[2] \subset J[m_2]\). 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 \(m_2\) is Eisenstein implies that \(a_p \equiv (p + 1)\) is even; thus, \(T_p \equiv (p + 1)\) annihilates \(E[2]\); thus \(m_2 = (2, E)\) annihilates \(E[2]\). On the other hand, clearly \(E[2] \not\cong \mathcal{C}[2]\), as \(\mathcal{C}[2]\) is constant. Therefore, \(\dim_{\mathbb{Z}/m_2} J[m_2] \geq \dim_{\mathbb{Z}/2} \mathcal{C}[2] + 1 = 3\). This gives a geometric proof of the fact that \(T_{m_2}\) 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 \(m \triangleleft T\) be an Eisenstein maximal ideal of odd residue characteristic \(p\). Let \(H \subset J[m^s]\), \(s \geq 1\), be a \(T(G_\mathbb{Q})\)-module. If \(J[m] \not\subset H\), then \(H \subseteq J[m]\).
Proof. We will assume that $J[m] \nsubseteq H$ and $H \nsubseteq J[m]$, and reach a contradiction. First, we make some simplifications. Since $H[m^2] \subset J[m^2]$ is a $T[G_Q]$-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 $H \subset J[m^2]$.

**Lemma 4.6.** We have $H \cong T/m^2$.

Proof. We can consider $H$ as a finite $T_m$-module. Since $T_m$ is a DVR, we have

$$H \cong T_m/m^{s_1} \times \cdots \times T_m/m^{s_r} \cong T/m^{s_1} \times \cdots \times T/m^{s_r}$$

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

Note that

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

Let $K := Q(H)$. If $K = Q$, then $p^2 = \#H$ divides $\#J(Q)_{\text{tor}}$. This contradicts Proposition 4.7, so we will assume from now on that $K \neq Q$. Let $\eta$ be a generator of $m$. Note that $\eta H = H[\eta] \subset J[m]$ is a proper non-trivial Galois invariant subgroup. On the other hand, the $G_Q$-invariant subgroups of $J[m]$ are $\Z/p\Z$ and $\mu_p$, so either

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

or

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

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 $Q$ contained in $Q(\mu_{p^2})$.

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

Proof. Since the actions of $T$ and $G_Q$ on $H$ commute, we have

$$\Gal(K/Q) \subset \Aut_T(T/m^2) \cong (T/m^2)^\times \cong \Z/(p-1)p\Z.$$ 

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

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

Assume $p = 7$. Since in this case $H$ is as in (4.3), $G_Q$ acts trivially on $pH$, so $\Gal(K/Q)$ is in the subgroup of units $(\Z/p^2\Z)^\times$ 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 $(\Z/p^2\Z)^\times$. Hence $K/Q$ 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 $\Gal(Q(\mu_{5^n_2})/Q) \times \Gal(Q(\mu_{13^n_3})/Q)$. Therefore, $K \subset Q(\mu_{p^n_1})$ is a subfield of
degree $p$ over $\mathbb{Q}$. There is a unique such field (as $\text{Gal}(\mathbb{Q}(\mu_{p^n 2}/\mathbb{Q})$ 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

$$\text{Gal}(\mathbb{Q}(\mu_{p^n 1}, \mu_{5p^2}, \mu_{13^n 3})/F) \cong \mathbb{Z}/(p - 1)p^{n_1 - 1} \times \mathbb{Z}(5 - 1)5^{n_2 - 1} \times \mathbb{Z}/13^{n_3 - 1}\mathbb{Z},$$

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

Finally, assume $p = 3$ and $\ell$ fits into an exact sequence (4.3). 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,

$$\text{Gal}(\mathbb{Q}(\mu_{p^n 1}, \mu_{5p^2}, \mu_{13^n 3})/FL) \cong \mathbb{Z}/p^{n_1 - 1} \times \mathbb{Z}(5 - 1)5^{n_2 - 1} \times \mathbb{Z}/13^{n_3 - 1}\mathbb{Z}.$$

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

Assume $p = 7$. By Lemma 4.7, we have $K = K_p$. Let $\ell$ be a prime which splits completely in $K_p$. Then $H$ is constant over $\mathbb{Q}_\ell$, so $H \subset J(\mathbb{Q}_\ell)_{\text{tor}}$. On the other hand, under the canonical reduction map, we have an injection $J(\mathbb{Q}_\ell)_{\text{tor}} \to J(\mathbb{F}_\ell)$; see Proposition 2.1. Therefore, we must have $p^2 | \# J(\mathbb{F}_\ell)$. It is easy to show that a prime $\ell$ 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 $3 \equiv 31$. These are $\{31, 30, 48, 18, 19, 1\}$. Thus, the smallest prime that splits completely in $K_7$ is 19, and $\# J(\mathbb{F}_{19})$ is prime, and $\# J(\mathbb{F}_{19}) = 2^3 \cdot 3^2 \cdot 7 \cdot 13 \cdot 2^3$. Since $7^2$ 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 $\mu_p$ is constant over $K'$, we have $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \cong J(K')/m \subset J(K')_{\text{tor}} \subset J(\mathbb{Q}_\ell)$. 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 $J(m) \not\subset H$, we see that $J(\mathbb{Q}_\ell)$ contains a subgroup isomorphic to $(\mathbb{Z}/p^2\mathbb{Z})^\times$. As earlier, it implies that $p^3 | \# J(\mathbb{Q}_\ell)$. A prime $\ell$ splits completely in $K' := \mathbb{Q}(\mu_{13}, \mu_{p^2})$ if and only if $\ell \equiv 1$ (mod 9) and $\ell \equiv 1$ (mod 13). The smallest such prime is $\ell = 937$, and $\# J(\mathbb{F}_{937}) = 2^3 \cdot 3^2 \cdot 7 \cdot 11^2 \cdot 41 \cdot 97 \cdot 2963$. Since $3^3$ does not divide this number, we get a contradiction. This concludes the proof of Proposition 4.5. □

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

Since $m$ has odd residue characteristic, the $T(\mathbb{Q}_T)$-module $J(m)$ is 2-dimensional over $T/m$. By [13 Prop. 14.2] and [22 Thm. 5.2], if $m$ is not Eisenstein, then $J(m)$ is irreducible. Since $J(m) \cap H \neq 0$, we must have $J(m) \subset H$, which contradicts our assumption on $\pi$. Hence $H$ is supported on the Eisenstein maximal ideals $m_3$ and $m_7$. 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 $H_p \subset J[m_p^s]$ for some $s \geq 1$, $p = 3, 7$, and $J[m_p] \not\subset H_p$. Applying Proposition 4.10 we conclude that $H_p \not\subset J[m_p]$. Thus $H_7 = 0$ or $C_7$, and $H_3 = 0$ or $\Sigma_3$ or $C_3$. Overall, $H$ can be one of the following subgroups of $J$:

\[(4.5) \quad 0, \quad C_3, \quad \Sigma_3, \quad C_7, \quad C_3 \times C_7, \quad \Sigma_3 \times C_7.\]

**Theorem 4.8.** If $A = J'$, then for $\pi : J \to J'$ chosen with the minimality condition discussed above, we must have $H = C_7$.

**Proof.** The reductions of $J$ and $J'$ at $p = 5$ or $13$ are purely toric, cf. [10], [22]. Let $\Phi(5)'$ and $\Phi(13)'$ be the component groups of $J'$ at $5$ and $13$. We have (see [10, p. 214]):

\[\Phi(5)' \cong \mathbb{Z}/6\mathbb{Z}, \quad \Phi(13)' \cong \mathbb{Z}/42\mathbb{Z}.\]

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 $(\Phi(p)''_{\text{odd}} \cong (\Phi(p)'_{\text{odd}}$. On the other hand, since we know the image and kernel of $\varphi_p : C \to \Phi(p)$, we can compute $\#(\Phi(p)''_{\text{odd}}$ for each possible $H$ from the list \([4.3]\) using Lemma \([2.3]\). This simple calculation shows that the only possible $H$ is $C_7$. (Note that the group scheme $\Sigma_3$ becomes constant over an unramified extension of $\mathbb{Q}_p$, but it is not important to know whether $\varphi_p : \Sigma_3 \to \Phi(p)$ is injective or trivial; neither of these possibilities gives the correct $\Phi(p)''$ if $\Sigma_3 \subset H$.)

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

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

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

\[C \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}, \quad \Sigma \cong \mu_4 \times \mu_3.\]

There is a unique Eisenstein maximal ideal $m_3 \triangleleft T$ of odd residue characteristic. There is a unique $Q$-isogeny class of elliptic curves of level 35. The optimal curve is [35, 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 $T_m$ is Gorenstein for any maximal ideal $m \triangleleft T$ (as $T$ is monogenic), $J[m]$ is two dimensional over $T/m$, so $J[m_3] = E[3] = C_3 \times \Sigma_3$. Now it is easy to analyze all $T[G_{\mathbb{Q}}]$-submodules of $J$ supported on $m_3$. 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 $\ker(\pi)_{\text{odd}} = 0$. Ogg’s conjecture in this case predicts that $\ker(\pi) \cong \mathbb{Z}/2\mathbb{Z} \subset C_2$.

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

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

We have

\[C \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}, \quad \Sigma \cong \mu_4.\]
There is a unique Eisenstein maximal ideal \( m_7 \triangleleft \mathbb{T} \) of odd residue characteristic. \( J'[m] \) fits into the exact sequence \( 1 \), which is non-split in this case. One can classify \( \mathbb{T}[G_0] \)-submodules of \( J \) supported on \( m_7 \) using an argument similar to the argument we used in Proposition \( 1.3 \). Finally, one deduces as in Theorem \( 1.8 \) that there is a Ribet isogeny \( \pi : J \to J' \) with \( \ker(\pi)_{\text{odd}} = C_7 \cong \mathbb{Z}/7\mathbb{Z} \). Ogg’s conjecture in this case predicts that \( \ker(\pi) = C_7 \).

Acknowledgements. 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] S. Bosch, W. Lütkebohmert, and M. Raynaud, Néron models, Springer-Verlag, 1990.
[2] S.-K. Chua and S. Ling, On the rational cuspidal subgroup and the rational torsion points of \( J_0(pq) \), Proc. Amer. Math. Soc. 125 (1997), 2255–2263.
[3] B. Conrad and W. Stein, Component groups of purely toric quotients, Math. Res. Lett. 8 (2001), 745–766.
[4] D. Cox, Primes of the form \( x^2 + ny^2 \), second ed., Pure and Applied Mathematics (Hoboken), John Wiley & Sons, Inc., Hoboken, NJ, 2013, Fermat, class field theory, and complex multiplication.
[5] J. Cremona, Algorithms for modular elliptic curves, second ed., Cambridge University Press, Cambridge, 1997.
[6] J. González and S. Molina, The kernel of Ribet’s isogeny for genus three Shimura curves, J. Math. Soc. Japan 68 (2016), no. 2, 609–655.
[7] J. González and V. Rotger, Equations of Shimura curves of genus two, Int. Math. Res. Not. (2004), no. 14, 661–674.
[8] A. Grothendieck, Modèles de Néron et monodromie, SGA 7, Exposé IX, 1972.
[9] D. Helm, On maps between modular Jacobians and Jacobians of Shimura curves, Israel J. Math. 160 (2007), 61–117.
[10] B. Jordan and R. Livné, On the Néron model of Jacobians of Shimura curves, Compositio Math. 60 (1986), no. 2, 227–236.
[11] N. Katz, Galois properties of torsion points on abelian varieties, Invent. Math. 62 (1981), no. 3, 481–502.
[12] S. Ling and J. Oesterlé, The Shimura subgroup of \( J_0(N) \), Astérisque (1991), no. 196-197, 171–203. Courbes modulaires et courbes de Shimura (Orsay, 1987/1988).
[13] B. Mazur, Modular curves and the Eisenstein ideal, Inst. Hautes Études Sci. Publ. Math. 47 (1977), 33–186.
[14] J.-F. Michon, Courbes de Shimura hyperelliptiques, Bull. Soc. Math. France 109 (1981), no. 2, 217–225.
[15] D. 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.
[16] A. Ogg, Mauvaise réduction des courbes de Shimura, Séminaire de théorie des nombres, Paris 1983–84, Progr. Math., vol. 59, Birkhäuser, 1985, pp. 199–217.
[17] M. Ohta, Eisenstein ideals and the rational torsion subgroups of modular Jacobian varieties II, Tokyo J. Math. 37 (2014), no. 2, 273–318.
[18] M. Papikian, On Jacquet-Langlands isogeny over function fields, J. Number Theory 131 (2011), no. 7, 1149–1175.
[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.
[20] K. Ribet, Sur les variétés abéliennes à multiplications réelles, C. R. Acad. Sci. Paris Sér. A-B 291 (1980), A121–A123.
[21] K. Ribet, *On the component groups and the Shimura subgroup of $J_0(N)$*, Séminaire de Théorie des Nombres, 1987–1988 (Talence, 1987–1988), Univ. Bordeaux I, Talence, 1987/1988, pp. Exp. No. 6, 10.

[22] K. Ribet, *On modular representations of $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ arising from modular forms*, Invent. Math. **100** (1990), 431–476.

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

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

Department of Mathematics, Queens College, City University of New York, 65-30 Kissena Blvd Flushing, NY 11367, USA
E-mail address: kklosin@qc.cuny.edu

Department of Mathematics, Pennsylvania State University, University Park, PA 16802, USA
E-mail address: papikian@psu.edu