JOURNAL
de Théorie des Nombres
de BORDEAUX
anciennement Séminaire de Théorie des Nombres de Bordeaux

Rémi LODH

On Tate's conjecture for the elliptic modular surface of level N over a prime field of characteristic $1 \bmod N$

Tome 32, nº 1 (2020), p. 193-204.

<http://jtnb.centre-mersenne.org/item?id=JTNB_2020__32_1_193_0>

Journal de Théorie des Nombres
de Bordeaux **32** (2020), 193–204

On Tate's conjecture for the elliptic modular surface of level N over a prime field of characteristic 1 mod N

par Rémi LODH

Résumé. Modulo une hypothèse de semi-simplicité partielle, on démontre le conjecture de Tate pour la surface elliptique modulaire $E(N)$ de niveau N sur un corps premier de cardinalité $p \equiv 1 \mod N$ et on montre que le rang du groupe de Mordell–Weil est nul dans ce cas. Pour $N \leq 4$ c'est un résultat de Shioda. De plus, on démontre que l'hypothèse de semi-simplicité vaut en dehors d'un ensemble de nombres premiers p de densité nulle.

Abstract. Assuming partial semisimplicity of Frobenius, we show Tate's conjecture for the reduction of the elliptic modular surface $E(N)$ of level N at a prime p satisfying $p \equiv 1 \mod N$ and show that the Mordell–Weil rank is zero in this case. This extends a result of Shioda to $N > 4$. Furthermore, we show that for every number field L partial semisimplicity holds for the reductions of $E(N)_L$ at a set of places of density 1.

1. Introduction

In this note we study cohomology classes of divisors on the elliptic modular surface $E(N)$ of level N, where $N \geq 3$. By definition, $E(N)$ is the universal object over the moduli space $X(N)$ of generalised elliptic curves with level N structure. Fix a prime p which does not divide N. Our main result is the following theorem, which goes back to Shioda [20, Appendix] for $N \leq 4$.

Theorem 1.1 (Corollary 3.8). *Assume the partial semisimplicity conjecture is true for $E(N)_{\mathbb{F}_p}$. If $p \equiv 1 \mod N$, then Tate's conjecture holds for $E(N)_{\mathbb{F}_p}$. Moreover, the Mordell–Weil group of a generic fibre of $E(N)_{\mathbb{F}_p} \to X(N)_{\mathbb{F}_p}$ is isomorphic to $(\mathbb{Z}/N)^2$.*

If k is a finite field with $q = p^n$ elements and D is a φ-module over $K_0 = W(k)[1/p]$, then we have an inclusion $D^{\varphi^n=1} \subset D^{(\varphi^n-1)^2=0}$ and we may ask if there is equality, i.e.

$$D^{(\varphi^n-1)^2=0} = D^{\varphi^n=1} \tag{PS}$$

Manuscrit reçu le 13 mai 2019, accepté le 29 novembre 2019.
2020 *Mathematics Subject Classification.* 11G05, 11F11, 14F30.
Mots-clefs. elliptic curves, modular forms, p-adic cohomology, zeta function.

The partial semisimplicity conjecture for a smooth projective surface S over k is the validity of (PS) when $D = H^2_{\mathrm{cris}}(S/K_0)$ is the second crystalline cohomology group of S, and $\varphi = F/p$ where F is the p-power crystalline Frobenius endomorphism. It is a consequence of Tate's conjecture for S. Using a result of Serre [19] on the l-adic representation of newforms, we show that it holds for $E(N)_{\mathbb{F}_p}$ for a set of primes p of density 1, thereby obtaining

Corollary 1.2 (Corollary 3.10)**.** *The conclusions of Theorem 1.1 hold for all* $p \equiv 1 \mod N$ *outside of a set of primes of density zero.*

In fact, for any number field L we show partial semisimplicity for $E(N)_v$ for all finite places v of L outside of a set of density zero (dependent on N and L), see Theorem 3.9. We remark that for $N \leq 4$ the (full) semisimplicity conjecture is known for $E(N)_v$ since it is either a rational ($N = 3$) or a K3 ($N = 4$) surface.

The starting point of the proof of Theorem 1.1 is the following exceptional property of $E(N)$:

(HT) $V_p \operatorname{Br}(E(N)_{\bar{\mathbb{Q}}})$ is a Hodge–Tate representation with weights ± 1

Here $\operatorname{Br}(-) := H^2_{\text{ét}}(-, \mathbb{G}_m)$ denotes the cohomological Brauer group and for any abelian group A we write $V_pA := \operatorname{Hom}(\mathbb{Q}_p/\mathbb{Z}_p, A) \otimes \mathbb{Q}$ (the p-adic Tate module of A tensored with $\mathbb{Q}$). (HT) is a consequence of a result of Shioda [20] on the Néron–Severi group of $E(N)_{\mathbb{C}}$ and the Hodge–Tate decomposition; alternatively, we shall deduce it from Faltings' p-adic Eichler–Shimura isomorphism [7].

The proof of Theorem 1.1 uses the theory of Hecke operators, in particular the Eichler–Shimura congruence relation between the pth Hecke operator T_p and Frobenius endomorphism. Our method can be summarised as follows. Let I_p be the automorphism of $X(N)$ given by multiplying the level structure by $p \in (\mathbb{Z}/N)^*$ and let $U \subset V_p \operatorname{Br}(E(N)_{\bar{\mathbb{Q}}})$ be the subset on which I_p acts trivially. Then (modulo (PS)) (HT) and the action of T_p imply $D_{\mathrm{cris}}(U)^{\varphi=1} = 0$, where φ is the Frobenius. For $p \equiv 1 \mod N$, I_p is the identity and the theorem follows.

In the case $p \not\equiv 1 \mod N$ we only know of Shioda's result [21] for $N = 4$. Our arguments do not apply to this case. In fact, Shioda shows that the Mordell–Weil group of the K3 surface $E(4)_{\mathbb{F}_p}$ has rank 2 for $p \equiv 3 \mod 4$, so the conclusion of Theorem 1.1 cannot hold. On the other hand, it is possible that our method can be applied to other types of modular varieties.

Notation. We denote by k a finite field of characteristic p, $W = W(k)$ its ring of Witt vectors, $K_0 = W[1/p]$, $\bar{k}$ an algebraic closure of k, $\bar{K}$ an algebraic closure of K_0, $G_{K_0} = \operatorname{Gal}(\bar{K}/K_0)$, $\hat{\bar{K}}$ the completion of $\bar{K}$ for the p-adic norm. All cohomology is étale unless stated otherwise.

2. A general result

We assume familiarity with the basics of Fontaine's theory of p-adic Galois representations [4, 8, 9].

2.1. Self-dual crystalline representations. Let V be a p-adic representation of G_{K_0}. We say that V is *self-dual* if it is isomorphic to its dual, i.e. it has a non-degenerate bilinear form

$$V \otimes_{\mathbb{Q}_p} V \to \mathbb{Q}_p$$

which is a homomorphism of G_{K_0}-modules.

Proposition 2.1. *Let V be a self-dual crystalline representation of G_{K_0} and let $D := D_{\mathrm{cris}}(V)$ be the associated filtered φ-module. Suppose the endomorphism $T := \varphi + \varphi^{-1}$ of D satisfies $T(F^1 D) \subset F^1 D$. If $D^{(\varphi-1)^2=0} = D^{\varphi=1}$ and $V^{G_{K_0}} = 0$, then $D^{\varphi=1} = 0$.*

Proof. The bilinear form on V induces a non-degenerate bilinear form $\cdot$ on D. Endow $D^{\varphi=1}$ with the filtration induced from D. Since V is crystalline we have $F^0 D^{\varphi=1} = V^{G_{K_0}} = 0$. If $D^{\varphi=1} = F^0 D^{\varphi=1}$, then we are done. If not, then there is $i < 0$ and $x \in F^i D^{\varphi=1} \setminus F^{i+1} D^{\varphi=1}$. Since V is self-dual, the map $c : D \to D^* := \mathrm{Hom}_{K_0}(D, K_0)$ induced by $\cdot$ is an isomorphism of filtered φ-modules, so we have $x^* := c(x) \in F^i D^* \setminus F^{i+1} D^*$. Note that x^* is the map $D \ni y \mapsto x \cdot y \in K_0$. Since by definition

$$F^i D^* = \{f \in D^* : f(F^j D) \subset F^{j+i} K_0 \ \ \forall\, j \in \mathbb{Z}\}$$

the condition $x^* \notin F^{i+1} D^*$ means that there is j such that $x^*(F^j D) \not\subset F^{j+i+1} K_0$, where K_0 has the trivial filtration, i.e.

$$F^k K_0 = \begin{cases} K_0 & k \le 0 \\ 0 & k > 0. \end{cases}$$

If $x^*(F^j D) \not\subset F^{j+i+1} K_0$, then we must have $x^*(F^j D) \neq 0$, i.e. $x^*(F^j D) = K_0$. So to say that $x^*(F^j D) \not\subset F^{j+i+1} K_0$ but $x^*(F^j D) \subset F^{i+j} K_0$ is equivalent to the condition $i + j = 0$. Hence $j = -i > 0$, and there is an element $y \in F^1 D$ such that $x \cdot y \neq 0$.

Now, up to dividing y by $x \cdot y$ we may assume that $x \cdot y \in \mathbb{Q}_p$. Let $0 \neq P(t) \in \mathbb{Q}_p[t]$ be such that $P(T)y = 0$. Since $\varphi(x) = x$ we have $x \cdot T(d) = T(x \cdot d)$ for all $d \in D$, hence

$$0 = x \cdot P(T)y = P(T)(x \cdot y) = (x \cdot y)P(2).$$

So $P(2) = 0$ and we deduce that $P(t) = (t-2)^e Q(t)$ for some $e \in \mathbb{N}$ and some $Q(t) \in \mathbb{Q}_p[t]$ not divisible by $t - 2$. Let $z := Q(T)y$. Note that $x \cdot z = (x \cdot y)Q(2) \neq 0$. Multiplying the equation $(T-2)^e z = 0$ by φ^e we find $(\varphi - 1)^{2e} z = 0$, hence $\varphi(z) = z$ since $D^{(\varphi-1)^2=0} = D^{\varphi=1}$. As $F^1 D$ is stable under T by assumption, we have $z \in F^1D$. Thus, $z \in F^1D^{\varphi=1} \subset V^{G_{K_0}} = 0$, a contradiction. □

Remark 2.2. The above argument no longer works if one replaces φ by a power φ^r. The problem is related to the fact that, unlike the case $r = 1$, for $r > 1$ we may have $F^1B_{\mathrm{cris}}^{\varphi^r=1} \neq 0$.

2.2. Application to surfaces. Let $E \to \operatorname{Spec}(W)$ be a smooth projective morphism with geometrically connected fibres of dimension 2. Let K_0^{ur} be the maximal unramified extension of K_0 in $\bar{K}$. The Kummer sequence gives an exact sequence of G_{K_0}-representations

$$0 \to NS(E_{\bar{K}}) \otimes \mathbb{Q}_p \to H^2_{\text{ét}}(E_{\bar{K}}, \mathbb{Q}_p)(1) \to V_p \operatorname{Br}(E_{\bar{K}}) \to 0$$

where $NS := \operatorname{Pic} / \operatorname{Pic}^0$ is the Néron–Severi group. By p-adic Hodge theory, applying the functor D_{cris} we get an exact sequence

$$0 \to D_{\mathrm{cris}}(NS(E_{\bar{K}})_{\mathbb{Q}_p}) \to H^2_{\mathrm{cris}}(E_k/K_0)[1] \to D_{\mathrm{cris}}(V_p \operatorname{Br}(E_{\bar{K}})) \to 0$$

where for a filtered φ-module D we denote $D[1]$ the filtered φ-module whose underlying K_0-module is D with $\varphi_{D[1]} := p^{-1}\varphi_D$ and $F^iD[1] := F^{i+1}D$. On the other hand, there is the specialisation map [3, Exp. X, appendice, 7.12]

$$\mathrm{sp} : NS(E_{\bar{K}}) \to NS(E_{\bar{k}})$$

which is G_{K_0}-equivariant and injective up to torsion. So $NS(E_{\bar{K}}) \otimes \mathbb{Q}_p$ is an unramified discrete representation of G_{K_0} hence is K_0^{ur}-admissible. Thus, $D_{\mathrm{cris}}(NS(E_{\bar{K}})_{\mathbb{Q}_p}) = (NS(E_{\bar{K}}) \otimes K_0^{\mathrm{ur}})^{\mathrm{Gal}(K_0^{\mathrm{ur}}/K_0)}$ (and similarly for $D_{\mathrm{cris}}(NS(E_{\bar{k}})_{\mathbb{Q}_p})$) and we have a commutative diagram

$$\begin{array}{ccc}
D_{\mathrm{cris}}(NS(E_{\bar{K}})_{\mathbb{Q}_p}) & \longrightarrow & H^2_{\mathrm{cris}}(E_k/K_0)[1] \\
\downarrow \mathrm{sp} & \nearrow c_1 & \\
D_{\mathrm{cris}}(NS(E_{\bar{k}})_{\mathbb{Q}_p}) & &
\end{array}$$

where c_1 is the first Chern class. In fact, c_1 is injective since

$$NS(E_{\bar{k}})_{\mathbb{Q}_p} \subset \left(H^2_{\mathrm{cris}}(E_k/K_0)[1] \otimes_{K_0} K_0^{\mathrm{ur}}\right)^{\varphi=1}$$

(cf. [11, II.5]). Therefore, defining $C := H^2_{\mathrm{cris}}(E_k/K_0)[1]/D_{\mathrm{cris}}(NS(E_{\bar{k}})_{\mathbb{Q}_p})$, we have a commutative diagram with exact rows

$$\begin{array}{ccccccccc}
0 & \longrightarrow & D_{\mathrm{cris}}(NS(E_{\bar{K}})_{\mathbb{Q}_p}) & \longrightarrow & H^2_{\mathrm{cris}}(E_k/K_0)[1] & \longrightarrow & D_{\mathrm{cris}}(V_p \operatorname{Br}(E_{\bar{K}})) & \longrightarrow & 0 \\
 & & \downarrow & & \| & & \downarrow & & \\
0 & \longrightarrow & D_{\mathrm{cris}}(NS(E_{\bar{k}})_{\mathbb{Q}_p}) & \longrightarrow & H^2_{\mathrm{cris}}(E_k/K_0)[1] & \longrightarrow & C & \longrightarrow & 0
\end{array}$$

and setting $M := D_{\mathrm{cris}}(NS(E_{\bar{k}})_{\mathbb{Q}_p})/D_{\mathrm{cris}}(NS(E_{\bar{K}})_{\mathbb{Q}_p})$ we deduce an exact sequence of φ-modules

$$0 \to M \to D_{\mathrm{cris}}(V_p \operatorname{Br}(E_{\bar{K}})) \to C \to 0.$$

Theorem 2.3. *Let* $D := D_{\mathrm{cris}}(V_p \operatorname{Br}(E_{\bar{K}}))$ *and* $T := \varphi + \varphi^{-1}$. *If*

$$D^{(\varphi-1)^2=0} = D^{\varphi=1}, \quad T(F^1D) \subset F^1D \quad \text{and} \quad V_p \operatorname{Br}(E_{\bar{K}})^{G_{K_0}} = 0,$$

then $M^{\varphi=1} = 0 = C^{\varphi=1}$.

Proof. By Poincaré duality, cup product is non-degenerate on $H^2_{\text{ét}}(E_{\bar{K}})(1)$ and, since numerical and algebraic equivalence coincide up to torsion for divisors [12, 9.6.17], it is also non-degenerate on $NS(E_{\bar{K}})_{\mathbb{Q}_p}$ and $NS(E_{\bar{k}})_{\mathbb{Q}_p}$. It follows that $V_p \operatorname{Br}(E_{\bar{K}}) \cong \left(NS(E_{\bar{K}})_{\mathbb{Q}_p}\right)^{\perp}$ has a canonical non-degenerate symmetric bilinear form we may apply Proposition 2.1 to obtain $D^{\varphi=1} = 0$. Moreover, the restriction of this form to M is non-degenerate since cup product is non-degenerate on both $D_{\mathrm{cris}}(NS(E_{\bar{K}})_{\mathbb{Q}_p})$ and $D_{\mathrm{cris}}(NS(E_{\bar{k}})_{\mathbb{Q}_p})$. Thus, $C \cong M^{\perp}$ and hence $C^{\varphi=1} = 0$. □

Corollary 2.4. *Under the assumptions of Theorem 2.3, Tate's conjecture holds for* E_k *and we have*

$$NS(E_{\bar{K}})^{G_{K_0}} \otimes \mathbb{Q} = NS(E_{\bar{k}})^{G_{K_0}} \otimes \mathbb{Q}.$$

Proof. Note that we have an exact sequence

$$0 \to D_{\mathrm{cris}}(NS(E_{\bar{K}})_{\mathbb{Q}_p})^{\varphi=1} \to D_{\mathrm{cris}}(NS(E_{\bar{k}})_{\mathbb{Q}_p})^{\varphi=1} \to M^{\varphi=1}$$

so since $M^{\varphi=1} = 0$ we find

$$\begin{aligned}(NS(E_{\bar{K}}) \otimes \mathbb{Q}_p)^{G_{K_0}} &= D_{\mathrm{cris}}(NS(E_{\bar{K}})_{\mathbb{Q}_p})^{\varphi=1} \\ &= D_{\mathrm{cris}}(NS(E_{\bar{k}})_{\mathbb{Q}_p})^{\varphi=1} \\ &= (NS(E_{\bar{k}}) \otimes \mathbb{Q}_p)^{G_{K_0}}\end{aligned}$$

as claimed. Tate's conjecture is well known [15] to be equivalent to the statement $C^{\varphi=1} = 0$. □

3. Elliptic modular surfaces

We fix throughout a positive integer N and a prime number p which does not divide N.

3.1. Definition. For $N \geq 3$, let $Y(N)$ to be moduli $\mathbb{Z}[1/N]$-scheme of elliptic curves with (full) level N structure and let $X(N)$ be its modular compactification. $X(N)$ classifies generalised elliptic curves with level N structure whose singular fibres are Néron N-gons. $X(N)$ is smooth over $\mathbb{Z}[1/N]$ and the normalisation of $\mathbb{Z}[1/N]$ in $X(N)$ is $\mathbb{Z}[\zeta_N, 1/N]$, where ζ_N

is a primitive Nth root of unity. See [6] for details. We denote the universal generalised elliptic curve by

$$g : E(N) \to X(N).$$

$E(N)$ is the *elliptic modular surface of level* N studied in [20]. That it is smooth over $\mathbb{Z}[1/N]$ follows from the results of [6, VII].

3.2. Application of Hodge theory. Assume $\zeta_N \in W$ (note that this is always true if $p \equiv 1 \mod N$, for then $\zeta_N^p = \zeta_N$, so $\zeta_N \in \mathbb{Z}_p$). To simplify the notation write

$$E := E(N) \otimes_{\mathbb{Z}[\zeta_N]} W, \qquad X := X(N) \otimes_{\mathbb{Z}[\zeta_N]} W,$$
$$Y := Y(N) \otimes_{\mathbb{Z}[\zeta_N]} W, \qquad \Sigma := X \setminus Y.$$

Let L be the conormal sheaf of the zero section of $g : E \to X$, and let $\omega = \Omega^1_X(\log \Sigma)$ denote the line bundle of differential forms on X with logarithmic poles along Σ.

Theorem 3.1 (Faltings [7])**.** *There are G_{K_0}-equivariant isomorphisms*

$$H^1(Y_{\bar{K}}, R^1 g_* \mathbb{Q}_p) \otimes_{\mathbb{Q}_p} \hat{\hat{K}} = H^1(X, L^{\otimes -1}) \otimes_W \hat{\hat{K}} \oplus H^0(X, L \otimes \omega) \otimes_W \hat{\hat{K}}(-2)$$
$$\widetilde{H}^1(Y_{\bar{K}}, R^1 g_* \mathbb{Q}_p) \otimes_{\mathbb{Q}_p} \hat{\hat{K}} = H^1(X, L^{\otimes -1}) \otimes_W \hat{\hat{K}} \oplus H^0(X, L \otimes \Omega^1_X) \otimes_W \hat{\hat{K}}(-2)$$

where $\widetilde{H}^1 := \mathrm{im}(H^1_c \to H^1)$ is the parabolic cohomology.

We shall use this result to determine the Hodge–Tate decomposition of $V_p \operatorname{Br}(E_{\bar{K}})$. Let $I \subset G_{K_0}$ be the inertia group.

Corollary 3.2. *$H^1(Y_{\bar{K}}, R^1 g_* \mathbb{Q}_p(1))$ is a Hodge–Tate representation with weights ± 1. In particular, $H^1(Y_{\bar{K}}, R^1 g_* \mathbb{Q}_p(1))^I = 0$.*

Corollary 3.3. *Let $E' = E \times_X Y$. Then*

(i) *$H^2(E'_{\bar{K}}, \mathbb{Q}_p(1)) = H^1(Y_{\bar{K}}, R^1 g_* \mathbb{Q}_p(1)) \oplus \mathbb{Q}_p e$, where e denotes the characteristic class of the zero section of g*

(ii) *$H^2(E_{\bar{K}}, \mathbb{Q}_p(1))^I$ is generated as a $\mathbb{Q}_p$-vector space by the characteristic classes of the irreducible components of singular fibres of g together with e.*

Proof. Since $Y_{\bar{K}}$ is an affine curve, the Leray spectral sequence

$$H^i(Y_{\bar{K}}, R^j g_* \mathbb{Q}_p(1)) \Rightarrow H^{i+j}(E'_{\bar{K}}, \mathbb{Q}_p(1))$$

gives an exact sequence

$$0 \to H^1(Y_{\bar{K}}, R^1 g_* \mathbb{Q}_p(1)) \to H^2(E'_{\bar{K}}, \mathbb{Q}_p(1)) \to H^0(Y_{\bar{K}}, R^2 g_* \mathbb{Q}_p(1)) \to 0$$

so $H^2(E'_{\bar{K}}, \mathbb{Q}_p(1))^I \subset H^0(Y_{\bar{K}}, R^2 g_* \mathbb{Q}_p(1)) = \mathbb{Q}_p$. In fact we must have equality since the class e of the zero section of g cannot be trivial. So e gives a splitting of the sequence, proving (i). For (ii) it suffices to note that the kernel of the map $H^2(E_{\bar{K}}, \mathbb{Q}_p(1)) \to H^2(E'_{\bar{K}}, \mathbb{Q}_p(1))$ is generated by the classes of the components of the fibres over the cusps. □

Note that combined with the Shioda–Tate formula [20, 1.5] this implies that the rank of the Mordell–Weil group of the generic fibre of g is zero, a result of Shioda [20, 5.1].

Corollary 3.4. *We have*

$$V_p \operatorname{Br}(E_{\bar{K}}) \otimes_{\mathbb{Q}_p} \hat{\bar{K}} = H^2(E, \mathcal{O}_E) \otimes \hat{\bar{K}}(1) \oplus H^0(E, \Omega^2_E) \otimes \hat{\bar{K}}(-1).$$

In particular, $V_p \operatorname{Br}(E_{\bar{K}})^I = 0$.

Proof. We have $V_p \operatorname{Br}(E_{\bar{K}}) \subset V_p \operatorname{Br}(E'_{\bar{K}})$ (cf. [10, II, 1.10]) and the latter is a quotient of $H^1(Y_{\bar{K}}, R^1 g_* \mathbb{Q}_p(1))$ by the last corollary, hence $V_p \operatorname{Br}(E_{\bar{K}})$ is a Hodge–Tate representation with weights contained in $\{\pm 1\}$. In particular, the map $H^1(E, \Omega^1_E) \otimes \hat{\bar{K}} \to V_p \operatorname{Br}(E_{\bar{K}}) \otimes_{\mathbb{Q}_p} \hat{\bar{K}}$ is zero, and so

$$H^2(E, \mathcal{O}_E) \otimes \hat{\bar{K}}(1) \oplus H^0(E, \Omega^2_E) \otimes \hat{\bar{K}}(-1) \to V_p \operatorname{Br}(E_{\bar{K}}) \otimes_{\mathbb{Q}_p} \hat{\bar{K}}$$

is surjective. Since

$$\begin{aligned}\dim_{\mathbb{Q}_p} V_p \operatorname{Br}(E_{\bar{K}}) &= \dim_{\mathbb{Q}_p} H^2(E_{\bar{K}}, \mathbb{Q}_p(1)) - \dim_{\mathbb{Q}_p} NS(E_{\bar{K}}) \otimes \mathbb{Q}_p \\ &\geq \dim_{\mathbb{Q}_p} H^2(E_{\bar{K}}, \mathbb{Q}_p(1)) - \dim_{\hat{\bar{K}}} H^1(E, \Omega^1_E) \otimes \hat{\bar{K}} \\ &= \dim_{\hat{\bar{K}}} H^2(E, \mathcal{O}_E) \otimes \hat{\bar{K}}(1) + \dim_{\hat{\bar{K}}} H^0(E, \Omega^2_E) \otimes \hat{\bar{K}}(-1)\end{aligned}$$

this implies the result. □

Corollary 3.5. *There is a canonical isomorphism*

$$V_p \operatorname{Br}(E_{\bar{K}}) = \widetilde{H}^1(Y_{\bar{K}}, R^1 g_* \mathbb{Q}_p(1)).$$

Proof. Let $E' := E \times_X Y$, $NS(E'_{\mathbb{C}}) := \operatorname{im}\big(NS(E_{\mathbb{C}}) \to H^2(E'(\mathbb{C}), \mathbb{Z}(1))\big)$, and write $V := \widetilde{H}^1(Y(\mathbb{C}), R^1 g_* \mathbb{Z}(1))$. By the classical Eichler–Shimura isomorphism (cf. Theorem 3.1), V is a weight 0 Hodge structure of type $\{(1,-1),(-1,1)\}$. We have $V \subset H^1(Y(\mathbb{C}), R^1 g_* \mathbb{Z}(1)) \subset H^2(E'(\mathbb{C}), \mathbb{Z}(1))$ and since $NS(E_{\mathbb{C}})$ is a Hodge structure of type $(0,0)$ (cf. Corollary 3.4) we have $(V \cap NS(E'_{\mathbb{C}})) \otimes \mathbb{Q} = 0$, hence $V \otimes \mathbb{Q} \subset H^2(E'(\mathbb{C}), \mathbb{Q}(1))/NS(E'_{\mathbb{C}}) \otimes \mathbb{Q}$.

Now, from the usual localisation sequence in singular cohomology we deduce an exact sequence

$$\begin{aligned}0 \to H^2(E(\mathbb{C}), \mathbb{Z}(1))/NS(E_{\mathbb{C}}) &\to H^2(E'(\mathbb{C}), \mathbb{Z}(1))/NS(E'_{\mathbb{C}}) \\ &\to \bigoplus_{x \in \Sigma(\mathbb{C})} H^3_{g^{-1}(x)}(E(\mathbb{C}), \mathbb{Z}(1)).\end{aligned}$$

By Poincaré duality $H^3_{g^{-1}(x)}(E(\mathbb{C}),\mathbb{Q}(1))^* = H^1(g^{-1}(x)(\mathbb{C}),\mathbb{Q}(1)) = \mathbb{Q}(1)$ (since $g^{-1}(x)$ is a Néron polygon), hence $\bigoplus_{x\in\Sigma(\mathbb{C})} H^3_{g^{-1}(x)}(E(\mathbb{C}),\mathbb{Z}(1))$ is a Hodge structure of weight 2 and therefore the map

$$V \to \bigoplus_{x\in\Sigma(\mathbb{C})} H^3_{g^{-1}(x)}(E(\mathbb{C}),\mathbb{Q}(1))$$

is zero. Thus,

$$V\otimes\mathbb{Q} \subset H^2(E(\mathbb{C}),\mathbb{Q}(1))/NS(E_{\mathbb{C}})_{\mathbb{Q}}.$$

Finally, by the Eichler–Shimura isomorphism (and Serre duality) we have $\dim V\otimes\mathbb{Q} = 2\dim H^0(X, L\otimes\Omega^1_X)$, and since $H^0(X, L\otimes\Omega^1_X) = H^0(E,\Omega^2_E)$ (cf. [18, Thm. 6.8]), from Corollary 3.4 (and Serre duality) we get $\dim V = \dim V_p \operatorname{Br}(E_{\bar{K}})$. As $\big(H^2(E(\mathbb{C}),\mathbb{Z}(1))/NS(E_{\mathbb{C}})\big)\otimes\mathbb{Q}_p = V_p\operatorname{Br}(E_{\bar{K}})$, we get $V\otimes\mathbb{Q}_p = V_p\operatorname{Br}(E_{\bar{K}})$. □

Remark 3.6. Shioda [20] shows that $H^1(E,\Omega^1_E)\otimes\hat{\bar{K}}$ is generated by the classes of divisors, which together with the Hodge–Tate decomposition gives another proof of Corollary 3.4. Combining this with Corollary 3.5, this gives another proof that $\widetilde{H}^1(Y_{\bar{K}}, R^1g_*\mathbb{Q}_p(1))$ is a Hodge–Tate representation with weights ±1.

3.3. Application of Hecke operators. The Eichler–Shimura congruence relation relates the pth Hecke operator T_p to the Frobenius morphism at p. We exploit this relationship to obtain the following

Theorem 3.7. *If $p\equiv 1 \mod N$ and $k=\mathbb{F}_p$, then $T := \varphi+\varphi^{-1}$ is an endomorphism of $D := D_{\mathrm{cris}}(V_p\operatorname{Br}(E_{\bar{K}}))$ which satisfies $T(F^1D)\subset F^1D$.*

Proof. Recall ([6, V, 1.14]) that there is a regular proper $\mathbb{Z}[1/N]$-scheme $X(N,p)$ (denoted $\mathcal{M}_{\Gamma(N)\cap\Gamma_0(p)}$ in loc. cit.; in [5] one only considers the dense open $M_{N,p} = \mathcal{M}^0_{\Gamma(N)\cap\Gamma_0(p)}$) classifying isomorphism classes of p-isogenies $\phi : (\mathcal{E},\alpha)\to(\mathcal{E}',\alpha')$ of generalised elliptic curves with level N structure. It is smooth away from p and has semistable reduction at p. It is equipped with two canonical (finite flat degree $p+1$) morphisms

$$q_1 : X(N,p)\to X(N) : \phi\mapsto(\mathcal{E},\alpha)$$
$$q_2 : X(N,p)\to X(N) : \phi\mapsto(\mathcal{E}',\alpha').$$

The universal object over $X(N,p)$ is a p-isogeny

$$\phi : q_1^*E \to q_2^*E$$

where $E\to X(N)$ is the universal curve. $X(N,p)$ is regular and has semistable reduction at p: its reduction is isomorphic to two copies of $X(N)_k$ meeting transversally at the supersingular points.

By definition (cf. [5, 3.18]), the Hecke correspondence T_p on E is the finite correspondence

$$\begin{array}{ccc} & q_1^*E & \\ {}^{q_1}\swarrow & & \searrow^{q_2\circ\phi} \\ E & & E \end{array}$$

(read from left to right). That is, T_p is the composition of the graph of $q_2 \circ \phi$ with the transpose of the graph of q_1 (these can be composed as in [14, 1A]).

Consider the open subsets $Y^h \subset X_k$ and $Y(p)^h \subset X(N,p)_k$, complement of the cusps (i.e. Σ) and the supersingular locus, and let $E^h := E \times_X Y^h$. Recall ([5, §4]) that $Y(p)^h$ is the disjoint union of two copies of Y^h. On one of these copies $T_p = F$ and on the other $T_p = I_p\,{}^{\mathrm{t}}F$, where F is the Frobenius of E^h, ${}^{\mathrm{t}}F$ is its transpose as a correspondence, and I_p is the (canonical extension to E of the) morphism of $X(N)$ defined $I_p(\mathcal{E},\alpha) := (\mathcal{E}, p\alpha)$ (loc. cit.). Thus, we have the Eichler–Shimura relation

$$T_p|_{E^h} = F + I_p\,{}^{\mathrm{t}}F.$$

Let $\Sigma^h := X_k \backslash Y^h$ and $Z := E_{\Sigma^h} \subset E_k$. We have a canonical exact sequence of rigid cohomology groups [2, 2.3.1]

$$H^2_{Z,\mathrm{rig}}(E_k/K_0) \to H^2_{\mathrm{rig}}(E_k/K_0) \xrightarrow{\lambda} H^2_{\mathrm{rig}}(E^h/K_0)$$

and by Poincaré duality [1] we have $H^2_{Z,\mathrm{rig}}(E_k/K_0) = H^2_{\mathrm{rig}}(Z/K_0)^*$. Moreover, since $\dim Z = 1$, for any smooth dense open $U \subset Z$ by loc. cit. we have

$$H^2_{\mathrm{rig}}(Z/K_0) = H^2_{c,\mathrm{rig}}(U/K_0) = H^0_{\mathrm{rig}}(U/K_0)^* = \prod_{C\in\pi_0(U)} H^0_{\mathrm{rig}}(C/K_0)^*$$

the product being over the irreducible components of Z. Thus, the kernel of λ is generated by the characteristic classes of the components of the fibres over the cusps and the supersingular locus. Note that these classes are specialisations of divisor classes of E_{K_0}: indeed, this is true for the components of the fibres over Σ by [6, VII, 2.5], and it is clear for the (smooth) supersingular fibres. Since $H^2_{\mathrm{cris}}(E_k/K_0) = H^2_{\mathrm{rig}}(E_k/K_0)$, $D_{\mathrm{cris}}(V_p\,\mathrm{Br}(E_{\bar{K}}))$ is therefore a quotient of $\mathrm{im}(\lambda)$. As $T_p = F + I_p\,{}^{\mathrm{t}}F$ on $H^2_{\mathrm{rig}}(E^h/K_0)$, this equality also holds on $D_{\mathrm{cris}}(V_p\,\mathrm{Br}(E_{\bar{K}}))$.

Now, since $p \equiv 1 \mod N$, I_p is the identity map and we obtain the relation

$$T_p|_{E^h} = F + {}^{\mathrm{t}}F.$$

Note that $p\varphi = F$ and ${}^{\mathrm{t}}FF = p^{\dim E_k} = p^2$, so $pT = T_p$ as endomorphisms of $D_{\mathrm{cris}}(V_p\,\mathrm{Br}(E_{\bar{K}}))$. Being defined over $\mathbb{Z}[1/N]$, the action of T_p

on $H^2_{\mathrm{dR}}(E_{K_0})$ respects the Hodge filtration, hence so does $\frac{1}{p}T_p = T$, which completes the proof. □

As a corollary we obtain Theorem 1.1.

Corollary 3.8. *Assume the partial semisimplicity conjecture for $E(N)_{\mathbb{F}_p}$. If $k = \mathbb{F}_p$ and $p \equiv 1 \mod N$, then*

(i) *Tate's conjecture holds for E_k*
(ii) $NS(E_{\bar{K}})^{G_{K_0}} \otimes \mathbb{Q} = NS(E_{\bar{k}})^{G_{K_0}} \otimes \mathbb{Q}$
(iii) *the Mordell–Weil group of the generic fibre of $E_k \to X_k$ is isomorphic to $(\mathbb{Z}/N)^2$.*

Proof. Note that the partial semisimplicity conjecture implies (PS) for $D_{\mathrm{cris}}(V_p \operatorname{Br}(E(N)_{\bar{K}}))$. So by Corollary 3.4 and Theorem 3.7, (i) and (ii) follow from Corollary 2.4. For (iii) it is enough to note that the torsion subgroup of the Mordell–Weil group is N-torsion, which follows from [18, Cor. 7.5]. □

3.4. Validity of (PS). We show that (PS) holds for $D_{\mathrm{cris}}(V_p \operatorname{Br}(E(N)_{\bar{K}}))$ for p in a set of density 1. Let $Y_1(N)$ denote the Deligne–Mumford moduli stack of triples $(\mathcal{E} \to S, P, P')$ where $\mathcal{E} \to S$ is an elliptic curve over a $\mathbb{Z}[1/N]$-scheme S, $P \in \mathcal{E}[N](S)$ a point of exact order N and $P' \in (\frac{\mathcal{E}[N]}{\langle P \rangle})(S) \cong \mu_N(S)$ a point of exact order N (cf. [6]). For $N \geq 5$ it is known to be a $\mathbb{Z}[1/N, \zeta_N]$-scheme with geometrically connected fibres. Let $g : E_1(N) \to Y_1(N)$ be the universal elliptic curve and consider $V_N := \widetilde{H}^1(Y_1(N)_{\bar{K}}, R^1 g_* \mathbb{Q}_p)(1)$. This makes sense for all $N \geq 1$ as the étale cohomology of a Deligne–Mumford stack; alternatively, if $N|M$ and $N \geq 5$ we have a canonical injective map $V_N \to V_M$ induced the inclusion of congruence subgroups $\Gamma_1(M) \subset \Gamma_1(N)$, and for $N < 5$ we can define $V_N := V_{Nl} \times_{V_{Nlm}} V_{Nm}$ for coprime integers l, m such that Nl and Nm are at least 5. We first explain why (PS) holds for $D_{\mathrm{cris}}(V_N)$ for p outside a set of primes of density zero, and then we shall see why this implies the same for $D_{\mathrm{cris}}(V_p \operatorname{Br}(E(N)_{\bar{K}}))$.

First of all, recall the Eichler–Shimura isomorphism (cf. [5, 2.10])

$$V_N \otimes \mathbb{C} = S_3(\Gamma_1(N)) \oplus \overline{S_3(\Gamma_1(N))}$$

giving the Hodge decomposition of V_N in terms of weight 3 cusp forms for $\Gamma_1(N)$. The Hodge structure V_N is canonically polarised (cf. [5, 3.20]), and the polarisation induces the Petersson product on $S_3(\Gamma_1(N))$.

Now, for every proper divisor d of N there are pairs of maps $\pi_i : V_{N/d} \to V_N$ $(i = 1, 2)$ defined just like for modular forms. (One map arises from the inclusion $\Gamma_1(N) \subset \Gamma_1(N/d)$ and the other from $\left(\begin{smallmatrix} d & 0 \\ 0 & 1 \end{smallmatrix}\right)\Gamma_1(N)\left(\begin{smallmatrix} d & 0 \\ 0 & 1 \end{smallmatrix}\right)^{-1} \subset \Gamma_1(N/d)$; cf. [13, VIII].) The image of these maps is a subspace V_N^{old} of V_N. The perfect pairing on V_N is non-degenerate on V_N^{old} and its orthogonal complement V_N^{new} corresponds to newforms. This follows from the analogous fact for cusp forms (loc. cit.) via Hodge theory. Furthermore, V_N^{new} splits under the action of the Hecke algebra as a direct sum

$$V_N^{\mathrm{new}} = \bigoplus_{i=1}^{m} V(f_i)$$

where $f_1, \ldots, f_m$ are a choice of representatives of the $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$-conjugacy classes of weight 3 normalised newforms for $\Gamma_1(N)$, and $V(f_i)(-1)$ is the p-adic representation of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ associated to f_i by Deligne [5]. The space $V(f_i)$ is free of rank 2 over $K_{f_i} \otimes \mathbb{Q}_p$, where K_{f_i} is the field of coefficients of f_i. Now, by induction on the number of prime divisors of N we may assume (PS) to hold for $D_{\mathrm{cris}}(V_N^{\mathrm{old}})$ for all p outside of a set of density zero, and it remains to consider $D_{\mathrm{cris}}(V_N^{\mathrm{new}}) = \bigoplus_{i=1}^{m} D_{\mathrm{cris}}(V(f_i))$.

Fix an integer $n \geq 1$. We claim that

$$D_{\mathrm{cris}}(V(f_i))^{(\varphi^n - 1)^2 = 0} = D_{\mathrm{cris}}(V(f_i))^{\varphi^n = 1}$$

for a set of primes p of density 1. It suffices to show this for $e \cdot V(f_i)$, where $e \in K_{f_i} \otimes \mathbb{Q}_p$ is a primitive idempotent; then $D_{\mathrm{cris}}(e \cdot V(f_i))$ is a 2-dimensional vector space over the field $e \cdot K_{f_i} \otimes \mathbb{Q}_p$ with linear Frobenius φ. Moreover, one easily sees that it is enough to show this with n replaced by a multiple; in particular we can assume that n is even. Assume for a contradiction that the claim does not hold. Then the minimal polynomial of φ^n is $(t-1)^2$. If f_i has CM, then φ^2 is diagonalisable (cf. [16, p. 41]), a contradiction. So we may assume f_i does not have CM. As both eigenvalues of φ^n are equal to 1 and the trace of φ is equal to $\frac{a_p}{p}$ where a_p is the pth coefficient of f_i (cf. [17, 1.2.4 (ii)]), we deduce that $a_p = (\zeta + \zeta')p$ for some nth roots of unity ζ, ζ'. By [19, Thm. 15] this can only happen for a set of primes of density zero (dependent on n). This proves the claim, which in turn implies the equality

$$D_{\mathrm{cris}}(V_N)^{(\varphi^n - 1)^2 = 0} = D_{\mathrm{cris}}(V_N)^{\varphi^n = 1} \tag{3.1}$$

for p in a set of density 1. We have nearly shown

Theorem 3.9. *Let $\mathbb{Q}[\zeta_N] \subset L$ be a finite extension. Then for every place v of L outside of set of density zero, the partial semisimplicity conjecture holds for the reduction of $E(N) \otimes_{\mathbb{Z}[\zeta_N]} L$ at v.*

Proof. Let n be a positive integer divisible by $[L(\zeta_{N^2}) : \mathbb{Q}]$. There is a finite étale morphism $Y_1(N^2) \otimes \mathbb{Q} \to Y(N) \otimes \mathbb{Q}$ arising from the inclusion $\left(\begin{smallmatrix} N & 0 \\ 0 & 1 \end{smallmatrix}\right)\Gamma_1(N^2)\left(\begin{smallmatrix} N & 0 \\ 0 & 1 \end{smallmatrix}\right)^{-1} \subset \Gamma(N)$. Thus, $D_{\mathrm{cris}}(\widetilde{H}^1(Y(N)_{\bar{K}}, R^1 g_* \mathbb{Q}_p(1))) = D_{\mathrm{cris}}(V_p \operatorname{Br}(E(N)_{\bar{K}}))$ is contained in $D_{\mathrm{cris}}(V_{N^2})$. From (3.1) we deduce that $D_{\mathrm{cris}}(V_p \operatorname{Br}(E(N)_{\bar{K}}))^{(\varphi^n - 1)^2 = 0} = D_{\mathrm{cris}}(V_p \operatorname{Br}(E(N)_{\bar{K}}))^{\varphi^n = 1}$ for a set of primes p of density 1. This easily implies partial semisimplicity. $\square$

Corollary 3.10. *The conclusions of Corollary 3.8 hold for all* $p \equiv 1 \mod N$ *outside of a set of density zero.*

References

[1] P. Berthelot, "Dualité de Poincaré et formule de Künneth en cohomologie rigide", *C. R. Math. Acad. Sci. Paris* **325** (1997), no. 5, p. 493-498.

[2] ———, "Finitude et pureté cohomologique en cohomologie rigide (avec un appendice par Aise Johan de Jong)", *Invent. Math.* **128** (1997), p. 329-377.

[3] P. Berthelot, A. Grothendieck & L. Illusie (eds.), *Théorie des intersections et théorème de Riemann–Roch (SGA 6)*, Lecture Notes in Mathematics, vol. 225, Springer, 1971.

[4] P. Colmez & J.-M. Fontaine, "Construction des représentations p-adiques semi-stables", *Invent. Math.* **140** (2000), p. 1-43.

[5] P. Deligne, "Formes modulaires et représentations l-adiques", in *Séminaire Bourbaki 1968/69*, Lecture Notes in Mathematics, vol. 179, Springer, 1971.

[6] P. Deligne & M. Rapoport, "Les schémas de modules de courbes elliptiques", in *Modular functions of one variable II*, Lecture Notes in Mathematics, vol. 349, Springer, 1973.

[7] G. Faltings, "Hodge–Tate structures and modular forms", *Math. Ann.* **278** (1987), p. 133-149.

[8] J.-M. Fontaine, "Le corps des périodes p-adiques", in *Périodes p-adiques*, Astérisque, vol. 223, Société Mathématique de France, 1994, p. 59-111.

[9] ———, "Représentations p-adiques semi-stables", in *Périodes p-adiques*, Astérisque, vol. 223, Société Mathématique de France, 1994, p. 113-184.

[10] A. Grothendieck, "Le groupe de Brauer", in *Dix exposés sur la cohomologie des schémas*, Advanced Studies in Pure Mathematics (Amsterdam), vol. 3, North-Holland, 1968.

[11] L. Illusie, "Complexe de de Rham–Witt et cohomologie cristalline", *Ann. Sci. Éc. Norm. Supér.* **12** (1979), p. 501-661.

[12] S. L. Kleiman, "The Picard scheme", in *Fundamental Algebraic Geometry*, Mathematical Surveys and Monographs, vol. 123, American Mathematical Society, 2005.

[13] S. Lang, *Introduction to Modular Forms (With two appendices, by D. B. Zagier and by W. Feit)*, Grundlehren der Mathematischen Wissenschaften, vol. 222, Springer, 1976.

[14] C. Mazza, V. Voevodsky & C. Weibel, *Lecture Notes on Motivic Cohomology*, Clay Mathematics Monographs, vol. 2, American Mathematical Society, 2006.

[15] J. S. Milne, "On a conjecture of Artin and Tate", *Ann. Math.* **102** (1975), p. 517-533.

[16] K. A. Ribet, "Galois representations attached to eigenforms with Nebentypus", in *Modular functions of one variable V*, Lecture Notes in Mathematics, vol. 601, Springer, 1977.

[17] A. J. Scholl, "Motives for modular forms", *Invent. Math.* **100** (1990), no. 2, p. 419-430.

[18] M. Schütt & T. Shioda, "Elliptic Surfaces", in *Algebraic geometry in East Asia – Seoul 2008*, Advanced Studies in Pure Mathematics, vol. 60, Mathematical Society of Japan, 2010, p. 51-160.

[19] J.-P. Serre, "Quelques applications du théorème de densité de Chebotarev", *Publ. Math., Inst. Hautes Étud. Sci.* **54** (1981), p. 123-201.

[20] T. Shioda, "On elliptic modular surfaces", *J. Math. Soc. Japan* **24** (1972), p. 20-59.

[21] ———, "Algebraic cycles on certain $K3$ surfaces in characteristic p", in *Manifolds–Tokyo 1973 (Proc. Internat. Conf., Tokyo, 1973)*, University of Tokyo Press, 1975, p. 357-364.

Rémi Lodh
Springer
4 Crinan St.
London N1 9XW, UK
E-mail: remi.shankar@gmail.com