Journal of Number Theory ••• (••••) •••–•••

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

On the arithmetic of elliptic curves and a homotopy limit problem

Igor Kriz [1]

ARTICLE INFO

Article history:
Received 3 October 2016
Received in revised form 18 August 2017
Accepted 19 August 2017
Available online xxxx
Communicated by S.J. Miller

Keywords:
Elliptic curves
Tate–Shafarevich group
Homotopy limit problem
Motivic cohomology
Etale cohomology

ABSTRACT

In this note, I study a comparison map between a motivic and étale cohomology group of an elliptic curve over $\mathbb{Q}$ just outside the range of Voevodsky's isomorphism theorem. I show that the property of an appropriate version of the map being an isomorphism is equivalent to certain arithmetical properties of the elliptic curve.

1. Introduction

The most well known theorem of motivic homotopy theory is Voevodsky's proof of the Beilinson–Lichtenbaum and Bloch–Kato conjectures [13]. In one form ([13], Theorem 6.17), this result states that for a pointed smooth simplicial scheme X, the natural homomorphism

$$\widetilde{H}^p_{Mot}(X, \mathbb{Z}/\ell(q)) \to \widetilde{H}^p_{\acute{e}t}(X, \mathbb{Z}/\ell(q)) \tag{1}$$

E-mail address: ikriz@umich.edu.

[1] Igor Kriz was supported by NSF grant DMS 1102614 and by a grant from the Simons Foundation, number 403297.

http://dx.doi.org/10.1016/j.jnt.2017.08.008
0022-314X/

is an isomorphism for $p \leq q$ and a monomorphism for $p = q + 1$.

The purpose of the present note is to study the map (1) when X is an elliptic curve over $\mathbb{Q}$, $p = 2$, $q = 1$. In this case, we know from Voevodsky's theorem that (1) is a monomorphism.

Theorem 1. *Let $X = E$ be an elliptic curve defined over $\mathbb{Q}$. Then the canonical homomorphism*

$$\widetilde{H}^2_{Mot}(E, \mathbf{Z}_\ell(1)) \to \widetilde{H}^2_{\text{ét}}(E, \mathbf{Z}_\ell(1))$$

where $\mathbf{Z}_\ell(1)$ denotes the homotopy limit of $\mathbb{Z}/\ell^k(1)$ in the category of motives (resp. étale motives) always has an uncountable cokernel.

The situation changes, however, if we work with finite models. For a large enough set S of primes in $\mathbb{Z}$, an elliptic curve E over $\mathbb{Q}$ has a smooth projective model over $\mathbb{Z}[S^{-1}]$, which we will denote by $E[S^{-1}]$.

Theorem 2. *Let $X = E$ be an elliptic curve defined over $\mathbb{Q}$. Then the canonical homomorphism*

$$\varinjlim_S \widetilde{H}^2_{Mot}(E[S^{-1}], \mathbf{Z}_\ell(1)) \to \varinjlim_S \widetilde{H}^2_{\text{ét}}(E[S^{-1}], \mathbf{Z}_\ell(1))$$

is an isomorphism if and only if $Ш(E)_{(\ell)}$ is finite and $rank_{\mathbb{Q}}(E) > 0$.

Remark. Both direct limits in the statement of the Theorem are in fact eventually constant.

Here

$$Ш(E) = \bigcap_\nu Ker(H^1(\mathbb{Q}, E) \to H^1(\mathbb{Q}_\nu, E_\nu))$$

(where the intersection is taken over all completions of $\mathbb{Q}$) is the *Tate–Shafarevich group*, the finiteness of which (even at one prime) is equivalent to the vanishing of the discrepancy between the rank of the group of rational points of E and its computable estimate (see, for example, [7] for an introduction).

We see easily (as reviewed in the next section) that for $p = 2$, $q = 1$, (1) is never an isomorphism for $X = S^0$. Therefore, it would never be an isomorphism for an elliptic curve if we took unreduced instead of reduced cohomology. It is worthwhile noting that philosophically speaking, by taking reduced cohomology, the weight of the motive in question increases by 1. If it increased by 2, we would be back in the range of Voevodsky's

Please cite this article in press as: I. Kriz, On the arithmetic of elliptic curves and a homotopy limit problem, J. Number Theory (2018), http://dx.doi.org/10.1016/j.jnt.2017.08.008

isomorphism theorem. Consequently, we are investigating a cohomology group which is really "just over the isomorphism line".

Let $T_\ell(E)$ be the ℓ-adic Tate module of E, i.e. the inverse limit of its ℓ^n-torsion. At some point in the proof, Theorem 2 is rephrased as the following statement in pure arithmetic:

Theorem 3. *Let E be an elliptic curve over $\mathbb{Q}$. Let ℓ be a prime. Then for a sufficiently large finite set of primes S in $\mathbb{Z}$, the Kummer map*

$$E(\mathbb{Z}[S^{-1}]) \otimes \mathbb{Z}_\ell \to H^1_{\text{ét}}(\mathbb{Z}[S^{-1}], T_\ell(E))$$

is an isomorphism if and only if $Ш(E)_{(\ell)}$ is finite and $rank_{\mathbb{Q}}(E) > 0$.

A reader interested only in arithmetic and not motivic cohomology can consider this statement only, and skip directly to Section 4. To the author, the motivic statement was the original motivation, which led to the observation. The author thanks J. Nekovář, C. Skinner and C. Weibel for discussions and for pointing out mistakes in earlier statements of this simple but tricky result, and for helping to correct them.

The present note is organized as follows: We review some notation and fix some definitions in the next section, and we give a more definitive statement of Theorem 2. In Section 3, we prove the easier of the two main implications of the theorem. In Section 4, we prove the harder implication, and also Theorem 3. Finally, in Section 5, we give an example where the statement of the harder implication can be proved by more elementary means.

2. Basic definitions and the main theorem

Let E be a smooth projective variety over a Noetherian scheme Z. We will mostly be interested in the case where

$$Z = Spec(\mathbb{Q}) \text{ or } Z = Spec(\mathbb{Z}[S^{-1}]) \text{ where } S \text{ is some finite set of primes.} \tag{2}$$

Let us begin with reviewing some notation. The Kummer short exact sequence of étale sheaves

$$0 \longrightarrow \mathbb{Z}/\ell^k(1) \longrightarrow \mathbb{G}_m \xrightarrow{\ell^k} \mathbb{G}_m \longrightarrow 0 \tag{3}$$

gives rise to a cofibration sequence in the derived category of étale sheaves

$$\mathbb{G}_m \xrightarrow{\ell^k} \mathbb{G}_m \xrightarrow{\phi_k} \mathbb{Z}/\ell^k(1)[1].$$

We then have the canonical homomorphism

Please cite this article in press as: I. Kriz, On the arithmetic of elliptic curves and a homotopy limit problem, J. Number Theory (2018), http://dx.doi.org/10.1016/j.jnt.2017.08.008

$$\phi_{k*} : H^1_{\acute{e}t}(E, \mathbb{G}_m) \to H^2_{\acute{e}t}(E, \mathbb{Z}/\ell^k(1)).$$

In this paper, we will make use of the derived categories of motives and the derived category of étale motives $\mathbf{DM}^-_{Nis}$, $\mathbf{DM}^-_{\acute{e}t}$ ([14,6]). Constant sheaves, $\mathbb{G}_m$, $\mathbb{Z}/\ell^k(1)$ are examples of étale sheaves with transfers, thereby defining objects of $\mathbf{DM}^-_{Nis}$, $\mathbf{DM}^-_{\acute{e}t}$. We will denote the corresponding objects of those categories by the same symbols. Smooth schemes over Z have well defined cohomology with coefficients in an object of $\mathbf{DM}^-_{Nis}$ or $\mathbf{DM}^-_{\acute{e}t}$. If the object of $\mathbf{DM}^-_{Nis}$ or $\mathbf{DM}^-_{\acute{e}t}$ comes from a homotopy invariant Nisnevich resp. étale sheaf with transfers, the cohomology with coefficients in the motive is the same as the corresponding Nisnevich (resp. étale) cohomology. Moreover, Nisnevich cohomology of smooth schemes with coefficients in homotopy invariant sheaves is the same as Zariski cohomology ([6], Proposition 13.9). We will refer to the latter simply as *motivic cohomology*. This justifies our identification of symbols, since we are solely interested in cohomology. We will decorate motivic resp. étale cohomology as H_{Mot}, $H_{\acute{e}t}$, thus eliminating the need to distinguish notations on the level of coefficients.

Next, in $\mathbf{DM}^-_{Nis}$, $\mathbf{DM}^-_{\acute{e}t}$, we shall write

$$\begin{aligned} \mathbf{Z}_\ell &= \operatorname{holim}_{\leftarrow} \mathbb{Z}/\ell^k \\ \mathbf{Z}_\ell(1) &= \operatorname{holim}_{\leftarrow} \mathbb{Z}/\ell^k(1). \end{aligned} \tag{4}$$

It is important to note that these are *not* the same objects as $\mathbb{Z}_\ell$, $\mathbb{Z}_\ell(1)$, which mean the Nisnevich or étale constant sheaf and its tensor with $\mathbb{Z}(1)$ respectively (or the associated Nisnevich or étale motive). For example, for $Z = Spec(k)$ where k is a field, by Theorem 4.1 of [6],

$$H^1(Spec(k), \mathbb{Z}_\ell(1)) = k^\times \otimes_{\mathbb{Z}} \mathbb{Z}_\ell,$$

which is in general not equal to

$$H^1(Spec(k), \mathbf{Z}_\ell(1)) = \lim_{\leftarrow}(k^\times/(k^\times)^{\ell^m}).$$

We have the usual $\lim^1$ exact sequence

$$0 \to \lim{}^1 H^{i-1}_{\acute{e}t}(E, \mathbb{Z}/\ell^k(1)) \to H^i_{\acute{e}t}(E, \mathbf{Z}_\ell(1)) \to \lim_{\leftarrow} H^i_{\acute{e}t}(E, \mathbb{Z}/\ell^k(1)) \to 0. \tag{5}$$

There is also a similar short exact sequence for the motivic groups. Étale cohomology groups with coefficients in $\mathbf{Z}_\ell(n)$ were first introduced by U. Jannsen [3].

Please cite this article in press as: I. Kriz, On the arithmetic of elliptic curves and a homotopy limit problem, J. Number Theory (2018), http://dx.doi.org/10.1016/j.jnt.2017.08.008

We have a canonical diagram

$$\begin{array}{ccc} H^1_{\acute{e}t}(E,\mathbb{G}_m) & \xrightarrow{\Phi} & H^2_{\acute{e}t}(E,\mathbf{Z}_\ell(1)) \\ & \searrow \quad \nearrow & \\ & H^1_{\acute{e}t}(E,\mathbb{G}_m)\otimes\mathbb{Z}_\ell. & \end{array} \tag{6}$$

Lemma 4. *We have the following isomorphisms both in* $\mathbf{DM}^-_{Nis}$ *and* $\mathbf{DM}^-_{\text{ét}}$*:*

$$\mathbb{Z}(1)\otimes\mathbf{Z}_\ell \xrightarrow{\simeq} \mathbf{Z}_\ell(1). \tag{7}$$

Proof. In the category of derived motives, $\mathbb{Z}(1) = \mathbb{G}_m[-1]$ is an invertible and hence strongly dualizable object with dual $\mathbb{Z}(-1)$, so we have

$$\mathbb{Z}(1)\otimes\mathbf{Z}_\ell = Hom(\mathbb{Z}(-1),\mathbf{Z}_\ell) =$$
$$\operatorname*{holim}_{\leftarrow} Hom(\mathbb{Z}(-1),\mathbb{Z}/\ell^m) = \operatorname*{holim}_{\leftarrow}\mathbb{Z}/\ell^m(1) = \mathbf{Z}_\ell(1),$$

as claimed. □

But also a smooth projective variety is strongly dualizable in the stable motivic homotopy category, and therefore its cohomology is equal to the homology of its dual. It follows that in the following comparison diagram, the top row (with notation analogous to the étale case) is an isomorphism in the case when E is an elliptic curve, and we have (2):

$$\begin{array}{ccc} H^1_{Mot}(E,\mathbb{G}_m)\otimes\mathbb{Z}_\ell & \xrightarrow[\Phi_{Mot}]{\cong} & H^2_{Mot}(E,\mathbf{Z}_\ell(1)) \\ \cong\downarrow{\scriptstyle \rho\otimes\mathbb{Z}_\ell} & & \downarrow{\scriptstyle \rho} \\ H^1_{\acute{e}t}(E,\mathbb{G}_m)\otimes\mathbb{Z}_\ell & \xrightarrow{\Phi} & H^2_{\acute{e}t}(E,\mathbf{Z}_\ell(1)). \end{array} \tag{8}$$

(To see that Φ_{Mot} is an isomorphism in (8), note that the group of rational points $E(\mathbb{Q})$ is a finitely generated abelian group. We have

$$H^2_{Mot}(E,\mathbb{Z}/\ell^m(1)) = E(\mathbb{Q})/\ell^m$$

by the Kummer exact sequence, while $H^1_{Mot}(E,\mathbb{Z}/\ell^m(1))$ is the ℓ^m-torsion subgroup of $E(\mathbb{Q})$, which is finite and hence the $\lim^1$ term vanishes in the motivic analogue of (5).)

On the other hand, the realization map

$$\rho : H^1_{Mot}(E,\mathbb{G}_m) \to H^1_{\acute{e}t}(E,\mathbb{G}_m)$$

Please cite this article in press as: I. Kriz, On the arithmetic of elliptic curves and a homotopy limit problem, J. Number Theory (2018), http://dx.doi.org/10.1016/j.jnt.2017.08.008

is well known to be an isomorphism (a version of Hilbert 90 theorem, see e.g. [8]). Therefore, the left column of diagram (8) is an isomorphism.

We must discuss another point. For a scheme X, one defines the *Brauer group*

$$Br(X) = H^2_{\acute{e}t}(X, \mathbb{G}_m).$$

Define also

$$T_\ell Br(X) = \lim_{\leftarrow} {}_{\ell^k} Br(X)$$

where ${}_n Br(X)$ is the n-torsion in $Br(X)$ (i.e. the subgroup of elements x where $nx = 0$). One writes $Br(R)$ instead of $Br(Spec(R))$.

As stated, there is no chance that the map ρ (or Φ) of diagram (8) would be an isomorphism. Let us consider the case of $Spec(R)$ where R is a number field or $\mathbb{Z}[S^{-1}]$. Then

$$H^1_{Mot}(Spec(R), \mathbb{G}_m) = 0,$$

and hence

$$H^2_{Mot}(Spec(R), \mathbf{Z}_\ell(1)) = 0, \tag{9}$$

whereas by (5), we have a short exact sequence

$$0 \to \lim{}^1 H^1_{\acute{e}t}(Spec(R), \mathbb{Z}/\ell^k(1)) \to H^2_{\acute{e}t}(Spec(R), \mathbf{Z}_\ell(1)) \\ \to \lim_{\leftarrow} H^2_{\acute{e}t}(Spec(R), \mathbb{Z}/\ell^k(1)) \to 0,$$

or, using (3),

$$0 \to \lim{}^1 R^\times / R^{\times \ell^k} \to H^2_{\acute{e}t}(Spec(R), \mathbf{Z}_\ell(1)) \to \lim_{\leftarrow} {}_{\ell^R} Br(R) \to 0.$$

The first term is clearly 0 (since the maps are onto), so we get

$$H^2_{\acute{e}t}(R, \mathbf{Z}_\ell(1)) \cong \lim_{\leftarrow} {}_{\ell^k} Br(R). \tag{10}$$

The right hand side of (10) is non-zero by class field theory. However, if E has a point over k, the map ρ from (9) to (10) is a retract of the map ρ in (8), so the map ρ cannot be an isomorphism. As customary, we will denote by $\widetilde{H}$ the kernel of either row of the diagram (8) to Z induced by a Z-point in E, and call this summand the corresponding *reduced cohomology group*.

Let $\ell = 2, 3, 5, \dots$ be a prime and let E be an elliptic curve defined over $\mathbb{Q}$. Denote by S the (finite) set of all primes in $\mathbb{Z}$ dividing the conductor of E. Note that by the criterion of Néron–Ogg–Shafarevich, $T_\ell(E)$ is unramified at all primes $p \notin S$, and the

Please cite this article in press as: I. Kriz, On the arithmetic of elliptic curves and a homotopy limit problem, J. Number Theory (2018), http://dx.doi.org/10.1016/j.jnt.2017.08.008

elliptic curve E has a smooth projective model over $\mathbb{Z}[S^{-1}]$, which we will denote by $E(\mathbb{Z}[S^{-1}])$.

Theorem 5. *The following are equivalent:*

(a) $Ш(E/\mathbb{Q}) \otimes \mathbb{Z}_{(\ell)}$ *is finite and* $rank_{\mathbb{Q}}(E) > 0$.
(b) *The realization map of diagram (8)*

$$\rho : \widetilde{H}^2_{Mot}(E(\mathbb{Z}[S^{-1}]), \mathbf{Z}_\ell(1)) \to \widetilde{H}^2_{\text{ét}}(E(\mathbb{Z}[S^{-1}]), \mathbf{Z}_\ell(1)) \tag{11}$$

is an isomorphism.
(c) *The map* ρ *of (11) is onto.*
(d) *The map*

$$\Phi : \widetilde{H}^1_{\text{ét}}(E(\mathbb{Z}[S^{-1}]), \mathbb{G}_m) \otimes \mathbb{Z}_\ell \to \widetilde{H}^2_{\text{ét}}(E(\mathbb{Z}[S^{-1}]), \mathbf{Z}_\ell(1)) \tag{12}$$

is an isomorphism.
(e) *The map* Φ *of (12) is onto.*
(f) *The map*

$$T_\ell Br(E(\mathbb{Z}[S^{-1}])) \to T_\ell Br(\mathbb{Z}[S^{-1}]) \tag{13}$$

induced by the inclusion of $0 \in E$ *is an isomorphism.*

3. Proof of the main theorem – the easy implication

Consider diagram (8) and the fact that the maps Φ, ρ when reduced mod ℓ^k become (by definition) isomorphisms. Since the source of Φ is a finitely generated $\mathbb{Z}_\ell$-module, it has no infinite ℓ-divisibility, which implies that Φ (and hence ρ) is injective. Therefore, we know that (b), (c), (d) and (e) of the statement are equivalent.

Let us prove that (b) implies the first statement of (a), i.e. that $Ш(E/\mathbb{Q}) \otimes \mathbb{Z}_{(\ell)}$ is finite. We follow [7], Chapter IV.2. Consider the diagram

Please cite this article in press as: I. Kriz, On the arithmetic of elliptic curves and a homotopy limit problem, J. Number Theory (2018), http://dx.doi.org/10.1016/j.jnt.2017.08.008

$$\begin{array}{ccccc} E(\mathbb{Q})/\ell E(\mathbb{Q}) & \xrightarrow{i_1} & S^{(\ell)}(E/\mathbb{Q}) & \xrightarrow{j_1} & H^1(\mathbb{Q}, {}_\ell E) \\ \uparrow{\scriptstyle \pi_1} & & \uparrow{\scriptstyle \alpha_1} & & \uparrow{\scriptstyle \gamma_1} \\ E(\mathbb{Q})/\ell^2 E(\mathbb{Q}) & \xrightarrow{i_2} & S^{(\ell^2)}(E/\mathbb{Q}) & \xrightarrow{j_2} & H^1(\mathbb{Q}, {}_{\ell^2} E) \\ \uparrow{\scriptstyle \pi_2} & & \uparrow{\scriptstyle \alpha_2} & & \uparrow{\scriptstyle \gamma_2} \\ E(\mathbb{Q})/\ell^3 E(\mathbb{Q}) & \xrightarrow{i_3} & S^{(\ell^3)}(E/\mathbb{Q}) & \xrightarrow{j_3} & H^1(\mathbb{Q}, {}_{\ell^3} E) \\ \uparrow{\scriptstyle \pi_3} & & \uparrow{\scriptstyle \alpha_3} & & \uparrow{\scriptstyle \gamma_3} \\ \vdots & & \vdots & & \vdots \end{array} \tag{14}$$

Here, as usual, ${}_nE$ denotes the n-torsion in E, and $S^{(n)}$ denotes the Selmer group, i.e. the kernel of the map

$$H^1(\mathbb{Q}, {}_nE) \to \prod_p H^1(\mathbb{Q}_p, E).$$

The maps i_n, j_n are inclusions, the π_n are projections (hence onto), and the other vertical maps are induced by projections. Since $Ш(E/\mathbb{Q})_{\ell^n}$ is a quotient of the finite group $S^{(\ell^n)}(E/\mathbb{Q})$, it is finite, so finiteness of $Ш(E/\mathbb{Q}) \otimes \mathbb{Z}_{(\ell)}$ is equivalent to the absence of infinitely ℓ-divisible non-zero elements in $Ш(E/\mathbb{Q})$. This, in turn, is equivalent to asserting that

$$i_1 : E(\mathbb{Q})/\ell E(\mathbb{Q}) \to \bigcap_n Im(\alpha_1\alpha_2 \dots \alpha_n) \text{ is onto.} \tag{15}$$

Clearly, (15) follows from

$$j_1 i_1 : E(\mathbb{Q})/\ell E(\mathbb{Q}) \to \bigcap_n Im(\gamma_1\gamma_2 \dots \gamma_n) \text{ is onto.} \tag{16}$$

We shall prove (16). We have

$$H^2_{Mot}(E, \mathbb{Z}(1)) \cong \mathbb{Z} \oplus E(\mathbb{Q})$$

where the first summand corresponds to the degree. More precisely, there is a short exact sequence of the form

$$0 \longrightarrow H^2_{Mot}(E, \mathbb{Z}(1))_0 \longrightarrow H^2_{Mot}(E, \mathbb{Z}(1)) \xrightarrow{deg} \mathbb{Z} \longrightarrow 0, \tag{17}$$

and there is a canonical isomorphism

$$H^2_{Mot}(E, \mathbb{Z}(1))_0 \cong E(\mathbb{Q}).$$

Please cite this article in press as: I. Kriz, On the arithmetic of elliptic curves and a homotopy limit problem, J. Number Theory (2018), http://dx.doi.org/10.1016/j.jnt.2017.08.008

We shall also be interested in the ℓ-adic version of (17):

$$0 \longrightarrow H^2_{Mot}(E, \mathbf{Z}_\ell(1))_0 \longrightarrow H^2_{Mot}(E, \mathbf{Z}_\ell(1)) \xrightarrow{deg} \mathbb{Z}_\ell \longrightarrow 0.$$

Now consider the diagram

$$\begin{array}{ccccc}
H^2(E(\mathbb{Z}[S^{-1}]), \mathbb{Z}/\ell\mathbb{Z}(1)) & \xrightarrow{\overline{r}} & \widetilde{H}^2_{\acute{e}t}(E(\mathbb{Z}[S^{-1}]), \mathbb{Z}/\ell\mathbb{Z}(1))_0 & \xrightarrow{\overline{u}} & H^1_{\acute{e}t}(\mathbb{Z}[S^{-1}], {}_\ell E) \\
\uparrow \subseteq & & \uparrow q & & \subseteq \uparrow s \\
E(\mathbb{Q})/\ell E(\mathbb{Q}) & \xrightarrow[r']{} & \widetilde{H}^2_{\acute{e}t}(E(\mathbb{Z}[S^{-1}], \mathbf{Z}_\ell(1))_0/(\ell) & \xrightarrow[u']{} & H^1_{\acute{e}t}(\mathbb{Z}[S^{-1}], T_\ell(E))/(\ell) \\
\uparrow \pi' & & \uparrow \gamma' \cong & & \uparrow \gamma \\
H^2_{Mot}(E(\mathbb{Q}), \mathbf{Z}_\ell(1))_0 & \xrightarrow{r} & \widetilde{H}^2_{\acute{e}t}(E(\mathbb{Z}[S^{-1}]), \mathbf{Z}_\ell(1))_0 & \xrightarrow{u} & H^1_{\acute{e}t}(\mathbb{Z}[S^{-1}], T_\ell(E)).
\end{array} \tag{18}$$

To explain this, first note that we have

$$H^2_{Mot}(E, \mathbf{Z}_\ell(1))_0/(\ell) = E(\mathbb{Q})/\ell E(\mathbb{Q}).$$

Next, the étale group with subscript 0 is defined in analogy with the corresponding motivic group, i.e. as the kernel of the degree map. The maps π', γ', γ are reductions mod ℓ, so they are onto. The map r is étale realization, and is an isomorphism by our assumption (b). The maps s, q are inclusions coming from the Bockstein long exact sequence associated with

$$0 \longrightarrow T_\ell(E) \xrightarrow{\ell} T_\ell(E) \longrightarrow {}_\ell E \longrightarrow 0$$

where $T_\ell(E)$ is the Tate module, i.e.

$$\lim_{\leftarrow} {}_{\ell^k} E,$$

which is non-canonically isomorphic to $\mathbb{Z}_\ell^2$. Now the map u comes from the Hochschild–Serre spectral sequence

$$E_2 = H^p_{\acute{e}t}(\mathbb{Z}[S^{-1}], H^q_{\acute{e}t}(E(K), \mathbf{Z}_\ell(1))) \Rightarrow H^{p+q}_{\acute{e}t}(E(\mathbb{Z}[S^{-1}]), \mathbf{Z}_\ell(1)) \tag{19}$$

where K is the maximal extension of $\mathbb{Q}$ over which all the primes outside of S are unramified. We have

$$T_\ell(E) = H^1_{\acute{e}t}(E(K), \mathbf{Z}_\ell(1)),$$

Please cite this article in press as: I. Kriz, On the arithmetic of elliptic curves and a homotopy limit problem, J. Number Theory (2018), http://dx.doi.org/10.1016/j.jnt.2017.08.008

so the $p = q = 1$ term is the target of u. Note (using purity) that the $p = 0, q = 2$ term is

$$H^0_{\acute{e}t}(\mathbb{Z}[S^{-1}], \mathbf{Z}_\ell) = \mathbb{Z}_\ell,$$

and the edge map in $p + q = 2$ is the degree map. Note also that the $p = 2$, $q = 0$ term is

$$H^2_{\acute{e}t}(\mathbb{Z}[S^{-1}], \mathbf{Z}_\ell(1));$$

the canonical map of the right hand side to $H^2_{\acute{e}t}(E(\mathbb{Z}[S^{-1}]), \mathbb{Z}_\ell(1))$ is the edge map. Therefore, since E contains a point over $\mathbb{Z}[S^{-1}]$, the projection given by the spectral sequence

$$H^2_{\acute{e}t}(E(\mathbb{Z}[S^{-1}]), \mathbf{Z}_\ell(1))_0 \to H^1_{\acute{e}t}(\mathbb{Z}[S^{-1}], T_\ell(E))$$

factors through an injection

$$u : \widetilde{H}^2_{\acute{e}t}(E(\mathbb{Z}[S^{-1}]), \mathbf{Z}_\ell(1))_0 \to H^1_{\acute{e}t}(\mathbb{Z}[S^{-1}], T_\ell(E)).$$

The map $\overline{u}$ is defined as the corresponding map for the analogous spectral sequence $\overline{E}^r_{pq}$ with coefficients reduced mod ℓ.

At this point, let us first assume that $\ell \neq 2$. Then u is onto since the only possible differential of (19) originating at $p = q = 1$ has target

$$H^3_{\acute{e}t}(\mathbb{Z}[S^{-1}], H^0_{\acute{e}t}(E(K), \mathbf{Z}_\ell(1))) = 0.$$

Next, observe that by the Bockstein spectral sequence,

$$Im(s\gamma) = \bigcap_n \gamma_1 \dots \gamma_n, \tag{20}$$

while

$$su'r' = j_1 i_1. \tag{21}$$

In effect, to prove (21), let us spell out the definition of $j_1 i_1$: Take $x \in E(\mathbb{Q})$, and set

$$y = \sqrt[\ell]{x} \in E. \tag{22}$$

Then define a 1-cocycle on $Gal(\mathbb{Q})$ by setting

$$g \mapsto \frac{g(y)}{y}. \tag{23}$$

Please cite this article in press as: I. Kriz, On the arithmetic of elliptic curves and a homotopy limit problem, J. Number Theory (2018), http://dx.doi.org/10.1016/j.jnt.2017.08.008

Now the analogue $\overline{E}^r_{p,q}$ of (19) with coefficients reduced mod ℓ has a motivic analogue ${}_{Mot}\overline{E}^r_{p,q}$ (although we do not know whether it converges). Nevertheless, we have a realization map of exact couples, and hence spectral sequences

$$ {}_{Mot}\overline{E}^r_{p,q} \to \overline{E}^r_{p,q}. \tag{24}$$

On $r = 2$, $p = q = 1$, and $r = 2$, $p = 0$, $q = 2$, the map (24) is an isomorphism. Now on the level of mod ℓ motivic cohomology, the definition corresponding to (22) and (23) is equal to $\overline{ur}$ by the definition of the exact couple which produces ${}_{Mot}\overline{E}^r_{p,q}$, which proves (21).

Now since u, γ are onto and r is an isomorphism, $u'r'$ is onto, and so is γ, so

$$Im(s\gamma) = Im(su's') = Im(s).$$

Therefore, (20) and (21) imply (16).

Now let us treat the case $\ell = 2$. We see that all that remains to show is that u is onto, which follows from the following Lemma.

Lemma 6. *In the Hochschild–Serre spectral sequence (19), we have*

$$\begin{array}{c} H^1_{\text{ét}}(\mathbb{Z}[S^{-1}], H^1_{\text{ét}}(E(K), \mathbf{Z}_2(1))) = H^1_{\text{ét}}(\mathbb{Z}[S^{-1}], T_2(E)) \\ \Big\downarrow {\scriptstyle d_2=0} \\ H^3_{\text{ét}}(\mathbb{Z}[S^{-1}], H^0_{\text{ét}}(E(K), \mathbf{Z}_2(1))) = H^3_{\text{ét}}(\mathbb{Z}[S^{-1}], \mathbf{Z}_2(1)). \end{array} \tag{25}$$

Proof. We have a restriction comparison diagram

$$\begin{array}{ccc} H^1_{\acute{e}t}(\mathbb{Z}[S^{-1}], H^1_{\acute{e}t}(E(K), \mathbf{Z}_2(1))) & \xrightarrow{d_2} & H^3_{\acute{e}t}(\mathbb{Z}[S^{-1}], H^0_{\acute{e}t}(E(K), \mathbf{Z}_2(1))) \\ \Big\downarrow & & \Big\downarrow \cong \\ H^1(\mathbb{R}, H^1_{\acute{e}t}(\overline{E}, \mathbf{Z}_2(1))) & \xrightarrow{d_2} & H^3(\mathbb{R}, H^0_{\acute{e}t}(\overline{E}, \mathbf{Z}_2(1))) \end{array}$$

where the right hand column is an isomorphism by Theorem B, p. 108 of [10]. Thus, we may replace $\mathbb{Q}$ by $\mathbb{R}$ in (25).

Then, however, we are dealing with a spectral sequence isomorphic to the Borel cohomology spectral sequence for the $\mathbb{Z}/2\mathbb{Z}$-action by complex conjugation on a (complexified) real elliptic curve, i.e. $E_{\mathbb{C}} = \mathbb{C}^\times/q^{\mathbb{Z}}$, $q \in \mathbb{R}$, $0 < q < 1$. We see then that topologically $\mathbb{Z}/2\mathbb{Z}$-equivariantly, we have

$$E \cong S^1 \times S^\alpha \tag{26}$$

where α is the sign representation and S^V is the one point compactification of a representation V. But stably (i.e. after taking suspension spectra), (26) splits as

Please cite this article in press as: I. Kriz, On the arithmetic of elliptic curves and a homotopy limit problem, J. Number Theory (2018), http://dx.doi.org/10.1016/j.jnt.2017.08.008

$$S^0 \vee S^1 \vee S^\alpha \vee S^{1+\alpha},$$

and hence the Borel cohomology spectral sequence collapses. □

4. The hard implication

Thus, we have shown that (b) implies the first statement of (a) To complete the proof, we will show that (a) implies (e), and that (e) together with the finiteness of $Ш(E/\mathbb{Q}) \otimes \mathbb{Z}_{(\ell)}$ implies $rank_{\mathbb{Q}}(E) > 0$.

We shall make use of the following

Lemma 7. *Let E be an elliptic curve defined over $\mathbb{Q}$. Let ℓ, p be primes. Then*

$$H^1(\mathbb{Q}_p, T_\ell(E)) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell \cong \begin{cases} 0 & \text{if } p \neq \ell \\ \mathbb{Q}_p \oplus \mathbb{Q}_p & \text{if } p = \ell \end{cases} \tag{27}$$

Proof. Let

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

We can use the Euler characteristic formula for local Galois cohomology [10] 5.7, Theorem 5 together with the fact that

$$V_\ell(E)^{Gal(\mathbb{Q}_\ell)} = 0, \tag{28}$$

and that

$$Hom_{\mathbb{Q}_\ell}(V_\ell(E), \mathbb{Q}_\ell)(1) \cong V_\ell(E) \tag{29}$$

as Galois representations.

(To prove (28), note that the same claim holds for every extension of $\mathbb{Q}_p$, and we will prove it in this case. By semi-stable reduction we may reduce to the cases, by taking a finite extension of the base field, if it is necessary, when E has either good or split multiplicative reduction. In the first case by p-adic Hodge theory the claim fails then the rigid cohomology of degree 1 of the reduction of $E \mod p$ has a trivial factor as an F-isocrystal. This is not possible by the Weil conjectures [2]. In the other case one can use the Tate uniformisation (cf. [11] Section V.2) of E to describe the Tate module of E as a non-trivial extension of $\mathbb{Q}_p(1)$ by $\mathbb{Q}_p$, and hence there are no invariants in this case either.)

The Euler characteristic formula is stated for finite modules in [10], but one can look at $T_\ell(E)/(\ell^m)$ and pass to the limit to get a statement about ranks. For any continuous $\mathbb{Z}_\ell[Gal(\mathbb{Q}_p)]$-module T satisfying (28) and (29), $V = T \otimes_{\mathbb{Z}_p} (\mathbb{Q}_p)$, the rank of $H^1(\mathbb{Q}_p, V)$ over $\mathbb{Q}_\ell$ is 0 for $\ell \neq p$ and is equal to $rank_{\mathbb{Q}_p}(V)$ for $\ell = p$ and 0 otherwise. □

Please cite this article in press as: I. Kriz, On the arithmetic of elliptic curves and a homotopy limit problem, J. Number Theory (2018), http://dx.doi.org/10.1016/j.jnt.2017.08.008

Now the inverse limit of the short exact sequences

$$0 \longrightarrow E_{\ell^k} \longrightarrow E \xrightarrow{\ell^k} E \longrightarrow 0 \tag{30}$$

has the form

$$0 \to T_\ell(E) \to \lim_{\leftarrow} E \to E \to 0. \tag{31}$$

(Again, there is no $\lim^1$ since the maps are onto.) Observe now that the first map factors as follows:

$$\begin{array}{ccc} T_\ell(E) & \longrightarrow & \lim_{\leftarrow} E \\ & \searrow \quad \nearrow & \\ & T_\ell(E) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell & \end{array} \tag{32}$$

Therefore, Lemma 7 has the following

Corollary 8. *The connecting map of (31)*

$$\delta = \delta_p : E(\mathbb{Q}_p) \to H^1(\mathbb{Q}_p, T_\ell(E)) \tag{33}$$

is onto for $p \neq \ell$ and for $p = \ell$, if $xp \in Im(\delta)$ with $x \in H^1(\mathbb{Q}_p, T_p(E))$, then $x \in Im(\delta)$.

Proof. For $p = \ell$, if $x \notin Im(\delta)$, then x maps to a non-zero element of $H^1(\mathbb{Q}_p, \lim_{\leftarrow} E)$, so xp maps to a non-zero element of $H^1(\mathbb{Q}_p, \lim_{\leftarrow} E)$, contradicting $xp \in Im(\delta)$. □

We also note that $Coker(\delta_\ell)$ is equal to $T_\ell H^1(\mathbb{Q}_\ell, E)$, which is torsion-free (in fact, isomorphic to $\mathbb{Z}_\ell$).

Now by our earlier discussion of the Hochschild–Serre spectral sequence (19), (e) is equivalent to the statement that

$$\delta_{\mathbb{Q}} : E(\mathbb{Q}) \otimes \mathbb{Z}_p \to H^1_{\acute{e}t}(\mathbb{Z}[S^{-1}], T_p(E)) \tag{34}$$

(which is injective) is onto, and to the statement of Theorem 3.

Lemma 9. *The inclusion of a ℓ-decomposition subgroup in $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ induces a homomorphism*

$$H^1_{\text{ét}}(\mathbb{Z}[S^{-1}], V_\ell(E)) \to H^1(\mathbb{Q}_\ell, V_\ell(E)) \tag{35}$$

whose image is isomorphic to $\mathbb{Q}_\ell$.

Please cite this article in press as: I. Kriz, On the arithmetic of elliptic curves and a homotopy limit problem, J. Number Theory (2018), http://dx.doi.org/10.1016/j.jnt.2017.08.008

Proof. Again, it is true more generally for any continuous $\mathbb{Z}_\ell[Gal(K/\mathbb{Q})]$-module T, $V = T \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$, satisfying (28) and (29) that for $p = \ell$, (35) is an inclusion whose image has $\mathbb{Q}_p$-rank equal to $rank_{\mathbb{Q}_p}(V)/2$. The Poitou–Tate exact sequence [12,9] is usually stated for a finite continuous $Gal(K/\mathbb{Q})$-module M:

$$\begin{array}{ccccccc} 0 & \longrightarrow & H^0_{\acute{e}t}(\mathbb{Z}[S^{-1}], M) & \longrightarrow & \prod_{p\in S} H^0(\mathbb{Q}_p, M) & \longrightarrow & H^2_{\acute{e}t}(\mathbb{Z}[S^{-1}], M')^* \\ & & & & & & \downarrow \\ & & H^1_{\acute{e}t}(\mathbb{Z}[S^{-1}], M')^* & \longleftarrow & \prod'_{p\in S} H^1(\mathbb{Q}_p, M) & \longleftarrow & H^1_{\acute{e}t}(\mathbb{Z}[S^{-1}], M) \\ & & \downarrow & & & & \\ & & H^2_{\acute{e}t}(\mathbb{Z}[S^{-1}], M) & \longrightarrow & \bigoplus_{p\in S} H^2(\mathbb{Q}_p, M) & \longrightarrow & H^0_{\acute{e}t}(\mathbb{Z}[S^{-1}], M')^* \longrightarrow 0 \end{array} \tag{36}$$

where M' denotes the Pontrjagin dual and $\prod'$ the restricted product (of course, in the present case, they are the same thing, since S is finite). Our statement can be proved by replacing T with $T/(\ell^m)$ and passing to the limit, also considering the fact that the Tate module is self-dual. □

Since the groups

$$H^0_{\acute{e}t}(\mathbb{Z}[S^{-1}], E_{\ell^k})$$

are finite, there is no $\lim^1$ term, and we have

$$H^1_{\acute{e}t}(\mathbb{Z}[S^{-1}], T_\ell(E)) = \lim_{\leftarrow} H^1_{\acute{e}t}(\mathbb{Z}[S^{-1}], E_{\ell^k}).$$

Therefore, for (34), it suffices to prove that the connecting map of (30)

$$E(\mathbb{Q}) \to Im(H^1_{\acute{e}t}(\mathbb{Z}[S^{-1}], T_\ell(E)) \to H^1_{\acute{e}t}(\mathbb{Z}[S^{-1}], E_{\ell^k})) \tag{37}$$

is onto. Take an element $x \in H^1_{\acute{e}t}(\mathbb{Z}[S^{-1}], T_\ell(E))$. By Corollary 8, the image of x in $H^1(\mathbb{Q}_\ell, T_\ell(E))$ is in the image of the connecting map (33) if and only if this is true rationally, i.e. if

$$\begin{array}{l} \text{The image of every element } x \in H^1_{\acute{e}t}(\mathbb{Z}[S^{-1}], V_\ell(E)) \text{ in } H^1(\mathbb{Q}_\ell, V_\ell(E)) \\ \text{is in the image of the connecting map} \\ \delta : E(\mathbb{Q}_\ell)\widehat{\otimes}\mathbb{Q}_\ell \to H^1(\mathbb{Q}_\ell, V_\ell(E)). \end{array} \tag{38}$$

If $rank_{\mathbb{Q}}(E) > 0$, then certainly (38) is true: By Lemma 9, the image of $H^1_{\acute{e}t}(\mathbb{Z}[S^{-1}], V_\ell(E))$ in $H^1(\mathbb{Q}_\ell, V_\ell(E))$ is a 1-dimensional (over $\mathbb{Q}_\ell$) subspace of $H^1(\mathbb{Q}_\ell, V_\ell(E))$ and if

Please cite this article in press as: I. Kriz, On the arithmetic of elliptic curves and a homotopy limit problem, J. Number Theory (2018), http://dx.doi.org/10.1016/j.jnt.2017.08.008

$$rank_{\mathbb{Q}}(E) > 0,$$

then a 1-dimensional $\mathbb{Q}_p$-subspace of the target of δ in (38) comes from the connecting map (34).

If (38) holds, noting that $p = \ell$, then the reduction x_m of our element $x \mod \ell^m$ is in the image of the connecting map. This means that

$$x_m \in S^{(\ell^m)}(E/\mathbb{Q}). \tag{39}$$

Therefore, assuming Ш has no ℓ-divisibility beyond ℓ^s, we see from (39) that $x_k = x_{k+s+1} \mod \ell^k$ is in the image of the connecting map (34), as claimed.

(Note that, in general, an element $x \in H^1_{\acute{e}t}(\mathbb{Z}[S^{-1}], T_\ell(E))$ lies in the ℓ-adic Selmer group $S_\ell = \varprojlim S^{(\ell^m)}$ if and only if $x_\ell \notin Im(\delta_\ell)$ (provided $\ell \neq 2$). Furthermore, $S_\ell/Im(\delta_{\mathbb{Q}}) = T_\ell Ш(E/\mathbb{Q})$, which means that $S_\ell = Im(\delta_{\mathbb{Q}})$ if and only if $Ш(E/\mathbb{Q}) \otimes \mathbb{Z}_{(\ell)}$ is finite.)

This completes the proof that (a) implies (e).

To prove that (e) implies that $rank_{\mathbb{Q}}(E) > 0$, note that we can assume $Ш(E)_{(\ell)} < \infty$, since we already proved that (e) implies it. Therefore, we have an isomorphism

$$E(\mathbb{Q}) \otimes \mathbb{Q}_\ell \xrightarrow{\cong} H^1_{\acute{e}t}(\mathbb{Z}[S^{-1}], V_\ell E). \tag{40}$$

On the other hand, the right hand side of (40) has non-zero $\mathbb{Q}_\ell$-rank, since by Lemma 9, its image in (35) has $\mathbb{Q}_\ell$-rank 1.

The following proof that (f) is equivalent to (b) was pointed out to me by C.Weibel: We have

$$H^2_{\acute{e}t}(E(\mathbb{Z}[S^{-1}]), \mathbb{Z}/\ell^k(1)) = Pic(E)/\ell^k, \tag{41}$$

$$H^2_{\acute{e}t}(E(\mathbb{Z}[S^{-1}]), \mathbb{Z}/\ell^k(1)) = Pic(E)/\ell^k \oplus {}_{\ell^k} Br(E(\mathbb{Z}[S^{-1}]) \tag{42}$$

(by the long exact sequence in cohomology associated with the short exact sequence of sheaves (3)). Also, we have

$$H^1_{\acute{e}t}(E(\mathbb{Z}[S^{-1}]), \mathbb{Z}/\ell^k(1)) =$$
$$\mathbb{Q}^*/\mathbb{Q}^{*\ell^k} \oplus {}_{\ell^k} Pic(E) \cong H^1_{\acute{e}t}(E(\mathbb{Z}[S^{-1}]), \mathbb{Z}/\ell^k(1)).$$

Now consider the diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \varprojlim{}^1 H^1(E(\mathbb{Z}[S^{-1}], \mathbb{Z}/\ell^k(1)) & \longrightarrow & H^2(E(\mathbb{Z}[S^{-1}]), \mathbf{Z}_\ell(1)) & \longrightarrow & \varprojlim H^2_{\acute{e}t}(E(\mathbb{Z}[S^{-1}]), \mathbb{Z}/\ell^k(1)) & \longrightarrow & 0 \\
 & & \downarrow \cong & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \varprojlim{}^1 H^1_{\acute{e}t}(E(\mathbb{Z}[S^{-1}]), \mathbb{Z}/\ell^k(1)) & \longrightarrow & H^2_{\acute{e}t}(E(\mathbb{Z}[S^{-1}]), \mathbf{Z}_\ell(1)) & \longrightarrow & \varprojlim H^2_{\acute{e}t}(E(\mathbb{Z}[S^{-1}]), \mathbb{Z}/\ell^k(1)) & \longrightarrow & 0.
\end{array}$$

Please cite this article in press as: I. Kriz, On the arithmetic of elliptic curves and a homotopy limit problem, J. Number Theory (2018), http://dx.doi.org/10.1016/j.jnt.2017.08.008

Using (41) and (42), we obtain

$$Coker(H^2(E(\mathbb{Z}[S^{-1}]), \mathbf{Z}_\ell(1)) \to H^2_{\acute{e}t}(E(\mathbb{Z}[S^{-1}), \mathbf{Z}_\ell(1)))$$
$$= T_\ell Br(E(\mathbb{Z}[S^{-1}])).$$

Of course, one can make the same calculation with E replaced by $Spec(\mathbb{Q})$, and naturality then gives that (f) is equivalent to (b). □

Finally, let us see why these arguments do not work with

$$H^1_{\acute{e}t}(\mathbb{Z}[S^{-1}], T_p(E))$$

replaced by the global Galois cohomology group $H^1(\mathbb{Q}, T_p(E))$. First, we note that (36) in fact holds for a finite module M without assuming that S is finite. Thus, we may replace S by the set of all primes in $\mathbb{Q}$, which amounts to replacing $\mathbb{Z}[S^{-1}]$ by $\mathbb{Q}$. Going even further, we see that the relevant $\lim_{\leftarrow}{}^1$-terms in this case are also 0, so even (36) remains valid with $\mathbb{Z}[S^{-1}]$ replaced by $\mathbb{Q}$.

The problem, however, is that the cohomology group $H^1(\mathbb{Q}, T_p(E))$ is huge: for S equal to the set of all primes in $\mathbb{Q}$, $M = T_\ell(E)/(\ell^k)$, we can find infinitely many primes p for which $E(\mathbb{Q}_p)$ has ℓ^k-torsion: By Chebotarev density theorem, it suffices to choose primes p at which $T_\ell(E)$ is unramified, and for which the Frobenius acts trivially on the field obtained by attaching the ℓ^k-E-torsion to $\mathbb{Q}$. In the inverse limit of the middle term (36) in the case when S contains all primes in $\mathbb{Q}$, then, the inverse limit of these infinite products of ℓ^k-torsion modules over diminishing sets of primes will create an uncountable non-torsion submodule, which must come from an uncountable torsion submodule of $H^1(\mathbb{Q}, T_\ell(E))$ by the exactness of the limit of (36). In view of the above discussion, this also proves Theorem 1. We remark that this argument is similar to the method of Kolyvagin [5].

5. An example

In this Section, we give an example where we can show for an elliptic curve that (38) is false directly. In the example, the conclusion can be made by Galois cohomology computations, thus in particular showing directly that $rank_{\mathbb{Q}}(E) = 0$ for any elliptic curve over $\mathbb{Q}$ with the same Galois data.

The elliptic curve over $\mathbb{Q}$ given by the equation

$$y^2 = x^3 + x^2 - 117x - 541$$

has conductor $N = 2^4 \cdot 11^2$, CM (0 rank), torsion 1 and ordinary good reduction at 3 (see the Cremona tables at http://johncremona.github.io/ecdata/). Looking at the smallest number field K over which E has $\mathbb{Z}/9 \times \mathbb{Z}/9$ torsion, one sees that

$$G = Gal(K/\mathbb{Q}) \cong \mathbb{Z}/6 \times \Sigma_3.$$

Please cite this article in press as: I. Kriz, On the arithmetic of elliptic curves and a homotopy limit problem, J. Number Theory (2018), http://dx.doi.org/10.1016/j.jnt.2017.08.008

The 3-decomposition subgroup of G is the normal subgroup

$$G_3 = \mathbb{Z}/6 \times \mathbb{Z}/3.$$

The representation of G on $T_3(E)/(9)$ can be described (up to isomorphism) as follows: the generator of the $\mathbb{Z}/6$-factor acts by

$$\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix},$$

the generator of the $\mathbb{Z}/3$-subgroup of Σ_3 acts by

$$\begin{pmatrix} 4 & 0 \\ 0 & 7 \end{pmatrix},$$

the generator σ of a $\mathbb{Z}/2$-subgroup of Σ_3 acts by

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

(The author obtained these results using SAGE.) Let $\Gamma = Gal(\mathbb{Q})$, and let $\Gamma_{(3)} \cong Gal(\mathbb{Q}_3)$ be a 3-decomposition subgroup. Let also Γ_3 be the pullback of Γ by $G_3 \to G$. Then we have inclusions

$$\Gamma_{(3)} \subset \Gamma_3 \subset \Gamma.$$

Lemma 10. *The restriction*

$$H^1(\Gamma_3, T_3(E)/(9)) \to H^1(\Gamma_{(3)}, T_3(E)/(9)) \cong \mathbb{Z}/9 \times \mathbb{Z}/9$$

is an isomorphism.

Proof. Once again, we know that the group $H^1(\Gamma_{(3)}, T_3(E)/(9))$ is isomorphic to $\mathbb{Z}/9 \times \mathbb{Z}/9$ by the Euler characteristic formula ([10], 5.7, Theorem 5). The corresponding cohomology group of Γ_3 can be computed in the following way: let Q be the Γ-module coinduced from the Γ_3-module $T_3(E)/(9)$. Then $|Q| = 9^4$, so by the Poitou–Tate exact sequence (36),

$$H^1(\Gamma, Q) \cong H^1(\Gamma_3, T_3(E)/(9)) \cong (\mathbb{Z}/9)^2.$$

To see that the restriction is an isomorphism, pick a G_3-equivariant section

Please cite this article in press as: I. Kriz, On the arithmetic of elliptic curves and a homotopy limit problem, J. Number Theory (2018), http://dx.doi.org/10.1016/j.jnt.2017.08.008

$$\begin{array}{ccc} T_3(E)/(9) & \longrightarrow & Q \\ & \searrow^{Id} & \downarrow \\ & & T_3(E)/(9) \end{array}$$

and consider the commutative diagram

$$\begin{array}{ccc} H^1(\Gamma, Q) & \longrightarrow & H^1(\Gamma_{(3)}, Q) \\ \cong \downarrow & & \uparrow \\ H^1(\Gamma_3, T_3(E)/(9)) & \longrightarrow & H^1(\Gamma_{(3)}, T_3(E)/(9)) \end{array}$$

and the Poitou–Tate exact sequence (36). □

Note that $T_3(E)/(9)$ as a G_3-module actually splits as

$$T_3(E)/(9) \cong M \oplus M'$$

where both M, M', as abelian groups, are isomorphic to $\mathbb{Z}/9$. The first cohomologies of both $\Gamma_{(3)}$ and Γ_3 on M and M' are therefore isomorphic to $\mathbb{Z}/9$.

Now the image of

$$\mathbb{Z}/9 \cong H^1(\Gamma, T_3(E)/(9)) \subset H^1(\Gamma_3, T_3(E)/(9)) \cong \mathbb{Z}/9 \oplus \mathbb{Z}/9$$

is, by the Hochschild–Serre spectral sequence, invariant under the action of the involution σ. We see that neither of the subgroups $H^1(\Gamma_3, M)$ nor $H^1(\Gamma_3, M')$ satisfies this property, since σ switches them.

This describes an obstruction modulo 3, but it lifts to a non-torsion obstruction. In fact, Kato [4] in Chapter 16 (cf. [1]) relates L_p to the p-adic L-function in case of newforms with ordinary good reduction. In our case, the Galois cohomology calculation shows that the 3-adic L-function is non-zero mod 3. It is interesting, however, that the calculation is elementary, giving hope that non-vanishing of the obstruction can be shown in contexts where modularity is not known, for example over more general number fields or for abelian varieties.

References

[1] C. Breuil, B. Conrad, F. Diamond, R. Taylor, On the modularity of elliptic curves over $\mathbb{Q}$, or 3-adic exercises, J. Amer. Math. Soc. 14 (2001) 849–939.
[2] P. Deligne, La conjecture de Weil I, Publ. Math. IHES 43 (1972) 273–307;
P. Deligne, La conjecture de Weil II, Publ. Math. IHES 52 (1980) 137–252.
[3] U. Jannsen, Continuous étale cohomology, Math. Ann. 280 (2) (1988) 207–245.
[4] K. Kato, p-adic Hodge theory and values of zeta functions of modular forms, Cohomologies p-adiques et applications arithmétiques III, Astérisque 295 (2004) 117–290.

Please cite this article in press as: I. Kriz, On the arithmetic of elliptic curves and a homotopy limit problem, J. Number Theory (2018), http://dx.doi.org/10.1016/j.jnt.2017.08.008

[5] V.A. Kolyvagin, Euler systems, in: The Grothendieck Festschrift, vol. II, in: Progr. Math., vol. 87, Birkhäuser Boston, Boston, MA, 1990, pp. 435–483.
[6] C. Mazza, V. Voevodsky, C. Weibel, Lecture notes on motivic cohomology, Clay Mathematics Monographs, vol. 2, 2006.
[7] J.S. Milne, Elliptic Curves, BookSurge Publishers, Charleston, SC, 2006.
[8] J.S. Milne, Étale Cohomology, Princeton Mathematical Series, vol. 33, Princeton University Press, Princeton, NJ, 1980.
[9] J.S. Milne, Arithmetic Duality Theorems, Perspectives in Mathematics, vol. 1, Academic Press, Inc., Boston, MA, 1986.
[10] J.P. Serre, Galois Cohomology, Springer Verlag, 1997.
[11] J.H. Silverman, Advanced Topics in the Arithmetic of Elliptic Curves, Graduate Texts in Mathematics, vol. 151, Springer Verlag, 1984.
[12] J. Tate, Duality theorems in Galois cohomology over number fields, in: Proc. ICM, Stockholm, 1962, 1963, pp. 285–295.
[13] V. Voevodsky, On motivic cohomology with $\mathbb{Z}/\ell$-coefficients, Ann. of Math. 174 (2011) 401–438.
[14] V. Voevodsky, Motives over simplicial schemes, J. K-Theory 5 (1) (2010) 1–38.

Please cite this article in press as: I. Kriz, On the arithmetic of elliptic curves and a homotopy limit problem, J. Number Theory (2018), http://dx.doi.org/10.1016/j.jnt.2017.08.008