Canad. J. Math. Vol. **67** (1), 2015 pp. 198–213
http://dx.doi.org/10.4153/CJM-2014-001-2


# Tate Cycles on Abelian Varieties with Complex Multiplication

V. Kumar Murty and Vijay M. Patankar

*Abstract.* We consider Tate cycles on an Abelian variety $A$ defined over a sufficiently large number field $K$ and having complex multiplication. We show that there is an effective bound $C = C(A, K)$ so that to check whether a given cohomology class is a Tate class on $A$, it suffices to check the action of Frobenius elements at primes $v$ of norm $\leq C$. We also show that for a set of primes $v$ of $K$ of density 1, the space of Tate cycles on the special fibre $A_v$ of the Néron model of $A$ is isomorphic to the space of Tate cycles on $A$ itself.

## 1 Introduction and Statement of Results

Let $K$ be a field that is finitely generated over its prime field. In our case, $K$ will in fact be a number field or a finite field. Let $A$ be an Abelian variety defined over $K$ of dimension $d$, say. For a prime $\ell$ with $\ell \nmid \operatorname{char}(K)$, and $n \geq 1$, we have the $\ell$-adic Tate module

$$T_\ell(A) = \operatorname{proj\,lim} A[\ell^n] \simeq \mathbb{Z}_\ell^{2d}.$$

In a natural way, it is a $G_K = \operatorname{Gal}(\overline{K}/K)$-module. Also set

$$V_\ell(A) = T_\ell(A) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell.$$

Set $\overline{A} = A \times_K \overline{K}$. Then, we may identify $V_\ell(A)$ with $H_{1,\ell}(\overline{A})$ and the cohomology of $A$ with the exterior algebra on the dual of $V_\ell(A)$. As usual, for a $G_K$-module $W$, we denote by $W(k)$ the $k$-fold Tate twist of $W$.

For any field $F$ with $K \subseteq F \subseteq \overline{K}$, set

$$\mathfrak{T}_\ell^k(A, F) = H_\ell^{2k}(\overline{A})(k)^{\operatorname{Gal}(\overline{K}/F)},$$

$$\mathfrak{T}_\ell^*(A) = \bigoplus_k \sum_{K \subseteq F \subseteq \overline{K}} \mathfrak{T}_\ell^k(A, F).$$

This is the space of Tate cycles on $A$. It is a finite dimensional $\mathbb{Q}_\ell$ vector space, and we may in fact restrict the field $F$ above to be of finite degree over $K$. Thus, for some finite extension $M$ of $K$, we have

$$\mathfrak{T}_\ell^*(A) = \oplus_k H_\ell^{2k}(\overline{A})(k)^{\operatorname{Gal}(\overline{K}/M)} = \oplus_k \mathfrak{T}_\ell^k(A, M).$$

Again, for $K \subseteq F \subseteq \overline{K}$, let $Z^k(A, F)$ denote the free Abelian group generated by algebraic cycles of co-dimension $k$ on $A$ (modulo homological equivalence) with a

Received by the editors April 30, 2013; revised January 24, 2014.
Published electronically March 18, 2014.
Research of VKM partially supported by an NSERC Discovery Grant.
AMS subject classification: **11G10**, 14K22.
Keywords: abelian varieties, complex multiplication, Tate cycles.

representative defined over $F$. The $\ell$-adic cycle class map is

$$c_{\ell,k,F}\colon Z^k(A,F)\otimes_{\mathbb{Z}}\mathbb{Q}_l \to \mathcal{T}^k_\ell(A,F).$$

***Conjecture 1.1*** ([16] Tate) *The $\ell$-adic cycle class map is surjective.*

This was proved by Tate for $k = 1$ in the case $K$ is a finite field and by Faltings in the case where $K$ is a number field. This conjecture is not known to be independent of $\ell$.

There is a related conjecture involving $L$-functions associated with $A$.

***Conjecture 1.2*** (Tate) *If $K$ is a number field, $L(H^{2k}_\ell(\overline{A}), s)$ has a meromorphic continuation to $Re(s) = 1 + k$ and*

$$\operatorname{ord}_{s=1+k} L\big(H^{2k}_\ell(\overline{A}), s\big) = -\dim \mathcal{T}^k_\ell(A,K).$$

*If $K$ is a finite field,*

$$\operatorname{ord}_{s=k} L\big(H^{2k}_\ell(\overline{A}), s\big) = -\dim \mathcal{T}^k_\ell(A,K).$$

Our aim is to study (in the case $K$ is a number field) the relationship between $\mathcal{T}^*_\ell(A)$ and $\mathcal{T}^*_\ell(A_v)$. Here $v$ is a prime of $K$ of good reduction for $A$, $\ell$ is assumed to be distinct from the characteristic of the residue field $k_v$ (of $K$ at $v$), and $A_v$ stands for the reduction of $A$ modulo $v$.

At a prime $v$ of good reduction for $A$, we have the natural reduction map, $A \to A_v$, which induces a natural map (under pull-back) $H^*_\ell(\overline{A_v}) \simeq H^*_\ell(\overline{A})$. Let

$$\iota_v\colon H^*_\ell(\overline{A}) \longrightarrow H^*_\ell(\overline{A_v}) \tag{1.1}$$

be the inverse of this isomorphism. We may view both sides as $\mathbb{Q}_\ell[G_v]$-modules, where $G_v \subset G_K$ is *the* decomposition group at $v$ (subgroup of $G_K$ unique up to conjugation). Indeed, the left-hand side $H^*_\ell(\overline{A})$ is naturally a $G_v$-module under restriction from $G_K$. The right-hand side is naturally a $\mathbb{Q}_\ell[G_{k_v}]$ module, where $G_{k_v}$ is the Galois group of the residue field $k_v$ at $v$. Since $G_{k_v}$ is naturally a quotient of $G_v$, we can consider $H^*_\ell(\overline{A_v})$ as a $\mathbb{Q}_\ell[G_v]$-module. Also, as $v$ is a prime of good reduction, the criterion of Néron–Ogg–Shafarevich [13] implies that the inertia subgroup at $v$ acts trivially on $H^*_\ell(\overline{A})$. Thus, the two sides in (1.1) are isomorphic as $\mathbb{Q}_\ell[G_v]$-modules, and so restriction gives us a map

$$\iota_v\colon \mathcal{T}^*_\ell(A) \to \mathcal{T}^*_\ell(A_v), \tag{1.2}$$

which is, in fact, injective.

We begin with the following observation. A class $\omega \in H^{2m}_\ell(\overline{A})(m)$ for which $\iota_v(\omega)$ is in $\mathcal{T}^m_\ell(A_v, k_v)$ at almost all places $v$ of $K$ (*i.e.,* at all but finitely many places of $K$) is in $\mathcal{T}^m_\ell(A,K)$. Indeed, this follows from the Chebotarev density theorem. This observation can be strengthened as follows.

***Proposition 1.3*** *Let $S$ be a set of places of $K$ with positive Dirichlet density, say $\delta > 0$. A class $\omega \in H^{2m}_\ell(\overline{A})(m)$ for which $\iota_v(\omega)$ is in $\mathcal{T}^m_\ell(A_v, k_v)$ at all places $v$ in $S$ is in $\mathcal{T}^m_\ell(A)$.*

https://doi.org/10.4153/CJM-2014-001-2 Published online by Cambridge University Press

**Proof** Note that the $\ell$-adic representation $\rho_\ell\colon G_K \to \operatorname{Aut}(H^{2m}_\ell(\overline{A})(m))$ is unramified at all but finitely many places $v$ of $K$. Let $L$ be the sub-extension of $\overline{K}$ fixed by $\operatorname{Ker}(\rho_\ell)$. Then $L$ is a Galois extension of $K$ and is unramified at all except finitely many places of $K$. At a finite prime $v$, to be a Tate class means that it is fixed by the *Frobenius automorphism* in $\operatorname{Gal}(\overline{k_v}/k_v)$ given by $x \mapsto x^{\mathbb{N}v}$, where $\mathbb{N}v$ is the cardinality of $k_v$ (also the norm of $v$). The Frobenius automorphism lifts to $\operatorname{Frob}_v$ (at almost all $v$) and thus, by (1.1) as above and the assumption, $\omega$ is fixed by $Frob_v \in \operatorname{Gal}(L/K)$. Let $G_S$ be the group generated by $\{\operatorname{Frob}_v \,|\, v \in S\}$ in $\operatorname{Gal}(L/K)$ as a topological group. Let $L^{G_S}$ be the sub-extension of $L$ cut out by $G_S$. The places of $S$ split completely in $L^{G_S}$. This implies that $L^{G_S}$ is a finite extension of $K$. Moreover, by the Chebotarev density theorem, $[\operatorname{Gal}(L/K){:}G_S] = [L^{G_S}{:}K] \leq 1/\delta$. Thus, it follows that if for all $v \in S$, $\iota_v(\omega)$ is in $\mathcal{T}^m_\ell(A_v, k_v)$, then $\omega$ is in $\mathcal{T}^m_\ell(A, L^{G_S})$, *i.e.*, it is a Tate class. ∎

With more work, we will show that in the case of Abelian varieties with complex multiplication, the condition of the above result can be replaced with a condition at a *finite* set of primes. Moroever, this can be done in an effective manner. Here also, the role of split primes is crucial.

We recall that for each prime $\ell$, Serre and Tate [13] define a conductor of $A$ (in terms of the Artin and the Swan character). It is an integer that they prove is independent of $\ell$ ([13, pp. 499–500]).

***Theorem 1.4*** *Let $A$ be an Abelian variety with complex multiplication and let $K$ be a number field over which both $A$ and its endomorphisms are defined. Denote by $d$ the dimension of $A$ and by $N$ the* conductor *of $A$. Then there is an effective bound $C = C(A, K)$ such that if $\omega \in H^{2m}_{\ell_0}(\overline{A})(m)$, for some prime $\ell_0$, is a Tate class considered as an element of $H^{2m}_{\ell_0}(\overline{A_v})(m)$ for all $v$ of $K$ with $N_{K/\mathbb{Q}}v \leq C$, then $\omega$ is Tate,* i.e., *$\omega \in \mathcal{T}^m_{\ell_0}(A, K)$.*

Several remarks are in order.

***Remark 1.5*** The main point of the above theorem is that the bound $C$ (defined by (6.2)) depends only on the Abelian variety $A$ (in fact, only on the conductor, the dimension, and the discriminant of the field of complex multiplication) and the number field $K$ and does not depend on $\ell_0$. However, if we fix a prime $\ell$, it is possible to prove (using the Chebotarev density theorem and Nakayama's lemma for finitely generated modules over $\mathbb{Z}_\ell$) the existence of a *constant* (that would depend on $A$, $K$ and $\ell$) so that a similar statement as in the theorem above is true.

***Remark 1.6*** The proof of Theorem 1.4 will produce an explicit expression for $C$ (as defined by (6.2)) only in terms of the degree $n_K$, the discriminant $d_K$ of $K$, the conductor $N$, the dimension $d$ of $A$ and the discriminant $d_F$ of the field $F$ of multiplication of $A$. We have not made any effort to find an optimal bound. However, we note that with the assumption of the Riemann Hypothesis for Dedekind zeta functions, the estimate for $C$ that comes from the proof of Theorem 1.4 can essentially be replaced by $(\log C)^2$. It would be very interesting to study to what extent it would be possible to get a bound that is uniform in each of the parameters $n_K, d_K, N, d_F$ and $d$.

https://doi.org/10.4153/CJM-2014-001-2 Published online by Cambridge University Press

***Remark 1.7*** Tate [17, Section 3, pp. 76–77] discusses the notion of an "almost algebraic" cycle. A Tate cycle is said to be *almost algebraic* if all but finitely many of its specializations are algebraic. According to Tate, this notion seems to be part of the folklore. Tate adds: "it is mentioned explicitly in [11, 5.2] that Künneth components of the 'diagonal' are almost algebraic (by [1, Theorem 2(1)])". Thus these "Künneth components of the diagonal" are examples of almost algebraic cycles that are not known to be algebraic. Tate further mentions a weaker conjecture than Conjecture 1.1: The space of Tate cycles is spanned by almost algebraic cycles.

***Remark 1.8*** Let us assume the Tate conjecture for Abelian varieties over finite fields. Suppose that $\omega$ is a class in $H^{2m}_\ell(\overline{A})(m)$ with the property that $\iota_v(\omega)$ is algebraic for each prime $v$ of $K$ of norm $\leq C$. Then $\iota_v(\omega)$ is algebraic for all but finitely many $v$. Indeed, by the above Theorem, $\omega$ is a Tate class, and hence so is its reduction $\iota_v(\omega)$. Now, by our assumption, it follows that $\iota_v(\omega)$ is algebraic. Hence $\omega$ is almost algebraic.

Our next result is about the field of definition of Tate cycles on an Abelian variety over a finite field obtained by reduction of Tate cycle on a fixed Abelian variety over a number field.

***Theorem 1.9*** *Let $A$ be an Abelian variety defined over a number field $K$. Then there is a bound $D = D(A)$ so that for all $v$ of good reduction, all Tate cycles on $A_v$ are defined over an extension of the residue field $k_v$ of degree $\leq D$.*

***Remark 1.10*** In fact our proof of this theorem can be suitably adapted to show that all the Tate cycles on an Abelian variety $A$ over a number field $K$ with complex multiplication by $F$ are defined over a "specific" extension of $K$ that depends on $d = \dim(A)$, the conductor of $A$, and the normal closure of $F$.

As is well known (and as implied by (1.2)) the dimension of the space of Tate cycles does not decrease under reduction modulo $v$. Our next result shows that in the CM case, for a set of primes of Dirichlet density 1, it does not increase either. The proof of this theorem uses Thereom 1.9.

***Theorem 1.11*** *Let $A$ be an Abelian variety of CM type. Let $K$ be sufficiently large so that all the Tate cycles on $A$ and all the endomorphisms of $A$ are defined over $K$. Then, for a set of primes $v$ of $K$ of Dirichlet density* 1,

$$\mathcal{T}^*_\ell(A) \simeq \mathcal{T}^*_\ell(A_v).$$

*In particular, the Tate conjecture for $A$ implies the Tate conjecture for $A_v$ for a set of primes $v$ of Dirichlet density* 1.

***Remark 1.12*** The condition that $K$ be sufficiently large is necessary as the following example illustrates. Let $E$ be an elliptic curve over $\mathbb{Q}$ with complex multiplication by an imaginary quadratic field, say $K = \mathbb{Q}(\sqrt{-d})$, with $d$ a square-free and positive integer. Let $A = E \times E$. Then $Z^1(A, K)$ is generated by $E \times \{0\}$, $\{0\} \times E$, the diagonal

https://doi.org/10.4153/CJM-2014-001-2 Published online by Cambridge University Press

$\Delta := \{(x,x) | x \in E\}$, and the graph of complex multiplication

$$\Delta' := \{(x, [\sqrt{-d}]x) | x \in E\},$$

where $[\sqrt{-d}]$ denotes the endomorphism of $E$ whose square is $[-d]$.

Then $E$ has super-singular reduction at a prime $p$ of $\mathbb{Q}$ that remains inert in $K$ and of good reduction for $E$. Let $A_p$ denote the reduction of $A$ modulo $p$ over $\mathbb{F}_p$. Then, $Z^1(A_p, \overline{\mathbb{F}_p})$ is generated by $E_p \times \{0\}$, $\{0\} \times E_p$, $\Delta_p$ (the reduction of $\Delta$ modulo $p$), $\Delta'_p$ (the reduction of $\Delta'$ modulo $p$), $\Delta_\phi := \{(x, \phi(x)) | x \in E_p\}$, and $\Delta_\psi := \{(x, \psi(x)) | x \in E_p\}$, where $\phi$ and $\psi$ are the other two generators of $\mathrm{End}_{\overline{\mathbb{F}_p}}(E_p)$. This proves that for such primes $p$, the rank of $\mathcal{T}^1_\ell(A)$ is 4 and the rank of $\mathcal{T}^1_\ell(A_p)$ is 6. Thus, the *reduction* map as in (1.2) is strictly injective for a set of primes $p$ of $\mathbb{Q}$ of Dirichlet density $\frac{1}{2}$! However, this is not a problem, as the set of primes of $\mathbb{Q}$ that are inert in $K$, has Dirichet density 0 considered as a set of primes of $K$.

***Remark 1.13*** The theorem is not true for Abelian varieties without complex multiplication as the following example illustrates. Let $E$ be an elliptic curve over $\mathbb{Q}$ without complex multiplication. Let $A = E \times E$ be as above. Then $Z^1(A, K)$ is generated by $E \times \{0\}$, $\{0\} \times E$ and the diagonal $\Delta$ for any number field $K$. Let $v$ be a finite place of $K$ of good reduction for $E$ and let $k_v$ be the finite residue field at $v$. Then $E$ always acquires the extra endomorphism (the *Frobenius*) and $Z^1(A_v, k_v)$ has rank at least 4. Thus, $\mathcal{T}_\ell(A)$ strictly injects into $\mathcal{T}_\ell(A_v)$ for all but finitely many places of $K$.

***Remark 1.14*** In our previous work [7], we studied the problem of when $A_v$ stays simple for a set of primes of positive density, given that $A$ is simple (or absolutely simple). If $A_v$ splits, this gives rise to extra classes in the Néron–Severi group of $A_v$ (and hence also extra Tate cycles on $A_v$).

In Section 2, we recall some basic properties of a compatible family of $\lambda$-adic representations. In Section 3, we recall some basic properties of the theory of complex multiplication. In Section 4, we develop an analytic estimate that will be crucial in the proofs of our main results. In Section 5, we present the Main Lemma, and in the following three sections, we give the proofs of Theorems 1.4, 1.9, and 1.11.

## 2 Brief Background on Compatible Family of $\lambda$-adic Representations

We recall (from [10]) some basics about *compatible* families of $\lambda$-adic Galois representations.

Let $K$ be a number field. Let $\overline{K}$ be a separable algebraic closure of $K$. Let $G_K$ denote the Galois group of $\overline{K}$ over $K$. Let $E_\lambda$ be a non-archimedean local field (finite extension of some $p$-adic field). Let $V$ be a vector space over $E_\lambda$. Let $\mathrm{Aut}(V)$ be the general linear group of $V$ with topology induced by that on $\mathrm{End}(V)$. If $n = \dim(V)$, we have $\mathrm{Aut}(V) \simeq \mathrm{GL}(n, E_\lambda)$.

***Definition 2.1*** A $\lambda$-adic representation of $G_K$ (or of $K$) is a continuous homomorphism $\rho\colon G_K \to \mathrm{Aut}(V)$, where $V$ is vector space over a non-archimedean local field $E_\lambda$, a finite extension of $\mathbb{Q}_p$.

For any number field $F$, we denote by $\Sigma_F$ the set of finite places of $F$. Recall that a $\lambda$-adic representation $\rho$ is said to be *rational* (resp., *integral*) if there exists a finite subset $S$ of $\Sigma_K$ such that

(a) for any place $v$ in $\Sigma_K - S$, $\rho$ is unramified at $v$;
(b) for $v \notin S$, the coefficients of $P_{v,\rho}(T)$ belong to $\mathbb{Q}$ (resp., $\mathbb{Z}$).

Let $E$ be a number field. For each finite prime $\lambda$ of $E$, let $\rho_\lambda$ be a rational $\lambda$-adic representation of $K$. For any given finite prime $\lambda$ of $E$, let us denote by $\ell_\lambda$ the prime of $\mathbb{Q}$ that lies below the prime $\lambda$ of $E$. The system $\{\rho_\lambda\}$ is said to be *strictly compatible* if there exists a finite subset $S$ of $\Sigma_K$, called the *exceptional* set, such that:

(a) for $S_\lambda := \{v | v \text{ lies over } \ell_\lambda\}$ and every $v \notin S \cup S_\lambda$, $\rho_\lambda$ is unramified at $v$ and $P_{v,\rho_\lambda}(T)$ has rational integral coefficients;
(b) $P_{v,\rho_\lambda}(T) = P_{v,\rho_{\lambda'}}(T)$ if $v \notin S \cup S_\lambda \cup S_{\lambda'}$.

***Definition 2.2*** Let $\rho(= \rho_\lambda)$ be a $\lambda$-adic representation of $G_K$. Then we say that $\rho$ is pure of weight $w \in \mathbb{Z}$ if there is a finite set $S$ of finite places of $K$ such that, for each finite place $v \notin S \cup S_\lambda$, $\rho(\mathrm{Frob}_v)$ is unramified, and the eigenvalues of $\rho(\mathrm{Frob}_v)$ are algebraic integers whose complex conjugates have complex absolute value $q_v^{w/2}$, where $q_v$ is the cardinality of the residue field of $K$ at $v$. We say that a compatible family $\{\rho_\lambda\}$ is of weight $w \in \mathbb{Z}$ if for each finite place $\lambda$ of $E$, $\rho_\lambda$ is of pure weight $w$.

As usual, we denote by $\chi_\ell$ the cyclotomic character giving the action of $\mathrm{Gal}(\overline{K}/K)$ on $\ell$-power roots of unity. The $\{\chi_\ell\}$ form a compatible family of $\ell$-adic representations.

## 3 Abelian Varieties with Complex Multiplication and the Shimura–Taniyama Theorem

We now briefly recall a few basic facts about Abelian varieties of *Complex Multiplication* (CM) type. The main references are [3, 8, 13, 14].

Let $A$ be an Abelian variety defined over a number field $K$ of dimension $d := \dim(A)$. Let $F$ be a number field of degree $2d$. Then $A$ is said to have CM by $F$ if there exists an embedding

$$\iota\colon F \to \mathrm{End}_{\mathbb{Q}}(A) := \mathrm{End}_{\overline{\mathbb{Q}}}(A) \otimes_{\mathbb{Z}} \mathbb{Q}.$$

It is a fact that such an $F$ must be a totally imaginary extension of a totally real number field. Let $E$ be the Galois closure of $F$. To such an Abelian variety, the Shimura–Taniyama theory associates Hecke characters $\psi_{i,\lambda}$ of the following type. For each $1 \le i \le 2d$ and for each finite place $\lambda$ of $E$ (lying over a prime $\ell$), we have a family of continuous characters of the Galois group $G_K := \mathrm{Gal}(\overline{K}/K)$:

$$\psi_{i,\lambda}\colon G_K \to E_\lambda^\times$$

with the property that for all $v$ not dividing $\ell N$, $\psi_{i,\lambda}(\mathrm{Frob}_v) \in F^\times$. Thus, the field generated by $\psi_{i,\lambda}(\mathrm{Frob}_v)$ for all $v$ over $\mathbb{Q}$ is contained in $E$. We have the following well-known result ([8, Theorem 2′, p. 171]):

***Theorem 3.1*** (Shimura–Taniyama) *(With notations and definitions as above) Let A be an Abelian variety defined over a number field with CM F. Let $H^k_\ell(\overline{A})$ be the k-th $\ell$-adic étale cohomology of A. Then*

$$H^k_\ell(\overline{A}) \otimes_{\mathbb{Q}_\ell} \overline{\mathbb{Q}_\ell} = \wedge^k H^1_\ell(\overline{A}) \otimes_{\mathbb{Q}_\ell} \overline{\mathbb{Q}_\ell} = \oplus_I H_I,$$

*where the direct sum is over subsets $I \subseteq \{\psi_{1,\lambda}, \dots, \psi_{2d,\lambda}\}$ of cardinality k and where each $H_I$ is a one dimensional $G_K$ invariant $\overline{\mathbb{Q}_\ell}$ subspace of $H^k_\ell(\overline{A}) \otimes_{\mathbb{Q}_\ell} \overline{\mathbb{Q}_\ell}$. Further more, for any finite place v of K away from $\ell$ and from places of bad reduction for A, and for all $x \in H_I$*

$$(\mathrm{Frob}_v)^{-1}(x) = \Big( \prod_{\psi_{i,\lambda} \in I} \psi_{i,\lambda}(\mathrm{Frob}_v) \Big) \cdot x.$$

In fact, the Shimura–Taniyama theory implies that for $1 \le i \le 2d$, $(\psi_{i,\lambda})_\lambda$ forms a compatible family of 1-dimensional continuous $\lambda$-adic representations of $G_K$, where $\lambda$ runs over finite places of $E$. We denote these compatible families by $\psi_i$. Let $\Psi := \{\psi_1, \dots, \psi_{2d}\}$ and $\Psi_\lambda := \{\psi_{1,\lambda}, \dots, \psi_{2d,\lambda}\}$.

***Theorem 3.2*** *(With notations as above) Let $\lambda$ be a prime of E lying over $\ell$. Then*

$$H^{2k}_\ell(\overline{A}) \otimes_{\mathbb{Q}_\ell} E_\lambda = \oplus_I H_{I,\lambda}$$

*where $I \subseteq \Psi_\lambda$ of size 2k and $H_{I,\lambda}$ is a 1 dimensional $G_K$ invariant $E_\lambda$-subspace such that for any finite place v of K away from $\ell$ and places of bad reduction for A,*

$$(\mathrm{Frob}_v)^{-1}(x) = \Big( \prod_{\psi_{i,\lambda} \in I} \psi_{i,\lambda}(\mathrm{Frob}_v) \Big) \cdot x$$

*for $x \in H_{I,\lambda}$.*

We have the following corollary.

***Corollary 3.3*** *With notations and definitions as above, $\{H_{I,\lambda}\}$ is a strictly-compatible family of $\lambda$-adic representations of $G_K$ as $\lambda$ varies over finite places of E.*

## 4 The Least Prime That Does Not Split Completely

Let $L$ and $K$ be number fields with $K \subseteq L$. In the proof of our results, it will be necessary to have an estimate for the norm of a prime $v$ of $K$ that does not split completely in $L$. Such an estimate is given in [6, Theorem 1], assuming the Generalized Riemann Hypothesis for the Dedekind zeta function $\zeta_L(s)$ of $s$ and assuming that $L/K$ is Galois. In the case that $K = \mathbb{Q}$, an unconditional estimate is given by X. Li in [4, Theorem 1], and also by Vaaler and Voloch in [18]. However, we need an (unconditional) estimate for a general $K$. Such an estimate is remarked after the proof of [6, Theorem 1]. What we prove is slightly weaker, though more than sufficient for our purposes.

Let us denote by $n_L$ and $n_K$ the degrees of $L$ and $K$ over $\mathbb{Q}$ respectively. Let $d_L$ and $d_K$ denote the discriminants of $L/\mathbb{Q}$ and $K/\mathbb{Q}$, respectively. We also note the effective prime number theorem in $K$ as given by Lagarias and Odlyzko (see [2] and

https://doi.org/10.4153/CJM-2014-001-2 Published online by Cambridge University Press

[12, Théorème 2]). This theorem tells us that the number $\pi_K(x)$ of primes of $K$ of norm $\leq x$ satisfies

$$|\pi_K(x) - \operatorname{Li} x + \operatorname{Li}(x^\beta)| \leq c_1 x \exp\bigl(-c_2\sqrt{\log x/n_K}\bigr) \tag{4.1}$$

provided $x \geq c_3 n_K(\log|d_K|)^2$. Here, $c_1, c_2, c_3 > 0$ are absolute and effective constants and $\beta$ is the possible exceptional zero of the Dedekind zeta function $\zeta_K(s)$ . If it exists, it is real and satisfies

$$1 - \frac{1}{4\log|d_K|} < \beta < 1.$$

Let us set

$$f(K) = \begin{cases} n_K^2 & \text{if } \zeta_K(s) \text{ does not have an exceptional zero,} \\ \max(n_K!\log|d_K|, |d_K|^{1/n_K}) + n_K^2 & \text{otherwise.} \end{cases} \tag{4.2}$$

Thus, for example, $f(\mathbb{Q}) = 1$.

***Theorem 4.1*** *There is an effective and absolute constant $c > 0$ with the following property. Let $K$ be a number field and let $L/K$ be a finite non-trivial Galois extension of degree $n$ . Then, there exists a prime ideal $\wp$ of $K$ such that*

- *$\wp$ is of degree 1 over $\mathbb{Q}$ and unramified in $L$;*
- *$\wp$ does not split completely in $L$, and*

$$\mathbb{N}_{K/\mathbb{Q}}\wp < \max(55, e^{cf(K)}|d_L|^{4/(n-1)}).$$

**Proof** From [15, Lemma 3], we have for $\sigma > 1$, the inequality

$$-\frac{\zeta_L'}{\zeta_L}(\sigma) < \frac{1}{\sigma} + \frac{1}{\sigma - 1} + \frac{1}{2}\log\Bigl(\frac{|d_L|}{2^{2r_2}\pi^{n_L}}\Bigr) + \frac{r_1}{2}\frac{\Gamma'}{\Gamma}(\sigma/2) + r_2\frac{\Gamma'}{\Gamma}(\sigma). \tag{4.3}$$

On the other hand, we have the Dirichlet series expansion

$$-\frac{\zeta_L'}{\zeta_L}(\sigma) = \sum_{\mathfrak{p},m}\frac{\log\mathbb{N}\mathfrak{p}}{(\mathbb{N}\mathfrak{p})^{m\sigma}},$$

where the sum ranges over primes $\mathfrak{p}$ of $L$ and $1 \leq m \in \mathbb{Z}$. If all primes $\wp$ of $K$ that are of degree 1 over $\mathbb{Q}$ and of norm less than $y$ (say) ramify or split completely in $L$, then we see that with $n = [L:K] = n_L/n_K$,

$$-\frac{\zeta_L'}{\zeta_L}(\sigma) \geq n \sum_{\mathbb{N}\wp \leq y}{}' \frac{\log\mathbb{N}\wp}{(\mathbb{N}\wp)^\sigma},$$

where the prime on the summation indicates that we range over primes $\wp$ of $K$ that are of degree 1 over $\mathbb{Q}$ and are unramified over $L$. Thus,

$$-\frac{\zeta_L'}{\zeta_L}(\sigma) \geq n \sum_{\mathbb{N}\wp \leq y}\frac{\log\mathbb{N}\wp}{(\mathbb{N}\wp)^\sigma} - nS_1 - nS_2,$$

where

$$S_1 = \sum_{\mathbb{N}\wp \leq y}{}^{r} \frac{\log\mathbb{N}\wp}{(\mathbb{N}\wp)^\sigma},$$

https://doi.org/10.4153/CJM-2014-001-2 Published online by Cambridge University Press

and the sum is taken over primes $\wp$ of $K$ that ramify in $L$, and

$$S_2 = \sum_{\substack{\mathbb{N}\wp \le y \\ \wp \text{ of degree } \ge 2}} \frac{\log \mathbb{N}\wp}{(\mathbb{N}\wp)^\sigma}.$$

For each prime $\wp$ counted in this sum, let $p$ be the rational prime that it divides. Then $(\log \mathbb{N}\wp)/(\mathbb{N}\wp)^\sigma \le 2(\log p)/p^{2\sigma}$. Moreover, given a rational prime $p$, there are at most $n_K$ primes $\wp$ of $K$ dividing $p$, and so

$$S_2 \le 2n_K \sum_p \frac{\log p}{p^{2\sigma}} \le 2n_K.$$

We are using the fact that for the Riemann zeta function, the inequality (4.3) gives

$$\sum_p \frac{\log p}{p^{2\sigma}} < -\frac{\zeta'}{\zeta}(2\sigma) < 1$$

for $\sigma > 1$. For $S_1$, we have ([6, p. 558])

$$S_1 \le \sum_{\wp | d_{L/K}} \log \mathbb{N}\wp \le \frac{2}{n} \log d_L.$$

Thus,

$$-\frac{\zeta_L'}{\zeta_L}(\sigma) \ge n \sum_{\mathbb{N}\wp \le y} \frac{\log \mathbb{N}\wp}{(\mathbb{N}\wp)^\sigma} - 2\log d_L - 2n_L. \tag{4.4}$$

To estimate the sum on the right, we use (4.1). Let us assume that $y \ge y_0 = c_3 n_K (\log |d_K|)^2$. By partial summation, we have

$$\sum_{\mathbb{N}\wp \le y} \frac{\log \mathbb{N}\wp}{(\mathbb{N}\wp)^\sigma} = \pi_K(y)(\log y)y^{-\sigma} + \int_1^y \pi_K(t)t^{-1-\sigma}(\sigma \log t + 1)dt. \tag{4.5}$$

The first term on the right is bounded by using the estimate $\pi_K(x) \le n_K \pi(x)$. Thus, we see that as $\sigma > 1$,

$$\pi_K(y)(\log y)y^{-\sigma} \le c_4 n_K.$$

Similarly, we see that

$$\int_1^{y_0} \pi_K(t)t^{-1-\sigma}(\sigma \log t + 1)dt \le 2c_4 n_K \log y_0.$$

The estimate (4.1) implies that replacing $\pi_K(t)$ with $\mathrm{Li}(x) - \mathrm{Li}(x^\beta)$ in the integral in (4.5) results in an error of at most

$$\le 2 \int_1^{\log y} \exp(-c_1 \sqrt{u/n_K})\, u du \le c_5\, n_K^2.$$

The term coming from the possible exceptional zero contributes to the integral an amount that is easily seen to be

$$\ll (\sigma - \beta)^{-1} < (1 - \beta)^{-1}.$$

https://doi.org/10.4153/CJM-2014-001-2 Published online by Cambridge University Press

To estimate this, we note that by [15, equations (27) and (28)], we have

$$\beta < \max\big(1 - (4n_K! \log|d_K|)^{-1}, 1 - (c_6|d_K|^{1/n_K})^{-1}\big).$$

This implies that

$$(1-\beta)^{-1} < \max(4n_K! \log|d_K|, c_6|d_K|^{1/n_K}).$$

Let us denote the right-hand side by $c_K$. Finally, it remains to estimate

$$\int_{y_0}^{y} (\mathrm{Li}\, t) t^{-1-\sigma}(\sigma \log t + 1) dt.$$

and this is easily seen to be

$$\sigma \int_1^y t^{-\sigma} dt + O(\int_1^y t^{-\sigma}(\log t)^{-1}) dt.$$

Taking $\sigma = 1 + (\log y)^{-1}$, this is easily seen to be $\geq (1 - e^{-1}) \log y - c_7 \log\log y$. Putting all this together into (4.4), we deduce that

$$-\frac{\zeta_L'}{\zeta_L}(\sigma) \geq n(1-e^{-1})\log y - n\big(c_K + c_5(\log|d_K|)^2 + c_7 \log\log y\big) \\ - c_8 n_L \log y_0 - 2\log d_L - 2n_L.$$

On the other hand, we can combine this with the upper bound given above (4.3). As mentioned in [15, p. 142], we have $\Gamma'(\sigma/2) < 0$ and $\Gamma'(\sigma) < 0$ for $1 < \sigma < 5/4$. Moreover, $\Gamma(x) > 0$ for $x > 0$ real. Hence, we deduce that provided $y > e^4 \sim 54.6$, there is an absolute and effective constant $c_9 > 0$ such that

$$n(1-e^{-1})\log y < 1 + \log y + \frac{5}{2}\log|d_L| + c_9 n f(K)$$

with $f(K)$ given by (4.2). It follows that there is a $c > 0$ such that

$$\log y \;\leq\; c f(K) + \frac{4}{(n-1)}\log|d_L|.$$

Thus, if $y > e^{cf(K)}|d_L|^{4/(n-1)}$, we get a contradiction, and this proves the result. ∎

We record here the following estimate of Hensel (see, for example, [5, pp. 44–45]), which we shall also need. We have

$$\log d_L \leq (n_L - 1) \sum_{p \in P(L/\mathbb{Q})} \log p + n_L(\log n_L)|P(L/\mathbb{Q})|,$$

where $P(L/\mathbb{Q})$ is the set of rational primes $p$ that ramify in $L$. In fact, when $L$ is Galois over $K$, the following stronger estimate holds:

$$\log d_L \leq (n_L - n_K) \sum_{p \in P(L/K)} \log p + n_L(\log n_L - \log n_K) + \frac{n_L}{n_K}\log d_K.$$

In particular, if $L/K$ is a Galois extension unramified outside of primes dividing $M$, then

$$\log d_L \ll n_L \log\Big(M\frac{n_L}{n_K}\Big) + \frac{n_L}{n_K}\log d_K. \tag{4.6}$$

https://doi.org/10.4153/CJM-2014-001-2 Published online by Cambridge University Press

## 5 Proof of the Main Lemma

***Lemma 5.1*** *Suppose $\omega \in H_l^*(\overline{A})$ is a (simultaneous) eigenvector for a conjugacy set $C \subset G_K$. Then so is every element of $\mathbb{Q}_l[G_K](\omega)$, the $G_K$-module generated by $\omega$ inside $H_l^*(\overline{A})$.*

**Proof** We need to show that for any $g \in G_K$, $g(\omega)$ is an eigenvector for any $\sigma \in C$. We have

$$\begin{aligned}\sigma(g(\omega)) &= g((g^{-1}\sigma g)(\omega)) \\ &= g(\tau(\omega)), \qquad \text{for some } \tau \in C \text{ as } C \text{ is a conjugacy set} \\ &= g(\lambda_\tau \cdot \omega) \qquad \text{for some } \lambda_\tau \in \mathbb{Q}_\ell \text{ by assumption} \\ &= \lambda_\tau \cdot g(\omega).\end{aligned}$$

The last step follows from the $\mathbb{Q}_\ell$ linearity of the $G_K$ action. ■

For integers $N, m, d \geq 1$ and a number field $K$, let us set

$$B = B(N, K, m, d) = e^{f(K)} N^{mn_K d^2} (f(K) + n_K \log N)^{mn_K d^2+1}.$$

Here

$$f(K) = \begin{cases} n_K^2 & \text{if } \zeta_K(s) \text{ does not have an exceptional zero,} \\ \max(n_K! \log |d_K|, |d_K|^{1/n_K}) + n_K^2 & \text{otherwise.} \end{cases}$$

as defined by (4.2), and $n_K = [K:\mathbb{Q}]$.

Let $G_K$ denote the absolute Galois group of a number field $K$. Let $E$ be some number field and $\mathcal{O}_E$ the ring of integers of $E$. For a finite place $\lambda$ of $E$, we denote by $E_\lambda$ the completion of $E$ at $\lambda$, and by $\mathcal{O}_\lambda$ the ring of integers of $E_\lambda$. Let $\{M_\lambda\}$ be a family of continuous $\mathcal{O}_\lambda[G_K]$-modules such that $\{M_\lambda \otimes_{\mathcal{O}_\lambda} E_\lambda\}$ is a strictly compatible family of continuous semi-simple $\lambda$-adic integral representations of $G_K$ of weight $2w$, conductor $N$ and dimension $d$, where $\lambda$ varies over all finite places of $E$. Let $S'$ be the set of exceptional places of $K$ for the system $\{M_\lambda\}$.

***Lemma 5.2*** (Main Lemma) *There are absolute and effective constants $c_1, c > 1$ so that if for some finite place $\lambda_0$ of $E$, the set*

$$S = \{\mathrm{Frob}_v : \mathbb{N}v \leq c_1 B(Nwd^2 \log d_E, K, n_E, d)^c\}$$

*acts as scalars on $M_{\lambda_0}$, then $G_K$ acts as scalars on $M_{\lambda_0}$ and hence on any $M_\lambda$ where $\lambda$ is a finite place of $E$.*

**Proof** By abuse of notation, we will use $M_\lambda$ to denote $M_\lambda$ as a module over $\mathcal{O}_E$ and as well as the associated vector space $M_\lambda \otimes_{\mathcal{O}_E} E_\lambda$ over $E_\lambda$.

First suppose that $\mathrm{Frob}_v$ acts as a scalar $\mu$ on $M_\lambda$. Then $(\mathbb{N}v)^{wd} = \mu^d$, since the characteristic polynomial of $\mathrm{Frob}_v$ has coefficients in $\mathbb{Z}$. So, in fact, $\mu = \epsilon(\mathbb{N}v)^w$ with $\epsilon^d = 1$. Since $\{\rho_\lambda\}$ is a compatible family of rational integral representations, the trace $d\epsilon(\mathbb{N}v)^w$ of $\mathrm{Frob}_v$, lies in $\mathbb{Z}$ and so $\epsilon = \pm 1$.

If $d = 1$, then there is nothing to prove, so we may assume without loss of generality that $d > 1$. Suppose that $G_K$ does not act as scalars on $M_{\lambda_0}$. By compatibility,

$G_K$ does not act as scalars on the family $\{M_\lambda\}$. We shall show that $S$ does not act as scalars either.

Let $S'$ be the exceptional set (of places of $K$) for the system $\{M_\lambda\}$. For a finite place $\lambda$ of $E$, let $\ell_\lambda$ denote the prime of $\mathbb{Q}$ that lies below $\lambda$. Let $S_\lambda := \{v | v \text{ lies over } \ell_\lambda\}$, the set of finite places of $K$ that divide $\ell_\lambda$. For $v \notin S' \cup S_\lambda$, let

$$P_{v,\lambda}(T) := \det\bigl(T - \rho_\lambda(\mathrm{Frob}_v)\bigr).$$

By compatibility, $P_{v,\lambda}(T)$ is independent of $\lambda$.

Let $v \notin S'$ be the prime with least norm such that $\mathrm{Frob}_v$ does not act as a scalar on $M_{\lambda_0}$. (Note that $\mathrm{Frob}_v$ is unique up to conjugation.) Since $\rho_\lambda$ is a semi-simple representation, this is equivalent to $P_v(T) \neq (T - \theta_v)^d$ for any $\theta_v \in \mathbb{C}$. Thus by compatibility, $\mathrm{Frob}_v$ does not act as a scalar on $M_\lambda$ for any $\lambda$.

Denote the eigenvalues of $\mathrm{Frob}_v$ by $\{\alpha_{i,v}\}$ for $i = 1$ to $d$. Let us choose $\ell$ unramified in $E$ so that the distinct eigenvalues of $\mathrm{Frob}_v$ remain distinct modulo $\ell$. This can be done by choosing an $\ell$ that does not divide the discriminant of $E$ and the norm of the product of the differences of any two distinct eigenvalues of $\mathrm{Frob}_v$. We have

$$\Bigl|\prod(\alpha_{i,v} - \alpha_{j,v})\Bigr| \leq \bigl(2(\mathbb{N}v)^w\bigr)^{d^2},$$

where the product is over pairs of distinct eigenvalues of $\mathrm{Frob}_v$. Thus, we can find such an $\ell$ satisfying

$$\ell \ll \log\Bigl\{ d_E\bigl(2\bigl(\mathbb{N}v\bigr)^w\bigr)^{d^2}\Bigr\} \ll wd^2 \log \mathbb{N}v + \log d_E, \tag{5.1}$$

where the implied constant is absolute.

Here, we are using the fact that for an integer $m > 1$, there exists a prime that is $O(\log m)$ that does not divide $m$. Indeed, by the prime number theorem, the product of all the primes less than $3 \log m$ (say) would be larger than $m$. Hence, at least one of these primes does not divide $m$.

It then follows that for at least one of the places $\lambda$ of $E$ that lie over $\ell$, the distinct eigenvalues of $\mathrm{Frob}_v$ remain distinct modulo $\lambda$. Thus, $\mathrm{Frob}_v$ does not act as a scalar on $\overline{M_\lambda} = M_\lambda/\lambda M_\lambda$.

Let $\overline{\rho_\lambda}$ be the natural map from $G_K$ to $PGL(\overline{M_\lambda})$, the projective general linear group associated with $\overline{M_\lambda}$. By above, the image of $\mathrm{Frob}_v$ to $PGL(\overline{M_\lambda})$ is not the identity. By applying Theorem 4.1 to this representation, it follows that there exists a prime $v'$ (say) for which the image of $\mathrm{Frob}_{v'}$ in $PGL(\overline{M_\lambda})$ is not the identity. In particular, $v'$ does not split completely in the fixed field $L$ (say) of the kernel of $\overline{\rho_\lambda}$. We know that $L$ is unramified outside $\ell N$, and as

$$\log \frac{n_L}{n_K} \leq [E\colon\mathbb{Q}]d^2 \log \ell,$$

it follows by (4.6) that

$$\log d_L \ll n_L[E\colon\mathbb{Q}]d^2 \log N\ell + \frac{n_L}{n_K} \log d_K.$$

Then by Theorem 4.1 and $n = n_L/n_K \geq 2$, we can choose $v'$ satisfying

$$\log Nv' \ll f(K) + \frac{n_K}{n_L} \log d_L \ll f(K) + n_K[E\colon\mathbb{Q}]d^2 \log N\ell.$$

By (5.1), we have

$$\log N v' \ll f(K) + n_K[E:\mathbb{Q}]d^2 \log(Nwd^2 \log \mathbb{N}v + N \log d_E).$$

Since $\mathrm{Frob}_{v'}$ does not act as a scalar on $\overline{M_\lambda}$, it does not act as a scalar on $M_\lambda$, and hence on $M_{\lambda_0}$ either, and as $v$ is a prime of least norm with this property, we have an absolute and effective constant $c > 0$ with

$$\mathbb{N}v \le \mathbb{N}v' \le \left(e^{f(K)}\{N(wd^2 \log \mathbb{N}v + \log d_E\}^{n_K[E:\mathbb{Q}]d^2}\right)^c.$$

Hence, we have proved that $\mathbb{N}v$ is bounded by

$$\ll \left(e^{f(K)}(Nwd^2 \log d_E)^{n_K n_E d^2}\right)^c \left(f(K) + n_K n_E d^2 \log(Nwd^2 \log d_E)\right)^{c n_K n_E d^2 + 1}.$$

Here the implied constant is absolute and effective. Thus,

$$\mathbb{N}v \le c_1 B(Nwd^2 \log d_E, K, n_E, d)^c.$$

This contradicts our assumption and proves the lemma. ■

## 6 Proof of Theorem 1.4

By assumption, $\omega \in H^{2m}_{\ell_0}(\overline{A})$. Let $M_{\ell_0}$ be the $\mathbb{Q}_{\ell_0}[G_K]$ sub-module generated by $\omega$ inside $H^{2m}_{\ell_0}(\overline{A})$. Let $\lambda_0$ be a place of $E$ lying over $\ell_0$. Let $M_{\lambda_0} := M_{\ell_0} \otimes_{\mathbb{Q}_{\ell_0}} E_{\lambda_0}$. Then by Theorem 3.2, $M_{\lambda_0}$ is isomorphic (as $E_{\lambda_0}[G_K]$ module) to a sum of $H_{J,\lambda_0}$ for certain subsets $J$ of $\Psi$ of size $2m$. Let us denote this set of subsets $J$ of $\Psi$ by $\mathcal{J}$. Thus,

$$M_{\lambda_0} = M_{\ell_0} \otimes_{\mathbb{Q}_{\ell_0}} E_{\lambda_0} = \oplus_{J \in \mathcal{J}} H_{J,\lambda_0}. \tag{6.1}$$

The right-hand side of (6.1) can be realised as the $\lambda_0$ component of a family of $\lambda$-adic representations, say $\{M_\lambda\}$, as follows. For any finite place $\lambda$ of $E$, let

$$M_\lambda := \oplus_{J \in \mathcal{J}} H_{J,\lambda}.$$

By Corollary 3.3, $\{M_\lambda\}$ is a strictly compatible family of semi-simple $\lambda$-adic representations of $G_K$. It is easy to see from the definition that the conductor of this family is bounded by the conductor of the family $\{H^{2m}_\lambda\}$. Moreover, the conductor of $H^{2m}_\lambda$ can be bounded in terms of $m$ and the conductor $N$ of $A$. In particular, we can get a bound depending on $N$ and the dimension $d$ of $A$ that majorizes the conductor of all the $\{H^{2m}_\lambda\}$.

We have $n_E \le (2d)!$ and the discriminant satisfies

$$\log d_E \le (2d)! \log d_F.$$

Notice that $w = m \le d$, and the dimension of the $M_\lambda$ is equal to $\binom{2d}{2m} \le 2^{2d}$. Thus, if we set

$$C(N, d, F, K) = c_1 B\left(2^{4d}(2d+1)! N \log d_F, K, (2d)!, 2^{2d}\right)^c \tag{6.2}$$

where $c, c_1$ and $B$ are as in Lemma 5.2, then applying Lemma 5.2 to $\{M_\lambda\}$, we get that $G_K$ acts as scalars (*i.e.*, acts by a one dimensional character) on $M_{\lambda_0} = \mathbb{Q}_{\ell_0}[G_K](\omega) \otimes_{\mathbb{Q}_{\ell_0}} E_{\lambda_0}$. This implies that $M_{\lambda_0} = \mathbb{Q}_{\ell_0} \cdot \omega \otimes_{\mathbb{Q}_{\ell_0}} E_{\lambda_0}$. Thus, $1 = \dim_{E_{\lambda_0}} M_{\lambda_0} = \dim_{\mathbb{Q}_{\ell_0}} M_{\ell_0}$, proving Theorem 1.4. ■

## 7 Proof of Theorem 1.9

Denote by $P(A_v, T)$ the characteristic polynomial of $\mathrm{Frob}_v$. Writing

$$P(A_v, T) = \prod(1 - \alpha_i T) \ \in \mathbb{Z}[T]$$

we see that the $\alpha_i$ are algebraic of degree $\leq \deg P(A_v, T) = 2\dim A_v = 2\dim A$.

Moreover, for any $n \geq 1$, if $k_{v,n}$ denotes the extension of $k_v$ of degree $n$,

$$P(A_v/k_{v,n}, T) = \prod(1 - \alpha_i^n T).$$

Now,

$$\dim \mathcal{T}_\ell^k(\overline{A_v}, k_{v,n}) = \#\{I : \alpha_I^n = q^{kn}\},$$

where $\alpha_I = \prod_{\alpha_i \in I} \alpha_i$ and $I$ runs over subsets of $\{\alpha_1, \dots, \alpha_{2d}\}$ of cardinality $2k$. The right-hand side is equal to

$$\#\{I : \alpha_I = q^k \zeta_n \text{ for some } \zeta_n \in \mu_n\}$$

But $\alpha_I$ is an algebraic number of degree $\leq b_{2k}(A) = \dim H_\ell^{2k}(\overline{A}) \leq \binom{2d}{2k}$. Hence if $\alpha_I = q^k\zeta_n$, then $n$ is bounded. In other words, all Tate classes are defined over an extension of $k_v$ of degree bounded independently of $v$. ■

## 8 Proof of Theorem 1.11

By definition, $\mathcal{T}_\ell^k(A)$ consists of cohomology classes $x \in H_\ell^{2k}(\overline{A})$ on which $G_K$ acts by the character $\chi_\ell^k$, where $\chi_\ell$ is the cyclotomic character of $G_K$ acting on the Tate module $\mathbb{Z}_\ell(1)$. Note that we are assuming that $K$ is sufficiently large so that all the Tate classes appear over $K$. By Theorems 3.1 and 3.2, we see that $G_K$ acts on the 1-dimensional subspaces $H_I$ by the Hecke character $\psi_I$. Here,

$$\psi_I = \prod_{j=1}^{2k} \psi_{i_j},$$

where $I$ is the subset $\{i_1, \dots, i_{2k}\}$ of $\{1, \dots, 2d\}$. Thus,

$$\dim \mathcal{T}_\ell^k(A) = \#\{I | \psi_I = \chi_\ell^k\}. \tag{8.1}$$

Similiarly, for a finite place $v$ of $K$ of good reduction for $A$,

$$\dim \mathcal{T}_l^k(A_v) = \#\{I : \psi_I(\mathrm{Frob}_v) = \zeta_n(\mathbb{N}v)^k\}, \tag{8.2}$$

where $\zeta_n$ is some $n$-th root of unity where $n \leq \binom{2d}{2k}$ is bounded indepedently of $v$ as proved in Theorem 1.9. Indeed, by Theorems 3.1 and 3.2, we see that $\mathrm{Frob}_v$ acts on the 1-dimensional vector subspaces $H_I$ by multiplication by $\psi_I(\mathrm{Frob}_v)$. On the other hand, by the above and by Theorem 1.9, $\mathcal{T}_\ell^k(A_v)$ consists precisely of those cohomology classes on which $\mathrm{Frob}_v$ acts by $\chi_\ell^k(\mathrm{Frob}_v) = \zeta_n(\mathbb{N}v)^k$, and so (8.2) follows.

Thus, for all finite places $v$ of good reduction, (8.1) and (8.2) imply:

$$S := \{I : \psi_I = \chi_\ell^k\} \subset S_v := \{I : \psi_I(\mathrm{Frob}_v) = \zeta_n(\mathbb{N}v)^k\}.$$

Let

$$T := \{v \mid S \subsetneq S_v\}.$$

https://doi.org/10.4153/CJM-2014-001-2 Published online by Cambridge University Press

For any $v \in T$, there exists some $J \notin S$ ($J$ depends on $v$) of cardinality $2k$ such that $\psi_J(\mathrm{Frob}_v) \neq \zeta_n(\mathbb{N}v)^k$, where $\zeta_n$ is some $n$-th root of unity. We can write $T = \bigcup_{J \notin S} T_J$,

$$T_J := \{v \in T \mid \psi_J(\mathrm{Frob}_v) = \zeta_n(\mathbb{N}v)^k\}.$$

We want to prove that $T$ is of density 0. Suppose not. By the above, since there are only finitely many index sets $J$, there exists a $J_0 \notin S$ such that $\delta(T_{J_0}) > 0$. Hence, for all $v \in T_{J_0}$, $\psi_{J_0}^n(\mathrm{Frob}_v) = (\mathbb{N}v)^{kn} = \chi_\ell^{kn}(\mathrm{Frob}_v)$. Applying [9, Theorem 2, p. 163] to the characters $\psi_{J_0}^n$ and $\chi_\ell^{kn}$, we deduce that $\psi_{J_0}^n = \chi_\ell^{kn}\chi_1$, where $\chi_1$ is a character of finite order. Hence $\psi_{J_0}^n = \chi_\ell^{kn}$ when restricted to $G_L := \mathrm{Gal}(\overline{K}/L)$, where $L$ is the fixed field cut out by $\mathrm{Ker}(\chi_1)$. Thus, $\psi := \psi_{J_0}^n \cdot \chi_\ell^{-k}$ is a character of $G_L$ of order $n$. Thus $\psi_{J_0} = \chi_\ell^k$ when restricted $\mathrm{Gal}(\overline{K}/L_\psi)$, where $L_\psi$ is the number field cut out by $\mathrm{Ker}(\psi)$. This implies that $J_0$ contributes to a *new* Tate cycle on $A$. However, this is a contradiction, since by assumption all the Tate cycles are defined over $K$ and $J_0 \notin S$. This proves that $T$ has density 0, which proves the result. ■

**Acknowledgements** The second author wishes to thank D. S. Nagaraj (Institute of Mathematical Sciences, Chennai) and Ramesh Sreekantan (Indian Statistical Institute, Bangalore centre) for some helpful discussions.

## References

[1] N. M. Katz and W. Messing, *Some consequences of the Riemann hypothesis for varieties over finite fields.* Invent. Math. **23**(1974), 73–77. http://dx.doi.org/10.1007/BF01405203

[2] J. C. Lagarias and A. M. Odlyzko, *Effective versions of the Chebotarev density theorem.* In: Algebraic number fields: $L$-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975), Academic Press, New York, 1977, pp. 409–464.

[3] S. Lang, *Complex multiplication.* Grundlehren der Mathematischen Wissenschaften, 255, Springer-Verlag, New York, 1983.

[4] X. Li, *The smallest prime that does not split completely in a number field.* Algebra Number Theory **6**(2012), no. 6, 1061–1096. http://dx.doi.org/10.2140/ant.2012.6.1061

[5] M. R. Murty and V. K. Murty, *Non-vanishing of L-functions and applications.* Progress in Mathematics, 157, Birkhauser, Basel, 1997.

[6] V. K. Murty, *The least prime that does not split completely.* Forum Math. **6**(1994), no. 5, 555–565.

[7] V. K. Murty and V. M. Patankar, *Splitting of Abelian varieties.* Internat. Math. Res. Not. **2008**, no. 12, Art. ID rnn033.

[8] H. Pohlmann, *Algebraic cycles on Abelian varieties of complex multiplication type.* Annals of Math **88**(1968),161–180. http://dx.doi.org/10.2307/1970570

[9] C. S. Rajan, *On strong multiplicity one for $\ell$-adic representations.* Internat. Math. Res. Notices **1998**, no. 3, 161–172.

[10] J.-P. Serre, *Abelian $\ell$-adic representations and elliptic curves.* W. A. Benjamin Inc., New York-Amsterdam, 1968.

[11] ———, *Valeurs propres des endomorphismes de Frobenius (d'apres P. Deligne).* Séminaire Bourbaki, no. 446, 1974, Lecture Notes in Math., 431, Springer, Berlin, 1974, pp. 190–204.

[12] ———, *Quelques applications du théoème de densité de Chebotarev.* Inst. Hautes Études Sci. Publ. Math. **54**(1981), 323–401.

[13] J.-P. Serre and J. Tate, *Good reduction of Abelian varieties.* Ann. of Math. **88**(1968), 492–517. http://dx.doi.org/10.2307/1970722

[14] G. Shimura, *Introduction to the arithmetic theory of automorphic functions.* Princeton University Press, Princeton, NJ, 1994.

[15] H. M. Stark, *Some effective cases of the Brauer-Siegel theorem.* Invent. Math. **23**(1974), 135–152. http://dx.doi.org/10.1007/BF01405166

[16] J. T. Tate, *Algebraic cycles and poles of zeta functions.* In: Arithmetical algebraic geometry, Harper and Row, New York, 1965, pp. 93–110.

[17] ———, *Conjectures on algebraic cycles in $\ell$-adic cohomology.* In: Motives (Seattle, WA, 1991), Proc. Symp. Pure Math., 55, Part 1, American Mathematical Society, Providence, RI, 1994, pp. 71–83.
[18] J. D. Vaaler and J. F. Voloch, *The least nonsplit prime in Galois extensions of* $\mathbb{Q}$. J. Number Theory **85**(2000), no. 2, 320–335. http://dx.doi.org/10.1006/jnth.2000.2551

*Department of Mathematics, University of Toronto, Toronto, ON M5S 2E4*
*e-mail*: murty@math.toronto.edu

*International Institute of Information Technology Bangalore, Bangalore, INDIA 560100*
*e-mail*: vijaypatankar@gmail.com