EXTENSIONS OF ELLIPTIC CURVES AND CONGRUENCES BETWEEN MODULAR FORMS

MATTHEW A. PAPANIKOLAS AND NIRANJAN RAMACHANDRAN

ABSTRACT. We study the group $\mathrm{Ext}^1_K(A, B)$ where A and B are abelian varieties over a number field K. In particular, if $K = \mathbb{Q}$, we relate $\mathrm{Ext}^1_{\mathbb{Q}}(A, B)$ to congruences between modular forms.

1. INTRODUCTION

J. Milne [11, 12] has established striking connections between arithmetic and the extensions of abelian varieties over finite fields. Our aim here is to consider extensions of abelian varieties over number fields and connect them to arithmetic. Specifically, we find that extensions of elliptic curves are an apt tool for encoding congruences between modular forms.

For abelian varieties A and B over a field K, we consider the group $\mathrm{Ext}^1_K(A, B)$ of isomorphism classes of Yoneda extensions of A by B in the category of commutative group schemes over K. This group is torsion by the Poincaré reducibility theorem, but it need not be finite. For instance, if A and B are non-isogenous elliptic curves over $K = \mathbb{C}$, then $\mathrm{Ext}^1_{\mathbb{C}}(A, B) \cong (\mathbb{Q}/\mathbb{Z})^4$. Moreover, if A is an elliptic curve with complex multiplication over $\mathbb{C}$, then a beautiful result of S. Lichtenbaum [16, Thm. 6.1] states that $\mathrm{Ext}^1_{\mathbb{C}}(A, A)$ is naturally isomorphic to the torsion subgroup of $A(\mathbb{C})$.

In the case of a finite field $K = \mathbb{F}_q$, Milne [11] has shown that $\mathrm{Ext}^1_{\mathbb{F}_q}(A, B)$ is finite and also computed its order. These results are key to his work [12, 13] on the conjecture of Birch and Swinnerton-Dyer and the geometric analogue of Artin-Tate. The point is, as he shows, that certain Tate-Shafarevich and Brauer groups can be identified with suitable Ext-groups. Furthermore, his formula [11, Thm. 1] for the order of $\mathrm{Ext}^1_{\mathbb{F}_q}(A, B)$ has now been reinterpreted as a special value of an L-function and extended to integral motives [15].

We are naturally led to ask: *If A and B are abelian varieties over a number field K, how is $\mathrm{Ext}^1_K(A, B)$ related to the arithmetic of A and B?* Our main results provide some answers.

Theorem 1 (Milne-Ramachandran). *Let A and B be abelian varieties over a number field K. Then $\mathrm{Ext}^1_K(A, B)$ is finite.*

The next three results provide a unifying way to connect congruences between modular forms to extensions of abelian varieties over $\mathbb{Q}$.

Theorem 2. *Let A and B be non-isogenous elliptic curves over $\mathbb{Q}$ of conductors M and N respectively. Let $f = \sum a_n q^n$ and $g = \sum b_n q^n$ be their associated normalized*

Research of the first author partially supported by an NSA grant.

newforms [2, 26]. *Then, for any integer n with* $\gcd(n, 2MN) = 1$,

$$a_n \equiv b_n \pmod{e},$$

where e is the exponent of $\operatorname{Ext}^1_{\mathbb{Q}}(A, B)$.

Let A be an elliptic curve over $\mathbb{Q}$ of conductor N, and let $\phi_A : X_0(N) \to A$ realize A as an optimal quotient of the modular curve $X_0(N)$, i.e. A is a strong Weil curve. The kernel C of the induced map $J_0(N) \twoheadrightarrow A$ is an abelian variety over $\mathbb{Q}$, and there is an exact sequence

$$\eta : \quad 0 \to C \to J_0(N) \to A \to 0.$$

Let d_A be the degree of the modular parametrization ϕ_A, and let r_A be the restricted congruence modulus of A which measures congruences away from $2N$ (see §4). There is a strong relation between d_A, r_A, and the exponent e_A of $\operatorname{Ext}^1_{\mathbb{Q}}(A, C)$.

Theorem 3. *Let $A/\mathbb{Q}$ be an elliptic curve which is an optimal quotient of $J_0(N)$. Then*

$$d_A \mid e_A \mid r_A.$$

In general, e_A does not divide the congruence modulus m_A of A (see §4). The analogous result for m_A requires a refinement of $\operatorname{Ext}^1_{\mathbb{Q}}(A, C)$, which involves the Hecke algebra $\mathbb{T} = \mathbb{Z}[T_1, T_2, \ldots]$ associated with $J_0(N)$. Namely, let $\operatorname{Ext}^1_{\mathbb{Q},\mathbb{T}}(A, C)$ be the Yoneda Ext-group in the category of commutative $\mathbb{T}$-group schemes over $\mathbb{Q}$, i.e. groups G together with a homomorphism $\mathbb{T} \to \operatorname{End}_{\mathbb{Q}}(G)$. Write $e_{A,\mathbb{T}}$ for the exponent of $\operatorname{Ext}^1_{\mathbb{Q},\mathbb{T}}(A, C)$.

Theorem 4. *Let $A/\mathbb{Q}$ be an elliptic curve which is an optimal quotient of $J_0(N)$. Then*

$$d_A \mid e_{A,\mathbb{T}} \mid m_A.$$

We will show that the forgetful map $\operatorname{Ext}^1_{\mathbb{Q},\mathbb{T}}(A, C) \to \operatorname{Ext}^1_{\mathbb{Q}}(A, C)$ is injective, and thus $e_{A,\mathbb{T}} \mid e_A$. Also, since d_A is expected to be unbounded [27, §6], Theorems 3 and 4 suggest that the order of $\operatorname{Ext}^1_{\mathbb{Q}}(A, C)$ is unbounded.

These results indicate that extensions provide a convenient way to encode congruences between modular forms. Also, they suggest a way to generalize the theory of congruences due to H. Hida [8] and K. Ribet [18], even in the absence of Fourier coefficients.

We should expect that $\operatorname{Ext}^1_K(A, B)$ is also related to the special values of L-functions. The group $\operatorname{Ext}^1_K(A, B)$ of Theorem 1 is a variant of $\operatorname{Ext}^1_K(A, \mathbb{G}_m)$ which, by the Weil-Barsotti formula, is the group $A^*(K)$ of rational points on the dual abelian variety A^*. Moreover, the rank of $A^*(K)$ and the order of the torsion subgroup of $A^*(K)$ appear in the Birch and Swinnerton-Dyer conjecture for A.

Hida [8] has related congruence moduli to special values of L-functions, and with this in mind the order of $\operatorname{Ext}^1_K(A, B)$ should be related to a special value of the L-function $L(A^* \otimes B, s)$ (as in [15]). For example, for an elliptic curve A over $\mathbb{Q}$ the order of $\operatorname{Ext}^1_{\mathbb{Q}}(A, A)$ appears in the denominator of the special value of $L(\operatorname{Sym}^2 A, s)$ at $s = 2$ (cf. [7, Eq. (2)]). We plan to pursue these relationships in a future paper.

Acknowledgements. We thank J. Milne for graciously allowing the unpublished proof of Theorem 1 to be included here. We also thank S. Lichtenbaum, G. Pappas, and J. Teitelbaum for their helpful remarks and suggestions.

2. Extensions over number fields

For any abelian group (scheme) G, let G_n denote the kernel of multiplication by the integer n. For a prime p, let $T_pG = \varprojlim G_{p^m}$ denote the associated Tate module.

Proof of Theorem 1. Let A and B be two abelian varieties over a number field K. For any integer n, taking $\mathrm{Ext}^i_K(-,B)$ of the Kummer sequence

$$0 \to A_n \to A \xrightarrow{n} A \to 0$$

gives a short exact sequence of abelian groups

$$(1) \qquad 0 \to \mathrm{Hom}_K(A,B) \otimes \mathbb{Z}/n\mathbb{Z} \to \mathrm{Hom}_K(A_n, B_n) \to \mathrm{Ext}^1_K(A,B)_n \to 0,$$

where in the middle term we have used that $\mathrm{Hom}_K(A_n, B) = \mathrm{Hom}_K(A_n, B_n)$.

This simple sequence (1) is fundamental to our discussion: it shows that the Ext-group is the appropriate tool to encode congruences of mod p Galois representations which do not come from global maps.

Taking the inverse limit of (1) over powers $n = p^m$ of a prime p and using that $\mathrm{Hom}_K(A_{p^m}, B_{p^m}) = \mathrm{Hom}_K(T_pA, B_{p^m})$, we have an exact sequence

$$(2) \qquad 0 \to \mathrm{Hom}_K(A,B) \otimes \mathbb{Z}_p \to \mathrm{Hom}_K(T_pA, T_pB) \to T_p\,\mathrm{Ext}^1_K(A,B) \to 0.$$

Faltings' theorem [6] implies that the first homomorphism in (2) is in fact an isomorphism, and so $T_p\,\mathrm{Ext}^1_K(A,B) = 0$ for all primes p. From (1), we see that $\mathrm{Ext}_K(A,B)_n$ is finite for all n. Thus the p-primary subgroup of $\mathrm{Ext}^1_K(A,B)$ is finite for all p.

Now by [10, Cor. 1], there is a constant $c = c(A,B)$ so that for all primes $p > c$,

$$\mathrm{Hom}_K(A,B) \otimes \mathbb{Z}/p\mathbb{Z} \cong \mathrm{Hom}_K(A_p, B_p).$$

Taking $n = p$ in (1) gives $\mathrm{Ext}^1_K(A,B)_p = 0$ for all $p > c$. This proves Theorem 1. $\square$

Remark. In the case of elliptic curves over $\mathbb{Q}$, the results of J.-P. Serre [20] provide upper bounds on the order of $\mathrm{Ext}^1_{\mathbb{Q}}(A,B)$.

Remark. Theorem 1 should also hold for pure integral motives [15], [21, p. 387] of equal weight and defined over a number field. This would follow from the properties expected of mixed motives such as semisimplicity of the category of pure isomotives, the adelic Tate conjecture [15, Lem. 3.1], and the conjecture [21, Conj. 10.10] of Serre.

3. Linking extensions over number fields and finite fields

Let A and B be abelian varieties over $\mathbb{Q}$. Let $N > 1$ be the least integer such that both A and B extend to abelian schemes (denoted $\mathcal{A}$ and $\mathcal{B}$) over $\mathbb{Z}[\frac{1}{N}]$. Let $S = 2N$, and take $\mathrm{Ext}^1_{\mathbb{Z}[1/S]}(\mathcal{A}, \mathcal{B})$ for the Ext-group in the category of commutative group schemes over $\mathbb{Z}[\frac{1}{S}]$. The change from N to S is due to the special nature of $p = 2$ and will be explained below.

If $p \geq 3$ is a prime with $p \nmid N$, then both A and B have good reduction at p. Let $\widetilde{A}$ and $\widetilde{B}$ denote the corresponding abelian varieties over $\mathbb{F}_p$. For any positive integer n, we obtain a commutative diagram from (1) with exact rows

$$\begin{tikzcd} 0 \arrow[r] & \mathrm{Hom}_{\mathbb{Q}}(A,B)\otimes\mathbb{Z}/n\mathbb{Z} \arrow[r] & \mathrm{Hom}_{\mathbb{Q}}(A_n,B_n) \arrow[r] & \mathrm{Ext}^1_{\mathbb{Q}}(A,B)_n \arrow[r] & 0 \\ 0 \arrow[r] & \mathrm{Hom}_{\mathbb{Z}[\frac{1}{S}]}(\mathcal{A},\mathcal{B})\otimes\mathbb{Z}/n\mathbb{Z} \arrow[r] \arrow[u, "a", "\wr"'] \arrow[d, "h"] & \mathrm{Hom}_{\mathbb{Z}[\frac{1}{S}]}(\mathcal{A}_n,\mathcal{B}_n) \arrow[r] \arrow[u, "b", "\wr"'] \arrow[d, "i"] & \mathrm{Ext}^1_{\mathbb{Z}[\frac{1}{S}]}(\mathcal{A},\mathcal{B})_n \arrow[r] \arrow[u, "c", "\wr"'] \arrow[d, "j"] & 0 \\ 0 \arrow[r] & \mathrm{Hom}_{\mathbb{F}_p}(\widetilde{A},\widetilde{B})\otimes\mathbb{Z}/n\mathbb{Z} \arrow[r] & \mathrm{Hom}_{\mathbb{F}_p}(\widetilde{A}_n,\widetilde{B}_n) \arrow[r] & \mathrm{Ext}^1_{\mathbb{F}_p}(\widetilde{A},\widetilde{B})_n \arrow[r] & 0. \end{tikzcd} \tag{3}$$

The middle row is obtained by the analogue of (1) using $0 \to \mathcal{A}_n \to \mathcal{A} \to \mathcal{A} \to 0$ [14, §II.5]. The vertical maps are the natural restriction maps. Now, a is an isomorphism by the Néron mapping property of $\mathcal{A}$ and $\mathcal{B}$; b is an isomorphism by [23, Cor. of Thm. 4.5.1] applied to the commutative finite flat group schemes $\mathcal{A}_n$, $\mathcal{B}_n$; it follows that c is an isomorphism.

Put $\alpha = h \circ a^{-1}$, $\beta = i \circ b^{-1}$, and $\gamma = j \circ c^{-1}$. It is important to note that

$$\beta : \mathrm{Hom}_{\mathbb{Q}}(A_n, B_n) \to \mathrm{Hom}_{\mathbb{F}_p}(\widetilde{A}_n, \widetilde{B}_n)$$

is injective: if $\gcd(n,p) = 1$, this is clear; and if $n = p^r$, this follows from the faithful nature of the functor $G \rightsquigarrow G \times_{\mathbb{Z}_p} \mathbb{F}_p$ which maps commutative finite flat group schemes over $\mathbb{Z}_p$ of p-power order to their special fiber (see the discussion following Example 4.3 on p. 409 of [3]). The injectivity of β provides an exact sequence

$$0 \to \ker(\gamma) \to \operatorname{coker}(\alpha) \to \operatorname{coker}(\beta) \to \operatorname{coker}(\gamma) \to 0. \tag{4}$$

Let us also record the following observation, which follows from (3).

Proposition 5. *The natural map*

$$\mathrm{Ext}^1_{\mathbb{Z}[\frac{1}{S}]}(\mathcal{A},\mathcal{B}) \to \mathrm{Ext}^1_{\mathbb{Q}}(A,B)$$

is an isomorphism.

Remark. Some parts of this discussion can be generalized to other number fields.

Let us explain the reason for the switch from N to S (harmless if N is already even). Assume that N is odd, i.e. that 2 is a prime of good reduction for A and B. We have used implicitly that the absolute ramification index e of $\mathbb{Z}_p$ satisfies the condition $e < p - 1$; this fails only when $p = 2$.

In general for odd N, the map $\mathrm{Ext}^1_{\mathbb{Z}[1/N]}(\mathcal{A},\mathcal{B}) \to \mathrm{Ext}^1_{\mathbb{Q}}(A,B)$ may not be an isomorphism. However, it is injective, because the map $\mathrm{Hom}_{\mathbb{Z}[1/N]}(\mathcal{A}_n,\mathcal{B}_n) \to \mathrm{Hom}_{\mathbb{Q}}(A_n,B_n)$ is injective. Given that a is an isomorphism over $\mathbb{Z}[\frac{1}{N}]$ by the Néron mapping property and that b is injective over $\mathbb{Z}[\frac{1}{S}]$, it suffices to check that the map $\mathrm{Hom}_{\mathbb{Z}_2}(\mathcal{A}_n,\mathcal{B}_n) \to \mathrm{Hom}_{\mathbb{Q}_2}(A_n,B_n)$, with $n = 2^r$ a power of 2, is injective. This is clear [23, p. 152]. Thus, the Ext-group over $\mathbb{Z}[\frac{1}{N}]$ might be smaller, and so the analogue of Theorem 2 will be weaker.

In addition, the definition of β over $\mathbb{Z}[\frac{1}{N}]$ is problematic, due to the non-exactness of the Néron model functor for $p = 2$ (see [1, Ex. 4, p. 190] for a counterexample to [1, Thm. 4, p. 187]).

Proof of Theorem 2. We shall proceed by combining the previous discussion with Milne's work on Ext-groups. As f and g are Hecke eigenforms, it suffices to show that $a_p \equiv b_p \pmod{e}$ for all primes p with $p \nmid 2MN$. We consider the non-trivial case that $a_p \neq b_p$. This implies that

$$\mathrm{Hom}_{\mathbb{F}_p}(\widetilde{A}, \widetilde{B}) = 0,$$

and so from (3), (4), and Theorem 1, it follows that the natural map

$$\gamma : \mathrm{Ext}^1_{\mathbb{Q}}(A, B) \hookrightarrow \mathrm{Ext}^1_{\mathbb{F}_p}(\widetilde{A}, \widetilde{B})$$

is injective. The following lemma is an application of Milne's formula [11, Thm. 3].

Lemma 6. *For non-isogenous elliptic curves E, E' over a finite field $\mathbb{F}$, we have* $\#\,\mathrm{Ext}^1_{\mathbb{F}}(E, E') = (\#E(\mathbb{F}) - \#E'(\mathbb{F}))^2$.

Thus, continuing with the proof of Theorem 2, it follows that

$$\#\,\mathrm{Ext}^1_{\mathbb{F}_p}(\widetilde{A}, \widetilde{B}) = (a_p - b_p)^2.$$

Moreover, Milne [12] has shown that

$$\mathrm{Ext}^1_{\mathbb{F}_p}(\widetilde{A}, \widetilde{B}) \cong Ш(\widetilde{B}/L),$$

where $Ш(\widetilde{B}/L)$ is the Tate-Shafarevich group of the constant elliptic curve $\widetilde{B}$ over the global function field $L := \mathbb{F}_p(\widetilde{A})$. Moreover, since A and B are elliptic curves, we know via the Cassels-Tate pairing that

$$Ш(\widetilde{B}/L) \cong T \times T,$$

for some abelian group T. Thus the exponent e of $\mathrm{Ext}^1_{\mathbb{F}_p}(\widetilde{A}, \widetilde{B})$ divides $\#T = |a_p - b_p|$. Combining this information with the injectivity of γ, we see that

$$e \mid (a_p - b_p), \quad \forall p \nmid 2MN,$$

thus finishing the proof of Theorem 2. □

Remark. V. Vatsal [25, Cor. 1.11] has shown how congruences, like those in Theorem 2, can often be translated into congruences for the algebraic part of the values at $s = 1$ of $L(s, f, \chi)$ and $L(s, g, \chi)$; see [25] for notation and details. Thus, non-triviality of $\mathrm{Ext}_{\mathbb{Q}}(A, B)$ can be linked with congruences of special values of the associated L-functions.

4. Modular parametrizations and congruence moduli

Let $J_0(N)$ be the Jacobian of the modular curve $X_0(N)$ over $\mathbb{Q}$, and let $S_2(\Gamma_0(N))$ be the space of weight two cusp forms on $\Gamma_0(N)$. For an elliptic curve A over $\mathbb{Q}$ of conductor N, let $f = \sum a_n q^n \in S_2(\Gamma_0(N))$ be its associated normalized newform. The *congruence modulus of* A [27, §5] is

$$m_A := \max\left\{ m \in \mathbb{Z} \;\middle|\; \begin{array}{c} \exists g = \sum b_n q^n \in (f)^\perp \cap \mathbb{Z}[\![q]\!] \text{ so that} \\ b_n \equiv a_n \pmod{m} \text{ for all } n \end{array} \right\},$$

where $(f)^\perp \subseteq S_2(\Gamma_0(N))$ is the orthogonal complement with respect to the Petersson inner product. The *restricted congruence modulus of* A is

$$r_A := \max\left\{ r \in \mathbb{Z} \;\middle|\; \begin{array}{c} \exists g = \sum b_n q^n \in (f)^\perp \cap \mathbb{Z}[\![q]\!] \text{ so that} \\ b_n \equiv a_n \pmod{r} \text{ for all } n \text{ with } \gcd(n, 2N) = 1 \end{array} \right\}.$$

Assume that A is an optimal quotient of $J_0(N)$ and that $\phi_A : X_0(N) \to A$ is its modular parametrization. This induces an exact sequence of abelian varieties over $\mathbb{Q}$,

$$\eta : \quad 0 \to C \to J_0(N) \xrightarrow{\phi_*} A \to 0.$$

This sequence is also an exact sequence of $\mathbb{T}$-group schemes over $\mathbb{Q}$. For any integer n, we have the following commutative diagram with exact rows,

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Hom}_{\mathbb{Q},\mathbb{T}}(A,C) \otimes \mathbb{Z}/n\mathbb{Z} \arrow[r] \arrow[d] & \mathrm{Hom}_{\mathbb{Q},\mathbb{T}}(A_n,C_n) \arrow[r] \arrow[d, "\kappa"'] & \mathrm{Ext}^1_{\mathbb{Q},\mathbb{T}}(A,C)_n \arrow[r] \arrow[d, "\iota"'] & 0 \\
0 \arrow[r] & \mathrm{Hom}_{\mathbb{Q}}(A,C) \otimes \mathbb{Z}/n\mathbb{Z} \arrow[r] & \mathrm{Hom}_{\mathbb{Q}}(A_n,C_n) \arrow[r] & \mathrm{Ext}^1_{\mathbb{Q}}(A,C)_n \arrow[r] & 0.
\end{tikzcd}$$

The bottom row is precisely (1), and since the Kummer sequence $0 \to A_n \to A \to A \to 0$ is a sequence of $\mathbb{T}$-group schemes, the top row is obtained in the same manner as (1) but with the requirement of $\mathbb{T}$-equivariance. Note also that the top row is an exact sequence of $\mathbb{T}$-modules. Now since $\mathrm{Hom}_{\mathbb{Q}}(A,C) = \mathrm{Hom}_{\mathbb{Q},\mathbb{T}}(A,C) = 0$ and the map κ is injective, it follows that ι is also injective. Alternately, any element of $\mathrm{Ext}^1_{\mathbb{Q},\mathbb{T}}(A,C)$ which splits in $\mathrm{Ext}^1_{\mathbb{Q}}(A,C)$ is split by a $\mathbb{T}$-equivariant morphism. By Theorem 1, the injectivity of ι shows that $\mathrm{Ext}^1_{\mathbb{Q},\mathbb{T}}(A,C)$ is finite.

Proposition 7. *The order of η in $\mathrm{Ext}^1_{\mathbb{Q},\mathbb{T}}(A,C)$ is equal to the degree of ϕ_A.*

Proof. Let $d_A = \deg \phi_A$. Because A is an optimal quotient of $X_0(N)$, the dual $\phi^* : A \to J_0(N)$ of ϕ_* is injective, and the composition $\phi_* \circ \phi^* \in \mathrm{Hom}_{\mathbb{Q}}(A,A)$ is multiplication by d_A. From the exact sequence $0 \to A \to J_0(N) \to C^* \to 0$ and the fact that $\mathrm{Hom}_{\mathbb{Q}}(A,C^*) = 0$, it follows that the map

$$\mathrm{Hom}_{\mathbb{Q}}(A,A) \xrightarrow{\sim} \mathrm{Hom}_{\mathbb{Q}}(A,J_0(N))$$

induced by ϕ^* is an isomorphism. Furthermore, the map

$$\mathrm{Hom}_{\mathbb{Q}}(A,A) \to \mathrm{Hom}_{\mathbb{Q}}(A,J_0(N)) \to \mathrm{Hom}_{\mathbb{Q}}(A,A),$$

induced by $\phi_* \circ \phi^*$, is multiplication by d_A, the image of $\mathrm{Hom}_{\mathbb{Q}}(A,J_0(N))$ is precisely $d_A(\mathrm{Hom}_{\mathbb{Q}}(A,A))$.

The long exact sequence for $\mathrm{Ext}^i_{\mathbb{Q}}(A,-)$ applied to η begins

$$0 \to \mathrm{Hom}_{\mathbb{Q}}(A,J_0(N)) \xrightarrow{\phi_*} \mathrm{Hom}_{\mathbb{Q}}(A,A) \to \mathrm{Ext}^1_{\mathbb{Q}}(A,C),$$

and the image of an endomorphism $\alpha \in \mathrm{Hom}_{\mathbb{Q}}(A,A)$ in $\mathrm{Ext}^1_{\mathbb{Q}}(A,C)$ is the pull-back $\alpha^*\eta$. Therefore, because $\mathrm{Hom}_{\mathbb{Q}}(A,A) = \mathbb{Z}$, it follows that the image of $\mathrm{Hom}_{\mathbb{Q}}(A,A)$ in $\mathrm{Ext}^1_{\mathbb{Q}}(A,C)$ is the subgroup generated by η. Thus the order of η in $\mathrm{Ext}^1_{\mathbb{Q}}(A,C)$ is d_A, and since η represents a class in $\mathrm{Ext}^1_{\mathbb{Q},\mathbb{T}}(A,C) \subseteq \mathrm{Ext}^1_{\mathbb{Q}}(A,C)$, we are done. $\square$

There are two ways to define a $\mathbb{T}$-module structure on $\mathrm{Ext}^1_{\mathbb{Q}}(A,C)$, namely by pushing out along C or pulling back along A. These two $\mathbb{T}$-module structures need not coincide. However, because $\mathrm{Ext}^1_{\mathbb{Q},\mathbb{T}}(A,C)$ consists of classes of extensions which are $\mathbb{T}$-equivariant, it follows that the two $\mathbb{T}$-module definitions restricted to $\mathrm{Ext}^1_{\mathbb{Q},\mathbb{T}}(A,C)$ *are* the same. In fact, $\mathrm{Ext}^1_{\mathbb{Q},\mathbb{T}}(A,C)$ is the largest subgroup of $\mathrm{Ext}^1_{\mathbb{Q}}(A,C)$ on which the two $\mathbb{T}$-module structures agree.

Proof of Theorem 4. By Proposition 7 it suffices now to prove that $e_{A,\mathbb{T}} \mid m_A$. Let I_A and I_C be the kernels of the maps $\mathbb{T} \to \mathrm{End}_{\mathbb{Q}}(A)$ and $\mathbb{T} \to \mathrm{End}_{\mathbb{Q}}(C)$. By the general considerations of [5, §2], we see that m_A is the exponent of $\mathbb{T}_{A,C} := \mathbb{T}/(I_A+$

I_C) as an abelian group. Now clearly both I_A and I_C annihilate $\mathrm{Ext}^1_{\mathbb{Q},\mathbb{T}}(A,C)$, and so $\mathrm{Ext}^1_{\mathbb{Q},\mathbb{T}}(A,C)$ is a $\mathbb{T}_{A,C}$-module. Thus we must have $e_{A,\mathbb{T}} \mid m_A$. □

Proof of Theorem 3. Again by Proposition 7 it suffices to prove that $e_A \mid r_A$. Let $\mathbb{T}' \subseteq \mathbb{T}$ be the subalgebra generated by all T_n with $\gcd(n,2N)=1$, and let I'_A and I'_C be the kernels of the maps $\mathbb{T}' \to \mathrm{End}_{\mathbb{Q}}(A)$ and $\mathbb{T}' \to \mathrm{End}_{\mathbb{Q}}(C)$. From [5, §2], it follows that r_A is the exponent of $\mathbb{T}'_{A,C} := \mathbb{T}'/(I'_A + I'_C)$. If we can show that $\mathrm{Ext}^1_{\mathbb{Q}}(A,C)$ is a $\mathbb{T}'_{A,C}$-module, then we are done. Namely, we need to show that the two operations of $\mathbb{T}'$ on $\mathrm{Ext}^1_{\mathbb{Q}}(A,C)$ coincide.

Consider T_p with $p \nmid 2N$. Since $\mathrm{Hom}_{\mathbb{Q}}(A,C)=0$, (1) implies that $\mathrm{Ext}^1_{\mathbb{Q}}(A,C)_n \cong \mathrm{Hom}_{\mathbb{Q}}(A_n,C_n)$. From the Eichler-Shimura relations [9, Thm. 4.2.1], we have that

$$T_p = F + V \in \mathrm{End}_{\mathbb{F}_p}(\widetilde{J}), \tag{5}$$

where $\widetilde{J}$ is the reduction of $J_0(N)$ modulo p, and F and V are the p-th power Frobenius and Verschiebung. As in (3), the natural map

$$\mathrm{Hom}_{\mathbb{Q}}(A_n,C_n) \hookrightarrow \mathrm{Hom}_{\mathbb{F}_p}(\widetilde{A}_n,\widetilde{C}_n) \tag{6}$$

is injective. Since both A and C are subabelian varieties of $J_0(N)$, the action of T_p on $\widetilde{A}_n$ and $\widetilde{C}_n$ is determined by the restriction of (5). In particular, for any $\alpha \in \mathrm{Hom}_{\mathbb{Q}}(A_n,C_n)$, its image $\tilde{\alpha} \in \mathrm{Hom}_{\mathbb{F}_p}(\widetilde{A}_n,\widetilde{C}_n)$ satisfies

$$\tilde{\alpha} \circ T_p|_{\widetilde{A}_n} = T_p|_{\widetilde{C}_n} \circ \tilde{\alpha}.$$

The injectivity of (6) shows that in fact $\alpha \circ T_p|_{A_n} = T_p|_{C_n} \circ \alpha$, and we are done. □

Corollary 8. *If the conductor N of A is square-free, then $d_A = e_{A,\mathbb{T}} = m_A$.*

Proof. For prime N, this follows from Theorem 4 and [27, Thm. 3], and for general N, by the recent work of Ribet [19] which resolves a conjecture of A. Agashe and W. Stein. □

Remark. If N is prime and if the form $g = \sum b_n q^n \in (f)^\perp \cap \mathbb{Z}[\![q]\!]$, which gives $b_n \equiv a_n \pmod{r_A}$ for all n with $\gcd(n,2N)=1$, also satisfies $b_2 \equiv a_2 \pmod{r_A}$, then in fact $d_A = e_{A,\mathbb{T}} = m_A = e_A = r_A$ by the Sturm bound [22].

Example. Theorems 3 and 4 are best possible in the following sense. The mod 3 representation of the elliptic curve $90A1$ in [4] of conductor 90, $A : y^2 + xy = x^3 - x^2 + 6x$, has image $\left(\begin{smallmatrix} 1 & * \\ 0 & * \end{smallmatrix}\right)$ [17, Thm. 3.2]. Likewise, the mod 3 representation of the elliptic curve $90C1$ in [4], also of conductor 90, $B : y^2+xy+y = x^3-x^2+13x-61$, has image $\left(\begin{smallmatrix} * & * \\ 0 & 1 \end{smallmatrix}\right)$. Thus there is a non-trivial element $\alpha \in \mathrm{Hom}_{\mathbb{Q}}(A_3,B_3)$, which induces a homomorphism $\alpha : A_3 \to C_3$, where C is the kernel of $J_0(90) \to A$. Thus $\mathrm{Ext}^1_{\mathbb{Q}}(A,C)_3 \cong \mathrm{Hom}_{\mathbb{Q}}(A_3,C_3)$ has a non-trivial element of order 3. However, direct computation provides $d_A = 8$ and $m_A = 8$. In particular, $e_A \nmid m_A$.

Remark. If A is an elliptic curve over $\mathbb{Q}$ and $\phi : J \to A$ realizes A as an optimal quotient of the Jacobian J of a Shimura curve, then we have an exact sequence

$$\eta : \quad 0 \to C \to J \xrightarrow{\phi} A \to 0.$$

Theorem 3 suggests that the order of $\mathrm{Ext}^1_{\mathbb{Q}}(A,C)$ provides a "congruence modulus" even in this setting where the lack of Fourier coefficients makes the theory of Hida-Ribet inapplicable. In fact, the Hida constant c_A defined by E. Ullmo [24, p. 326] is the order of $\eta \in \mathrm{Ext}^1_{\mathbb{Q}}(A,C)$.

References

[1] S. Bosch, W. Lütkebohmert, and M. Raynaud, *Néron models*, Springer-Verlag, Berlin, 1990.

[2] C. Breuil, B. Conrad, F. Diamond, and R. Taylor, *On the modularity of elliptic curves over* **Q***: wild* 3*-adic exercises*, J. Amer. Math. Soc. **14** (2001), 843–939.

[3] B. Conrad, *The flat deformation functor*, Modular forms and Fermat's last theorem (Boston, MA, 1995), Springer, New York, 1997, pp. 373–420.

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

[5] F. Diamond, *On congruence modules associated to* Λ*-adic forms*, Compositio Math. **71** (1989), 49–83.

[6] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73** (1983), 349–366.

[7] M. Flach, *A finiteness theorem for the symmetric square of an elliptic curve*, Invent. Math. **109** (1992), 307–327.

[8] H. Hida, *Congruence of cusp forms and special values of their zeta functions*, Invent. Math. **63** (1981), 225–261.

[9] H. Hida, *Geometric modular forms and elliptic curves*, World Scientific Publishing, River Edge, NJ, 2000.

[10] D. W. Masser and G. Wüstholz, *Refinements of the Tate conjecture for abelian varieties*, Abelian varieties (Egloffstein, 1993), de Gruyter, Berlin, 1995, pp. 211–223.

[11] J. S. Milne, *Extensions of abelian varieties defined over a finite field*, Invent. Math. **5** (1968), 63–84.

[12] J. S. Milne, *The Tate-Šafarevič group of a constant abelian variety*, Invent. Math. **6** (1968), 91–105.

[13] J. S. Milne, *On a conjecture of Artin and Tate*, Ann. of Math. (2) **102** (1975), 517–533.

[14] J. S. Milne, *Arithmetic duality theorems*, Academic Press Inc., Boston, MA, 1986.

[15] J. S. Milne and N. Ramachandran, *Integral motives and special values of zeta functions*, preprint, math.NT/0204065, 2002.

[16] M. A. Papanikolas and N. Ramachandran, *A Weil-Barsotti formula for Drinfeld modules*, J. Number Theory (to appear).

[17] A. Reverter and N. Vila, *Images of mod* p *Galois representations associated to elliptic curves*, Canad. Math. Bull. **44** (2001), 313–322.

[18] K. A. Ribet, *Congruence relations between modular forms*, Proceedings of the International Congress of Mathematicians, Vol. 1, 2 (Warsaw, 1983), PWN, Warsaw, 1984, pp. 503–514.

[19] K. A. Ribet, *Congruences and the modular degree*, in preparation.

[20] J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), 259–331.

[21] J.-P. Serre, *Propriétés conjecturales des groupes de Galois motiviques et des représentations* l*-adiques*, Motives (Seattle, WA, 1991), Proc. Sympos. Pure Math., vol. 55, Amer. Math. Soc., Providence, RI, 1994, pp. 377–400.

[22] J. Sturm, *On the congruence of modular forms*, Number theory (New York, 1984–1985), Lecture Notes in Math., vol. 1240, Springer, Berlin, 1987, pp. 275–280.

[23] J. Tate, *Finite flat group schemes*, Modular forms and Fermat's last theorem (Boston, MA, 1995), Springer, New York, 1997, pp. 121–154.

[24] E. Ullmo, *Sur la constante de Hida des courbes modulaires et des courbes de Shimura*, J. Théor. Nombres Bordeaux **13** (2001), 325–337.

[25] V. Vatsal, *Canonical periods and congruence formulae*, Duke Math. J. **98** (1999), 397–419.

[26] A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. (2) **141** (1995), 443–551.

[27] D. Zagier, *Modular parametrizations of elliptic curves*, Canad. Math. Bull. **28** (1985), 372–384.

Department of Mathematics, Brown University, Providence, RI 02912 USA
E-mail address: `map@math.brown.edu`

Department of Mathematics, University of Maryland, College Park, MD 20742 USA

Max-Planck-Institut für Mathematik, Vivatsgasse 7, D-53111 Bonn, Germany
E-mail address: atma@math.umd.edu