Available online at www.sciencedirect.com

SCIENCE DIRECT®

Journal of Number Theory 112 (2005) 386–400

JOURNAL OF Number Theory

www.elsevier.com/locate/jnt

Extensions of abelian varieties defined over a number field

Matthew A. Papanikolas[a,*,1], Niranjan Ramachandran[b,c,2]

[a]*Department of Mathematics, Texas A&M University, College Station, TX 77843, USA*
[b]*Department of Mathematics, University of Maryland, College Park, MD 20742, USA*
[c]*Max-Planck-Institüt für Mathematik, Vivatsgasse 7, D-53111 Bonn, Germany*

Received 3 December 2003; revised 20 April 2004

Communicated by D. Goss

Available online 11 November 2004

Abstract

We study the arithmetic aspects of the finite group of extensions of abelian varieties defined over a number field. In particular, we establish relations with congruences between modular forms and special values of *L*-functions.

MSC: Primary 11G05; Secondary 11F33; 14K15

Keywords: Abelian varieties; Extension groups; Congruences between modular forms; Symmetric square *L*-function

1. Introduction

Milne [16,17] has established striking connections between arithmetic and the extensions of abelian varieties over finite fields (see Theorem 1). Our aim here is to relate extensions of abelian varieties over number fields to congruences between modular forms and special values of *L*-functions of motives.

[*] Corresponding author.
E-mail addresses: map@math.tamu.edu (M.A. Papanikolas), atma@math.umd.edu (N. Ramachandran).
[1] Partially supported by NSF and NSA grants.
[2] Partially supported by MPIM.

0022-314X/$ - see front matter © 2004 Elsevier Inc. All rights reserved.
doi:10.1016/j.jnt.2004.08.005

For abelian varieties A and B over a field K, 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, $\mathrm{Ext}^1_{\mathbb{C}}(A,B) \cong (\mathbb{Q}/\mathbb{Z})^4$ when A and B are non-isogenous elliptic curves over $\mathbb{C}$. If A is an elliptic curve with complex multiplication over $\mathbb{C}$, then a beautiful result of Lichtenbaum [20, Theorem 6.1] states that $\mathrm{Ext}^1_{\mathbb{C}}(A,A)$ is naturally isomorphic to the torsion subgroup of $A(\mathbb{C})$.

When K is a number field, the group $\mathrm{Ext}^1_K(A,B)$ is finite (Theorem 2). We show that the order of $\mathrm{Ext}^1_K(A,B)$ is related to the following objects:

- (Corollary 5) congruences between modular forms, when A and B are elliptic curves over $\mathbb{Q}$;
- (Theorems 6, 7) the congruence modulus and modular degree of an elliptic curve over $\mathbb{Q}$;
- (Theorem 10) the special value of the L-function $L(\mathrm{Sym}^2 E, s)$ at $s=2$ for certain elliptic curves E over $\mathbb{Q}$.

It is important to note that the third result is simply a restatement of the deep results of Diamond, Flach, and Guo [5,6] in our context.

2. Preliminaries

2.1. Extensions over finite fields

We recall the fundamental results of Milne [16,17] on $\mathrm{Ext}(A,B)$ over a finite field.

Theorem 1 (*Milne (a)* [16, Theorem 3]; *(b)* [17]). *Let A and B be abelian varieties over a finite field $\mathbb{F}_q$.*

(a) *The group $\mathrm{Ext}^1_{\mathbb{F}_q}(A,B)$ is finite, and its order is given by*

$$\#\mathrm{Ext}^1_{\mathbb{F}_q}(A,B) = \pm\frac{q^{d_A d_B}}{D}\prod_{a_i \neq b_j}\left(1-\frac{a_i}{b_j}\right),$$

where a_i and b_j are the eigenvalues of Frobenius associated with A and B over $\mathbb{F}_q$, d_A and d_B are the dimensions of A and B, and D is the discriminant of the trace pairing $\mathrm{Hom}_{\mathbb{F}_q}(A,B) \times \mathrm{Hom}_{\mathbb{F}_q}(B,A) \to \mathrm{End}(A) \to \mathbb{Z}$.

(b) *Let J be the Jacobian of a smooth projective curve C over $\mathbb{F}_q$. The group $\mathrm{Ext}^1_{\mathbb{F}_q}(J,A)$ is isomorphic to the Tate-Shafarevich group $Ш(A/\mathbb{F}_q(C))$ of the constant abelian variety A over the function field $\mathbb{F}_q(C)$ of C.*

Remark. Every abelian variety A defines integral motives $h^1(A)$ and $h_1(A)$; note that $h_1(A)$ is isomorphic to $h^1(A^\vee)(1)$ defined by the dual abelian variety $A^\vee$. Part (a) of Theorem 1 relates the order of $\mathrm{Ext}^1_{\mathbb{F}_q}(A, B)$ to the special value at $s = 0$ of the L-function $L(h_1(A) \otimes h^1(B), s)$ of the tensor product motive [19, Theorem 10.1].

2.2. *Finiteness of* $\mathrm{Ext}^1_K(A, B)$ *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, and let $TG = \varprojlim G_n$ denote the total Tate module.

Theorem 2 (*Milne–Ramachandran*). *Let A and B be abelian varieties over a number field K. Then $\mathrm{Ext}^1_K(A, B)$ is finite.*

Proof. 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

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

using $\mathrm{Hom}_K(A_n, B) = \mathrm{Hom}_K(A_n, B_n)$. Now 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

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

By Faltings' theorem [7, Section IV.1], α is an isomorphism, and so $T_p\mathrm{Ext}^1_K(A, B) = 0$ for all p. As $\mathrm{Ext}^1_K(A, B)_n$ is finite for all n by (1), the p-primary subgroup $\mathrm{Ext}^1_K(A, B)(p)$ of $\mathrm{Ext}^1_K(A, B)$ is finite for all p. To prove the theorem, it now suffices to show that $\mathrm{Ext}^1_K(A, B)(p)$ is nonzero only for finitely many p. This follows from [7, Section IV.4] which says that α_p in (1) is an isomorphism for sufficiently large primes p. □

Remark. (i) In the case of an elliptic curve A over $\mathbb{Q}$, the results of Serre [24] provide upper bounds on the order of $\mathrm{Ext}^1_{\mathbb{Q}}(A, A)$. (ii) There are explicit bounds (see [14, Corollary 1]) for the primes dividing $\#\mathrm{Ext}^1_K(A, B)$. (iii) The group $\mathrm{Ext}^1_K(A, B)$ is not invariant under isogeny.

2.3. Representability issues

Fix abelian varieties A and B over a field K. The group $\mathrm{Ext}^1_K(A, B)$ is similar to the group $\mathrm{Ext}^1_K(A, \mathbb{G}_m)$, but there are some differences. For example, the functor $S \mapsto \mathrm{Ext}^1_S(A \times S, \mathbb{G}_m)$ on the category of schemes over K is representable (by the dual abelian variety). However, the corresponding functor for $\mathrm{Ext}^1_K(A, B)$ is not representable. If L is an extension of K, then the natural map $\mathrm{Ext}^1_K(A, B) \to \mathrm{Ext}^1_L(A, B)$ need not be injective. In fact, if L/K is a Galois extension with Galois group G, the kernel of this map can be computed via the exact sequence

$$0 \to H^1(G, \mathrm{Hom}_L(A, B)) \to \mathrm{Ext}^1_K(A, B) \to \mathrm{Ext}^1_L(A, B)^G.$$

Over a number field K, the group $\mathrm{Ext}^1_K(A, \mathbb{G}_m)$ can be infinite whereas $\mathrm{Ext}^1_K(A, B)$ is always finite.

3. Congruences between modular forms

We will maintain the following notations throughout this section. Let K be a number field with ring of integers $\mathcal{O}$ and discriminant D. Let A and B be abelian varieties over K, and let $R > 1$ be the least integer such that both A and B extend to abelian schemes (denoted $\mathcal{A}$ and $\mathcal{B}$) over $\mathcal{O}[\frac{1}{R}]$. Let

$$S := R \prod_{\substack{p \ \text{prime} \\ \exists \mathfrak{p} | p, \ \ e(\mathfrak{p}) \geqslant p-1}} p,$$

where $e(\mathfrak{p})$ is the ramification index of $\mathfrak{p}$ in $\mathcal{O}$. Now take $\mathrm{Ext}^1_{\mathcal{O}[\frac{1}{S}]}(\mathcal{A}, \mathcal{B})$ for the Ext-group in the category of commutative group schemes over $\mathcal{O}[\frac{1}{S}]$. The necessity of changing from R to S will be explained below.

Proposition 3. *For abelian varieties A and B over a number field K, the natural map $\mathrm{Ext}^1_{\mathcal{O}[\frac{1}{S}]}(\mathcal{A}, \mathcal{B}) \to \mathrm{Ext}^1_K(A, B)$ is an isomorphism.*

Now suppose that A and B are elliptic curves. Let $\mathfrak{p}$ be an ideal of $\mathcal{O}$ coprime to S. Both A and B have good reduction at $\mathfrak{p}$; let $\widetilde{A}$ and $\widetilde{B}$ denote the corresponding elliptic curves over $\mathbb{F}_\mathfrak{p}$.

Theorem 4. *Let A and B be elliptic curves over a number field K, and let e be the exponent of $\mathrm{Ext}^1_K(A, B)$. For a prime ideal $\mathfrak{p}$ of $\mathcal{O}$ coprime to S,*

$$\#\widetilde{A}(\mathbb{F}_\mathfrak{p}) \equiv \#\widetilde{B}(\mathbb{F}_\mathfrak{p}) \pmod{e}.$$

This theorem has the following corollary for congruences between Fourier coefficients of modular forms. We provide two proofs of this corollary. The first is a direct application of Theorem 4. The second proof, found by Ribet after reading a previous version of this paper, is direct and relies on the theta operator.

Corollary 5. *Suppose A and B are 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 the associated normalized newforms of A and B, and let e be the exponent of $\operatorname{Ext}^1_{\mathbb{Q}}(A, B)$. Then, for any integer n with* $\gcd(n, 2MN) = 1$,

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

Remark. It is possible to strengthen the corollary. Since f and g depend only on the isogeny class of A and B and yet the group $\operatorname{Ext}^1_{\mathbb{Q}}(A, B)$ is not invariant under isogeny (in general), one can replace e in the corollary above by (i) the exponent e' of the group $\operatorname{Ext}^1_{\mathbb{Q}}(A', B')$ where A' and B' are isogenous to A and B over $\mathbb{Q}$; or, (ii) the least common multiple of the set of all e'.

Proof of Proposition 3. Let n be any positive integer. We first show that the natural map

$$b : \operatorname{Hom}_{\mathcal{O}[\frac{1}{S}]}(\mathcal{A}_n, \mathcal{B}_n) \xrightarrow{\sim} \operatorname{Hom}_K(A_n, B_n)$$

is an isomorphism. This follows from standard patching arguments [15, pp. 43–45] once we show that, for each prime $\mathfrak{q}$ coprime to S, the natural map

$$\operatorname{Hom}_{\mathcal{O}_\mathfrak{q}}(\mathcal{A}_n, \mathcal{B}_n) \xrightarrow{\sim} \operatorname{Hom}_{K_\mathfrak{q}}(A_n, B_n)$$

is an isomorphism. Let q be the residue characteristic of $\mathfrak{q}$. The second map is clearly an isomorphism if $q \nmid n$: the étale group schemes $\mathcal{A}_n$ and $\mathcal{B}_n$ over $\operatorname{Spec} \mathcal{O}_\mathfrak{q}$ are determined by the Galois modules $A_n(\overline{K}_\mathfrak{q})$ and $B_n(\overline{K}_\mathfrak{q})$ [15, pp. 43–45]. In the case that $q \mid n$, write $n = dr$ with d a power of q and r coprime to q. We apply [26, Corollary of Theorem 4.5.1] to the commutative finite flat group schemes $\mathcal{A}_d$, $\mathcal{B}_d$ over $\operatorname{Spec} \mathcal{O}_\mathfrak{q}$, which implies that the natural map

$$\operatorname{Hom}_{\mathcal{O}_\mathfrak{q}}(\mathcal{A}_d, \mathcal{B}_d) \to \operatorname{Hom}_{\operatorname{Gal}(\overline{K}_\mathfrak{q}/K_\mathfrak{q})}(A_d(\overline{K}_\mathfrak{q}), B_d(\overline{K}_\mathfrak{q}))$$

is an isomorphism. As the result [26, Corollary of Theorem 4.5.1] assumes that the ramification index $e(\mathfrak{q})$ of $\mathcal{O}_\mathfrak{q}$ is less than $q - 1$, we are forced to switch from R to S.

We obtain a commutative diagram from (1) with exact rows

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

The second row is obtained by the analogue of (1) using $0 \to \mathcal{A}_n \to \mathcal{A} \to \mathcal{A} \to 0$ [18, Section II.5]. The vertical maps are the natural restriction maps. Now, a is an isomorphism by the Néron mapping properties of $\mathcal{A}$ and $\mathcal{B}$. By the preceding paragraph, b is also an isomorphism. Therefore, c is an isomorphism. □

Proof of Theorem 4. Let $\mathfrak{p}$ be a prime of $\mathcal{O}$, coprime to S, with residue characteristic p. We obtain the following diagram that can be appended to (3):

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Hom}_{\mathcal{O}[\frac{1}{S}]}(\mathcal{A},\mathcal{B})\otimes\mathbb{Z}/n\mathbb{Z} \arrow[r] \arrow[d, "h"'] & \mathrm{Hom}_{\mathcal{O}[\frac{1}{S}]}(\mathcal{A}_n,\mathcal{B}_n) \arrow[r] \arrow[d, "i"'] & \mathrm{Ext}^1_{\mathcal{O}[\frac{1}{S}]}(\mathcal{A},\mathcal{B})_n \arrow[r] \arrow[d, "j"'] & 0 \\
0 \arrow[r] & \mathrm{Hom}_{\mathbb{F}_\mathfrak{p}}(\widetilde{A},\widetilde{B})\otimes\mathbb{Z}/n\mathbb{Z} \arrow[r] & \mathrm{Hom}_{\mathbb{F}_\mathfrak{p}}(\widetilde{A}_n,\widetilde{B}_n) \arrow[r] & \mathrm{Ext}^1_{\mathbb{F}_\mathfrak{p}}(\widetilde{A},\widetilde{B})_n \arrow[r] & 0.
\end{tikzcd} \tag{4}$$

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

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

is injective: if $\gcd(n, p) = 1$, this is clear; and if $n = p^r$, this follows from the faithful nature of the functor $G \rightsquigarrow G \times_{\mathcal{O}_\mathfrak{p}} \mathbb{F}_\mathfrak{p}$ which maps commutative finite flat group schemes over $\mathcal{O}_\mathfrak{p}$ of p-power order to their special fiber (see [2, Theorem 4.5] and [10, Theorem 1, p. 171; Theorem 2, p. 217]). These references give the required result as the ramification index $e(\mathfrak{p})$ is less than $p - 1$. The injectivity of β provides an exact sequence

$$0 \to \ker(\gamma) \to \operatorname{coker}(\alpha) \to \operatorname{coker}(\beta) \to \operatorname{coker}(\gamma) \to 0. \tag{5}$$

We can now complete the proof of the theorem. We consider the non-trivial case that $\#\widetilde{A}(\mathbb{F}_\mathfrak{p}) \neq \#\widetilde{B}(\mathbb{F}_\mathfrak{p})$. This implies that $\mathrm{Hom}_{\mathbb{F}_\mathfrak{p}}(\widetilde{A}, \widetilde{B}) = 0$, and so combining (3)–(5) and Theorem 2, we have the injectivity of $\gamma : \mathrm{Ext}^1_K(A, B) \hookrightarrow \mathrm{Ext}^1_{\mathbb{F}_\mathfrak{p}}(\widetilde{A}, \widetilde{B})$. By Theorem 1(a),

$$\#\mathrm{Ext}^1_{\mathbb{F}_p}(\widetilde{A}, \widetilde{B}) = \bigl(\#A(\mathbb{F}_\mathfrak{p}) - \#B(\mathbb{F}_\mathfrak{p})\bigr)^2.$$

Moreover, since A and B are elliptic curves, Theorem 1(b) and the Cassels–Tate pairing combine to give

$$Ш(\widetilde{B}/\mathbb{F}_{\mathfrak{p}}(\widetilde{A})) \cong T \times T,$$

for some abelian group T. Thus the exponent e of $\mathrm{Ext}^1_{\mathbb{F}_p}(\widetilde{A}, \widetilde{B})$ divides $\#T = |\#A(\mathbb{F}_{\mathfrak{p}}) - \#B(\mathbb{F}_{\mathfrak{p}})|$. This, with the injectivity of γ, gives

$$e \mid \big(\#A(\mathbb{F}_{\mathfrak{p}}) - \#B(\mathbb{F}_{\mathfrak{p}})\big), \quad \forall \mathfrak{p} \nmid S. \qquad \square$$

Proof of Corollary 5. The corollary follows almost immediately from Theorem 4. We need only note that since $K = \mathbb{Q}$, the primes which divide S are exactly the primes which divide $2MN$. The congruence for all n with $\gcd(n, S) = 1$ follows since f and g are Hecke eigenforms. □

Remark. Suppose that $K = \mathbb{Q}$ and that R is odd. (i) The map $\mathrm{Ext}^1_{\mathbb{Z}[\frac{1}{R}]}(\mathcal{A}, \mathcal{B}) \to \mathrm{Ext}^1_{\mathbb{Q}}(A, B)$ may not be an isomorphism. However, it is injective. As a is an isomorphism even over $\mathbb{Z}[\frac{1}{R}]$ by the Néron mapping property, it suffices to show that the map $\mathrm{Hom}_{\mathbb{Z}[\frac{1}{R}]}(\mathcal{A}_n, \mathcal{B}_n) \to \mathrm{Hom}_{\mathbb{Q}}(A_n, B_n)$ is injective. Given 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 $n = 2^r$, is injective. This is clear [26, p. 152]. Thus, the Ext-group over $\mathbb{Z}[\frac{1}{R}]$ might be smaller than $\mathrm{Ext}^1_{\mathcal{O}[\frac{1}{S}]}(\mathcal{A}, \mathcal{B})$, and so a potential analogue of Theorem 4 will be weaker.

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

Direct Proof of Corollary 5. (This proof is due to Ribet.) Since f and g are Hecke eigenforms, it suffices to show that $a_p \equiv b_p \pmod{\lambda}$ for all primes $p \nmid 2MN$ and prime powers $\lambda = \ell^m$ dividing e. Fix now such p and $\lambda = \ell^m$.

Suppose first that $p \neq \ell$. Let $G_{\mathbb{Q}} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Now letting $\sigma \in G_{\mathbb{Q}}$ be a Frobenius element at p, the Eichler–Shimura relations [12, Theorem 4.2.2] dictate that

$$\sigma^2 - a_p\sigma + p = 0 \quad \text{on } A_\lambda,$$
$$\sigma^2 - b_p\sigma + p = 0 \quad \text{on } B_\lambda.$$

Now from (1) with $n = \lambda$, it follows that there is a Galois equivariant morphism $\alpha : A_\lambda \to B_\lambda$ with exponent λ. Because α is $G_{\mathbb{Q}}$-equivariant, it follows that the operators

$a_p\sigma$ and $b_p\sigma$ agree on the image of α in B_λ, which has exponent λ. Hence $a_p \equiv b_p \pmod{\lambda}$.

Now suppose that $p = \ell$. In particular, $\ell \nmid 2MN$. Now by the preceding paragraph, we see that $a_n \equiv b_n \pmod{\lambda}$ whenever n is coprime to $2MN\ell$. Let $\hat{f}$ and $\hat{g}$ be modular forms with Fourier expansions

$$\hat{f} = \sum_{\substack{n=1 \\ \gcd(n,2MN)=1}}^{\infty} a_n q^n, \qquad \hat{g} = \sum_{\substack{n=1 \\ \gcd(n,2MN)=1}}^{\infty} b_n q^n.$$

(These modular forms can be obtained by twisting twice by appropriate quadratic characters, and as such have level dividing $4M^2N^2$.) Thus, if we let $\Theta = q\frac{d}{dq}$ be the usual Θ operator on modular forms, we see that Θ^m annihilates $\hat{f} - \hat{g}$ modulo λ. In particular, as power series in q,

$$\Theta(\hat{f} - \hat{g}) \equiv 0 \pmod{\ell}.$$

Since ℓ is odd, the Θ operator is injective modulo ℓ on modular forms of weight 2 [13, Section II]. Therefore $\hat{f} \equiv \hat{g} \pmod{\ell}$. Moreover, if $m > 1$, we see that Θ annihilates $(\hat{f} - \hat{g})/\ell$ modulo ℓ, and thus $\hat{f} \equiv \hat{g} \pmod{\ell^2}$. By induction, $\hat{f} \equiv \hat{g} \pmod{\lambda}$. □

Remark. (Ribet) When e is odd, the arguments in both proofs of Corollary 5 imply that $a_n \equiv b_n \pmod{e}$ for $\gcd(n, MN) = 1$ instead of $\gcd(n, 2MN) = 1$. In some sense, having the Θ operator injective modulo odd primes is similar to having the absolute ramification index of $\mathbb{Z}_p$ strictly less than $p - 1$ in the first proof of Corollary 5.

4. Modular parametrizations and congruence moduli

We now investigate how the theory of congruence moduli of Hida [11], Ribet [22] and Zagier [28] fits in with the Ext-group.

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* [28, Section 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 $J_0(N)$ (i.e. a strong Weil curve) and that $\phi_A : X_0(N) \to A$ is its modular parametrization. This induces an exact sequence of abelian varieties over $\mathbb{Q}$,

$$\eta : \quad 0 \to C \to J_0(N) \overset{\phi_*}{\to} A \to 0. \tag{6}$$

A well-known result of Ribet and Zagier [28] is that: *the degree d_A of ϕ_A divides m_A*, i.e.

$$d_A \mid m_A.$$

Of course m_A divides r_A. Our next result, that the exponent e_A of $\operatorname{Ext}^1_{\mathbb{Q}}(A, C)$ sits between d_A and r_A, ultimately relies on the Eichler–Shimura relations.

Theorem 6. *With notations as above, one has*

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

Remark. Since d_A is unbounded, Theorem 6 shows that the order of $\operatorname{Ext}^1_{\mathbb{Q}}(A, C)$ is unbounded.

In general, e_A does not divide the congruence modulus m_A. 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 $\operatorname{Ext}^1_{\mathbb{Q},\mathbb{T}}(A, C)$. We show below that the natural forgetful map $\operatorname{Ext}^1_{\mathbb{Q},\mathbb{T}}(A, C) \to \operatorname{Ext}^1_{\mathbb{Q}}(A, C)$ is injective, and thus $e_{A,\mathbb{T}} \mid e_A$.

Theorem 7. *With notations as above, one has*

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

The sequence (6) 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 $\mathrm{Hom}_{\mathbb{Q}}(A,C) = 0 = \mathrm{Hom}_{\mathbb{Q},\mathbb{T}}(A,C)$ 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 2, the injectivity of ι shows that $\mathrm{Ext}^1_{\mathbb{Q},\mathbb{T}}(A,C)$ is finite.

Proposition 8. *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, and so 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. □

Now 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 that 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 7. By Proposition 8 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 [4, Section 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 6. Again by Proposition 8 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 [4, Section 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 [12, Theorem 4.2.1], we have that

$$T_p = F + V \in \mathrm{End}_{\mathbb{F}_p}(\widetilde{J}), \tag{7}$$

where $\widetilde{J}$ is the reduction of $J_0(N)$ modulo p, and F and V are the p-th power Frobenius and the Verschiebung on $\widetilde{J}$. As in (4), the natural map

$$\mathrm{Hom}_{\mathbb{Q}}(A_n, C_n) \hookrightarrow \mathrm{Hom}_{\mathbb{F}_p}(\widetilde{A}_n, \widetilde{C}_n) \tag{8}$$

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

Corollary 9. *If the conductor N of A is square-free, then $d_A = e_{A,\mathbb{T}} = m_A$.*

Proof. For prime N, Ribet and Zagier [28, Theorem 3] have shown that $d_A = m_A$. For square-free N, that $d_A = m_A$ has been proved recently by Ribet [23] as a consequence of his proof of a conjecture of Agashe and 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 [25].

Example. Theorems 6 and 7 are best possible in the following sense. The mod 3 representation of the elliptic curve $90C1$ in [3] of conductor 90,

$$A : y^2 + xy + y = x^3 - x^2 + 13x - 61,$$

has image $\left(\begin{smallmatrix} * & * \\ 0 & 1 \end{smallmatrix}\right)$ [21, Theorem 3.2]. Likewise, the mod 3 representation of the elliptic curve $90A1$ in [3], also of conductor 90,

$$B : y^2 + xy = x^3 - x^2 + 6x,$$

has image $\begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix}$. Both A and B are strong Weil curves. By their mod 3 representations, 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 $d_A = 16$ and $m_A = 16$. In particular, $m_A \neq r_A$ and $e_A \nmid m_A$.

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 6 suggests that the exponent of $\mathrm{Ext}^1_{\mathbb{Q}}(A, C)$ provides a "congruence modulus". In fact, the Hida constant c_A defined by Ullmo [27, p. 326] is the order of $\eta \in \mathrm{Ext}^1_{\mathbb{Q}}(A, C)$.

5. Special values of *L*-functions

We provide a restatement in terms of Ext-groups of the deep results of Diamond, Flach, and Guo [5,6] on the Bloch–Kato conjecture.

5.1. Symmetric square of an elliptic curve

Let E be an elliptic curve over $\mathbb{Q}$ of conductor N with $\mathrm{End}_{\overline{\mathbb{Q}}}(E)=\mathbb{Z}$. Consider the symmetric square L-function $L(\mathrm{Sym}^2 E, s)$ of E [9]. Note that

$$L(\mathrm{Sym}^2 E, s) = L(\mathrm{Sym}^2 h_1(E), s) = L(\mathrm{Sym}^2 h^1(E), s+2).$$

The Bloch–Kato conjecture [9, Eq. (2)] on the special value at $s=2$ of $L(\mathrm{Sym}^2 E, s)$ states that

$$\frac{L(\mathrm{Sym}^2 E, 2)}{\Omega(2)} = \frac{\#Ш(\mathbb{Q}, A(2))}{\#H^0(\mathbb{Q}, A(1)) \cdot \#H^0(\mathbb{Q}, A(2))} \prod_p c_p. \tag{9}$$

For the sake of brevity we refer to Flach [9, Sections 0–1] for definitions, and we use his notation.

For a field K, set $G_K := \mathrm{Gal}(\overline{K}/K)$. Let P_E denote the finite set of rational primes consisting of (a) all $\ell \mid 2N$; and (b) all ℓ such that the Galois representation on E_ℓ restricted to G_F, where $F = \mathbb{Q}(\sqrt{(-1)^{(\ell-1)/2}\,\ell})$, is not absolutely irreducible. For $\ell \notin P_E$, the ℓ-part of the Bloch–Kato conjecture has been proved by Diamond, Flach, and Guo [5, Theorem 0.2], [6, Theorem 8.9]. The following theorem is a reformulation of their result in terms of Ext-groups.

Theorem 10. *If E is an elliptic curve over $\mathbb{Q}$ with $\mathrm{End}_{\overline{\mathbb{Q}}}(E)=\mathbb{Z}$, then up to powers of ℓ for $\ell \in P_E$,*

$$\frac{L(\mathrm{Sym}^2 E, 2)}{\Omega(2)} = \frac{\#Ш(\mathrm{Ext}^1_{\overline{\mathbb{Q}}}(E, E))}{\#\mathrm{Ext}^1_{\mathbb{Q}}(E, E) \cdot \#\mathrm{Ext}^1_{\overline{\mathbb{Q}}}(E, E)(1)^{G_\mathbb{Q}}} \prod_p c_p. \tag{10}$$

Proof. Because of the results [5, Theorem 0.2] and [6, Theorem 8.9], it suffices to match the terms in (9) with those of (10).

The total Tate module TE of E is a rank two module over $\widehat{\mathbb{Z}} := \varprojlim \mathbb{Z}/n\mathbb{Z}$. By the Weil pairing, TE is isomorphic to the Tate twist $TE^\vee(1)$ of the dual module $TE^\vee$. From (2), we see that $T\mathrm{Ext}^1_{\overline{\mathbb{Q}}}(E, E)$ is isomorphic to the quotient of $\mathrm{End}_{\widehat{\mathbb{Z}}}(TE)$ by the $\widehat{\mathbb{Z}}$-submodule generated by the identity map. Via the self-duality $\mathrm{End}_{\widehat{\mathbb{Z}}}(TE) \cong TE \otimes TE^\vee$, we have

$$T\mathrm{Ext}^1_{\overline{\mathbb{Q}}}(E, E) \cong (\mathrm{Sym}^2 TE)(-1). \tag{11}$$

The terms in the denominator of (9) can easily be identified as

$$\begin{aligned}\#H^0(\mathbb{Q}, A(1)) &= \#H^0(G_{\mathbb{Q}}, (\mathrm{Sym}^2 TE)(-1) \otimes \mathbb{Q}/\mathbb{Z}),\\ \#H^0(\mathbb{Q}, A(2)) &= \#H^0(G_{\mathbb{Q}}, (\mathrm{Sym}^2 TE) \otimes \mathbb{Q}/\mathbb{Z}).\end{aligned}$$

By (11), the former is $\#\mathrm{Ext}^1_{\overline{\mathbb{Q}}}(E, E)^{G_{\mathbb{Q}}}$, and the latter is $\#\mathrm{Ext}^1_{\overline{\mathbb{Q}}}(E, E)(1)^{G_{\mathbb{Q}}}$. Moreover, the numerator of (9) is

$$\#Ш((\mathrm{Sym}^2 TE) \otimes \mathbb{Q}/\mathbb{Z}) = \#Ш((\mathrm{Sym}^2 TE)(-1) \otimes \mathbb{Q}/\mathbb{Z}),$$

where the equality follows from [8, Theorem 1]. The proof of the theorem is then complete by the following lemma. □

Lemma 11. *Let E be an elliptic curve over a number field K with $\mathrm{End}_{\overline{K}}(E) = \mathbb{Z}$. For any odd integer n, $\mathrm{Ext}^1_K(E, E)_n \cong \mathrm{Ext}^1_{\overline{K}}(E, E)_n^{G_K}$.*

Proof. By taking the long exact sequence of G_K-cohomology of (1) with $K = \overline{K}$, we obtain an exact sequence

$$\begin{aligned}0 \to \mathrm{Hom}_K(E, E) \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z} &\to \mathrm{Hom}_K(E_n, E_n) \to \mathrm{Ext}^1_{\overline{K}}(E, E)_n^{G_K}\\ &\to \mathrm{Hom}(G_K, \mathbb{Z}/n\mathbb{Z}) \xrightarrow{\phi} H^1(G_K, \mathrm{Hom}_{\overline{K}}(E_n, E_n)).\end{aligned}$$

If $f \in \ker\phi$, then $\phi(f)$ is represented by a coboundary which takes values in the trace 0 space of $\mathrm{Hom}_{\overline{K}}(E_n, E_n)$. However, by definition $\phi(f)(\sigma) = f(\sigma) \cdot \mathrm{id}$, for $\sigma \in G_K$. Thus for all $\sigma \in G_K$, we have $2f(\sigma) = 0$, which implies $f = 0$. Therefore, ϕ is injective, and the result follows from (1). □

Acknowledgments

We thank J. Milne for graciously allowing the unpublished proof of Theorem 2 in Section 2 to be included here. We thank K. Ribet for sharing his proof of Corollary 5 in Section 3 with us and for permitting us to include it to supplement our own. We also thank S. Ahlgren, V. Balanzew, N. Dummigan, S. Lichtenbaum, G. Pappas, and J. Teitelbaum for their helpful remarks and suggestions. We thank the referee for many useful suggestions.

References

[1] S. Bosch, W. Lütkebohmert, M. Raynaud, Néron Models, Springer, Berlin, 1990.

[2] B. Conrad, The Flat Deformation Functor, in: Modular Forms and Fermat's Last Theorem (Boston, MA, 1995), Springer, New York, 1997, pp. 373–420.

[3] J. Cremona, Algorithms for Modular Elliptic Curves, 2nd ed., Cambridge University Press, Cambridge, 1997.

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

[5] F. Diamond, M. Flach, L. Guo, The Bloch–Kato conjecture for adjoint motives of modular forms, Math. Res. Lett. 8 (2001) 437–442.

[6] F. Diamond, M. Flach, L. Guo, Adjoint motives of modular forms and the Tamagawa number conjecture, preprint, Ann. Sci. ENS, Paris, to appear, 2001.

[7] G. Faltings, G. Wüstholz, F. Grunewald, N. Schappacher, U. Stuhler, Rational Points, 2nd ed., Vieweg, Braunschweig, 1986.

[8] M. Flach, A generalisation of the Cassels–Tate pairing, J. Reine Angew. Math. 412 (1990) 113–127.

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

[10] J.-M. Fontaine, Groupes p-divisibles sur les corps locaux, Astérisque, No. 47–48. Soc. Math. de France, Paris, 1977.

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

[12] H. Hida, Geometric Modular Forms and Elliptic Curves, World Scientific Publishing, River Edge, NJ, 2000.

[13] N.M. Katz, A result on modular forms in characteristic p, Modular Functions of One Variable, V, Lecture Notes in Mathamatics, Vol. 601, Springer, Berlin, 1977, pp. 53–61.

[14] D.W. Masser, G. Wüstholz, Refinements of the Tate Conjecture for Abelian Varieties, in: Abelian Varieties (Egloffstein, 1993), de Gruyter, Berlin, 1995, pp. 211–223.

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

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

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

[18] J.S. Milne, Arithmetic Duality Theorems, Academic Press Inc., Boston, MA, 1986.

[19] J.S. Milne, N. Ramachandran, Integral motives and special values of zeta functions, J. Amer. Math. Soc. 17 (2004) 499–555.

[20] M.A. Papanikolas, N. Ramachandran, A Weil-Barsotti formula for Drinfeld modules, J. Numb. Theory 98 (2003) 407–431.

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

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

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

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

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

[26] J. Tate, Finite Flat Group Schemes, in: Modular Forms and Fermat's Last Theorem (Boston, MA, 1995), Springer, New York, 1997, pp. 121–154.

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

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