Canad. J. Math. Vol. **57** (4), 2005 pp. 812–843

On the Vanishing of μ-Invariants of Elliptic Curves over $\mathbb{Q}$

Mak Trifković

Abstract. Let $E_{/\mathbb{Q}}$ be an elliptic curve with good ordinary reduction at a prime $p > 2$. It has a well-defined Iwasawa μ-invariant $\mu(E)_p$ which encodes part of the information about the growth of the Selmer group $\mathrm{Sel}_{p^\infty}(E_{/K_n})$ as K_n ranges over the subfields of the cyclotomic $\mathbb{Z}_p$-extension $K_\infty/\mathbb{Q}$. Ralph Greenberg has conjectured that any such E is isogenous to a curve E' with $\mu(E')_p = 0$. In this paper we prove Greenberg's conjecture for infinitely many curves E with a rational p-torsion point, $p = 3$ or 5, no two of our examples having isomorphic p-torsion. The core of our strategy is a partial explicit evaluation of the global duality pairing for finite flat group schemes over rings of integers.

1 Notation

Fix a rational prime $p > 2$. We denote by $K_\infty \supset \cdots \supset K_n \supset \cdots \supset K_0 = \mathbb{Q}$ the unique (cyclotomic) $\mathbb{Z}_p$-tower over $\mathbb{Q}$. We write $\Gamma \cong \gamma^{\mathbb{Z}_p}$ for the Galois group $G_{K_\infty/\mathbb{Q}}$ and a choice of topological generator γ. Set $\mathcal{O}_n$ = ring of integers of K_n, $X_n = \mathrm{Spec}\,\mathcal{O}_n$.

We choose

$$\pi_n = N_{\mathbb{Q}(\zeta_{p^{n+1}})/K_n}(1 - \zeta_{p^{n+1}})$$

as our preferred generator of the unique prime of K_n above p. The π_n's satisfy the norm compatibility relation $N_{K_{n+1}/K_n}(\pi_{n+1}) = \pi_n$.

Let F be a number field. For any elliptic curve $E_{/F}$, we write $\mathcal{E}_{/\mathcal{O}_F}$ for its Néron model. We define the discrete and compact Selmer groups of $E_{/F}$ by

$$\mathrm{Sel}_{p^n}(E_{/F}) = \ker(H^1(F, E[p^n]) \to \prod_{v\nmid\infty, v|\infty} H^1(F_v, E)), \quad 1 \le n \le \infty$$

$$X_p(E) = \mathrm{Sel}_{p^\infty}(E_{/K_\infty})^\vee$$

respectively. Here $G^\vee = \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z})$ stands for the Pontryagin dual of a group G.

2 Introduction

Let $E_{/\mathbb{Q}}$ be an elliptic curve with good ordinary reduction at a prime $p > 2$. Under this assumption, the compact Selmer group $X_p(E)$ is a finitely generated torsion module over the Iwasawa algebra $\Lambda = \mathbb{Z}_p[[\Gamma]] \cong \mathbb{Z}_p[[T]]$, and as such has a characteristic power series $f_E^{\mathrm{alg}}(T) \in \mathbb{Z}_p[[T]]$. The condition $p^{\mu(E)_p} \parallel f_E^{\mathrm{alg}}(T)$ in $\mathbb{Z}_p[[T]]$ defines the

Received by the editors August 5, 2003.
AMS subject classification: 11R23.

Iwasawa μ-invariant $\mu(E)_p$ of $X_p(E)$, which controls the growth rate of $\text{Ш}(E_{/K_n})[p]$ as K_n goes up the cyclotomic tower $K_\infty/\mathbb{Q}$. One can say when it vanishes in purely elementary terms:

$$\mu(E)_p = 0 \iff \text{Ш}(E_{/K_n})[p] \text{ is bounded as } n \to \infty.$$

Ralph Greenberg has made the following:

Conjecture 1 *Every $E_{/\mathbb{Q}}$ with good ordinary reduction at $p > 2$ is isogenous to a curve E' with $\mu(E')_p = 0$.*

When $E[p]$ is irreducible, the Conjecture predicts that $\mu(E)_p = 0$. This, the generic case, seems intractable at present.

The situation is rather brighter when $E[p]$ is reducible, *i.e.*, when it sits in a short exact sequence of $G_{\mathbb{Q}}$-modules

$$0 \to \Phi \to E[p] \to \Psi \to 0. \tag{1}$$

This case bifurcates into two sub-cases:

(1) Φ is odd and unramified at p, or even and ramified at p. In this case, Greenberg and Vatsal [4] prove that E itself has $\mu = 0$. The result follows by a fairly simple bootstrapping from the Ferrero–Washington theorem.

(2) Φ is even and unramified at p, or odd and ramified at p, the harder case. Here it can happen that $\mu(E)_p > 0$, and we can in fact precisely describe the isogeny which conjecturally annihilates it (see Corollary 1). This paper will approach this sub-case of Greenberg's conjecture in the special instance where $E[p]$ sits in a *non-split* short exact sequence

$$0 \to \mathbb{Z}/p\mathbb{Z} \to E[p] \to \mu_p \to 0.$$

In this situation Greenberg predicts that $\mu(E)_p = 0$, which we indeed prove for infinitely many examples, some of them essentially new, when $p = 3$ or 5.

For instance, by the end of the paper we will show that the curve

$$E_1 : y^2 + xy = x^3 - 6390x - 215900,$$

with a rational 3-torsion point has $\mu(E_1)_3 = 0$. As far as we know, the best previous estimate, coming from Schneider's evaluation of $f_{E_1}^{\mathrm{alg}}(0)$ (see [3]), gives $\mu(E_1)_3 \leq 4$. The same argument, *mutatis mutandis*, will show that $\mu(E_2)_3 = 0$ for the rank 1 curve

$$E_2 : y^2 + xy = x^3 + 58x - 22684,$$

for which the author does not know of a previous upper bound. Both these examples are instances of a general theorem, Theorem 3, which proves that $\mu(E)_p = 0$ in our setting provided there are "enough" cyclotomic units mod l for certain primes l of bad reduction. The main interest of this result is that it gives a criterion for $\mu(E)_p = 0$ which depends only on the number theory of the cyclotomic tower, and not on the curve itself. We will apply Theorem 3 to find infinitely many essentially distinct examples of curves with $\mu = 0$ inside Kubert's families parametrizing elliptic curves with a rational p-torsion point, for $p = 3$ or 5.

It is interesting to compare the state of our knowledge about Conjecture 1 with what we know about the Main Conjecture of Iwasawa theory. The latter predicts that the characteristic power series $f_E^{\mathrm{alg}}(T)$ is, up to multiplication by $\Lambda^\times$, equal to the power series $f_E^{\mathrm{an}}(T)$, associated to the analytic p-adic L function defined from modular symbols by Mazur and Swinnerton–Dyer. Kato has almost completely proved one half of the Main Conjecture: he shows that $f_E^{\mathrm{alg}}(T) | f_E^{\mathrm{an}}(T)$ as elements in $\mathbb{Q}_p[[T]]$. In other words, he makes no claim about the relationship between the powers of p dividing $f_E^{\mathrm{an}}(T)$ and $f_E^{\mathrm{alg}}(T)$. He can show that $f_E^{\mathrm{alg}}(T) | f_E^{\mathrm{an}}$ in $\mathbb{Z}_p[[T]]$ only when $G_{\mathbb{Q}} \to \mathrm{Aut} E[p]$ is surjective, and p is outside an explicit set of primes (see [9]), so it is fortunate that we can get some independent information on μ in the reducible cases.

2.1 μ-Annihilating Isogenies

It is not hard to refine Conjecture 1 to say precisely which curve isogenous to E has μ-invariant zero. Let $C \subset E(\bar{\mathbb{Q}})$ be a cyclic subgroup of order p^n, stable under $G_{\mathbb{Q}}$. Then the $G_{\mathbb{Q}}$-module C has a unique composition series

$$C \supset pC \supset \cdots \supset p^{n-1}C = C[p] \supset 0,$$

with each composition factor isomorphic to $C[p]$. We say that C is ramified at p (resp., odd) if and only if the action of I_p (resp., the complex conjugation) on $C[p]$ is non-trivial. The following lemma relates the μ-invariants of E and E/C.

Lemma 1 *We have the formula*

$$\mu(E/C)_p = \mu(E)_p + \delta,$$

where the value of δ, depending on the parity and ramification of the Galois action on C, is given by the table:

C	*ramified*	*unramified*
odd	$-n$	0
even	0	n

Proof Since E is good ordinary at p, reduction mod p gives an exact sequence of $G_{\mathbb{Q}_p}$-modules

$$0 \to \mathfrak{F} \to E[p^\infty] \to \tilde{E}[p^\infty] \to 0.$$

Consider the exact sequence $0 \to C \to E \to E' \to 0$ over $\mathbb{Q}$. Schneider [10] gives a formula relating the μ-invariants of E and E':

$$\mu(E')_p - \mu(E)_p = \mathrm{ord}_p(|C(\mathbb{R})|) - \mathrm{ord}_p(|C \cap \mathfrak{F}|).$$

https://doi.org/10.4153/CJM-2005-032-9 Published online by Cambridge University Press

If $|C| = p$, $C \cap \mathcal{F}$ is C or 0, depending on whether C is ramified or not, so we get

$$\mu(E')_p = \mu(E)_p + \begin{array}{c|c|c} C & \text{ramified} & \text{unramified} \\ \hline \text{odd} & -1 & 0 \\ \hline \text{even} & 0 & 1 \end{array}$$

If C is cyclic of order p^n, we can factor the isogeny $E \to E' = E/C$ into n isogenies with kernels isomorphic to $C[p]$. Adding up, we get the lemma. For a much more general version, see [2, Theorem 2.2]. ■

This allows us to say precisely which curve isogenous to E should have μ-invariant zero:

Corollary 1 *Let $M \subset E(\bar{\mathbb{Q}})$ be the maximal subgroup which is*

- *cyclic p-primary,*
- *$\mathbb{Q}$-rational, $G_{\mathbb{Q}}$-action on M odd and ramified at p.*

Set $|M| = p^m$. Then

(a) *the minimal value of $\mu(E')_p$ as E' ranges over the isogeny class of E (over $\mathbb{Q}$) is attained for $E' = E/M$.*
(b) *Conjecture* 1 *is equivalent to $\mu(E/M)_p = 0$, i.e. $\mu(E)_p = m$.*
(c) *When $E[p]$ fits into an exact sequence* (1)*, Conjecture* 1 *is equivalent to the following claim: $\mu(E)_p = 0 \Leftrightarrow$*
   (1) *Φ is even and ramified at p, or odd and unramified at p, or*
   (2) *Φ is even and unramified p, and the exact sequence* (1) *is non-split (to prevent Ψ from lifting to an odd ramified subgroup, which would increase the μ-invariant).*

The beauty of Conjecture 1 is that it allows us to read off the μ-invariant, which is a priori some sort of growth rate all the way up the cyclotomic tower, solely from the arithmetic of E over $\mathbb{Q}$.

Example The situation described in Corollary 1(c) is visible in the very first example, the isogeny class of curves of conductor 11, with $p = 5$. Of the three, $E = X_1(11)$ has a non-split sequence $0 \to \mathbb{Z}/5\mathbb{Z} \to E[5] \to \mu_5 \to 0$, and Greenberg [3] proves that $\mu(X_1(11))_5 = 0$. In general, the curve with vanishing μ is expected to be the optimal quotient of $X_1(N)$ in its isogeny class, and to have a number of other canonicality properties (see the forthcoming paper of Vatsal [12]).

2.2 Approaching $\mu(E)_p = 0$

This paper will outline an approach to the following special case of Greenberg's conjecture, as listed in Corollary 1, case (c)(2):

Conjecture 2 *If $E[p]$ lives in a non-split sequence of $G_{\mathbb{Q}}$-modules $0 \to \mathbb{Z}/p\mathbb{Z} \to E[p] \to \mu_p \to 0$, then $\mu(E)_p = 0$.*

https://doi.org/10.4153/CJM-2005-032-9 Published online by Cambridge University Press

In the good ordinary case we are dealing with, $X_p(E)$ is a finitely generated torsion Λ-module. The following simple, yet useful criterion for detecting the vanishing of the μ-invariant follows immediately from the structure theory of such Λ-modules:

Lemma 2 *$\mu(E)_p = 0 \Leftrightarrow X_p(E)/pX_p(E)$ $(= (\mathrm{Sel}_{p^\infty}(E_{/K_\infty})[p])^\vee)$ is a torsion $\mathbb{F}_p[[T]]$-module.*

Thus to show $\mu(E)_p = 0$, it suffices to prove that $\mathrm{Sel}_{p^\infty}(E_{/K_\infty})[p]$ has $\mathbb{F}_p[[T]]$-corank equal to zero. Up to finite kernel and cokernel, $\mathrm{Sel}_{p^\infty}(E_{/K_\infty})[p]$ is just $\mathrm{Sel}_p(E_{/K_\infty}) \subset H^1(K_\infty, E[p])$, the standard Selmer group for $E[p]$.

Greenberg [3] and Greenberg–Vatsal [4] prove this in the case (c)(1) of Corollary 1 by fitting the Selmer group for $E[p]$ between suitably defined Selmer groups for Φ and Ψ, and deducing from the Ferrero–Washington theorem that both of the latter have $\mathbb{F}_p[[T]]$-corank zero. The assumptions on parity and ramification of Φ and Ψ are just right to make Ferrero–Washington applicable.

The main reason why the approach of Greenberg–Vatsal fails in the case (c)(2) is that for any reasonable Galois-theoretic definition of finite-singular structures for which we would get an exact sequence of the form

$$0 \to \mathrm{Sel}(\mathbb{Z}/p\mathbb{Z}_{/K_\infty}) \to \mathrm{Sel}(E[p]_{/K_\infty}) \to \mathrm{Sel}(\mu_{p/K_\infty}),$$

the last Selmer group, $\mathrm{Sel}(\mu_p/K_\infty)$, has $\mathbb{F}_p[[T]]$-rank 1. The main idea for rescuing the argument is to carefully (and naturally) cut this group down to something small enough to be $\mathbb{F}_p[[T]]$-torsion, yet big enough to receive a map from $\mathrm{Sel}(E[p])$.

To do this, we replace the sequence (1) of $G_{\mathbb{Q}}$-modules with the short exact sequence of quasi-finite flat group schemes over $X_0 = \operatorname{Spec} \mathbb{Z}$ associated to the Néron model $\mathcal{E}_{/X_0}$ of E,

$$0 \to \mathbb{Z}/p\mathbb{Z} \to \mathcal{E}[p] \to \mu \to 0, \tag{2}$$

where μ is a quasi-finite group scheme isomorphic to μ_p over $\mathbb{Z}[1/N]$ and to $\{1\}$ elsewhere. Here N, the "p-torsion conductor", is the product of all primes l for which $\mu(\bar{\mathbb{F}}_l) = \{1\}$. A good way to picture μ is as μ_p punctured over $l|N$. Since $\mu(\bar{\mathbb{F}}_l) = \mathcal{E}(\bar{\mathbb{F}}_l)/\mathbb{Z}/p\mathbb{Z}$, we get a "hole" in μ at l if and only if $\mathcal{E}[p](\bar{\mathbb{F}}_l) \cong \mathbb{Z}/p\mathbb{Z}$. For this to happen, E must have bad reduction at l. Specifically, $l|N$ if and only if the reduction of E at l is

- multiplicative, and $p \nmid c_l$, the number of connected components of $\mathcal{E}_{/\mathbb{F}_l}$, or
- additive, in which case the presence of a rational torsion point forces $p = 3$, and the reduction is of type IV or IV^*.

The sequence (2) is base-change invariant in the sense that its base-change to X_n gives the structure of the p-torsion of the Néron model of $E_{/K_n}$.

We concomitantly replace the Galois-theoretic Selmer groups

$$\mathrm{Sel}_p(E_{/K_n}) \subset H^1(K_n, E[p])$$

with the flat cohomology groups $H^1_{fl}(X_n, \mathcal{E}[p])$.

Lemma 3 *There are maps $H^1_{fl}(X_\infty, \mathcal{E}[p]) \to Z \leftarrow \mathrm{Sel}_p(E_{/K_\infty})$ with finite kernel and cokernel. Thus $H^1_{fl}(X_\infty, \mathcal{E}[p])$ is $\mathbb{F}_p[[T]]$-torsion if and only if $\mathrm{Sel}_p(E_{/K_\infty})$ is. To show that $\mu(E)_p = 0$, it suffices to prove that $H^1_{fl}(X_\infty, \mathcal{E}[p])$ has corank 0 as an $\mathbb{F}_p[[T]]$-module.*

Proof For the first part, see [6, Prop. 6.4]. The second claim is Lemma 2. ■

We will thus focus on showing $H^1_{fl}(X_\infty, \mathcal{E}[p])$ is a co-torsion $\mathbb{F}_p[[T]]$-module. Over X_∞ we get the long exact sequence in flat cohomology associated to (2)

$$(3) \qquad H^1_{fl}(X_\infty, \mathbb{Z}/p\mathbb{Z}) \to H^1_{fl}(X_\infty, \mathcal{E}[p]) \to H^1_{fl}(X_\infty, \mu) \xrightarrow{\delta} H^2_{fl}(X_\infty, \mathbb{Z}/p\mathbb{Z}).$$

To show that $\mu(E)_p = 0$, we will see below that it suffices to find an $\mathbb{F}_p[[T]]$-*divisible* class $b \in H^1_{fl}(X_\infty, \mu)$ such that $\delta b \neq 0$. How to go about verifying that $\delta b \neq 0$? A naïve idea, which will ultimately work, would be to find a functional $\alpha\colon H^2_{fl}(X_\infty, \mathbb{Z}/p\mathbb{Z}) \to \mathbb{Q}_p/\mathbb{Z}_p$ such that $\alpha(\delta b) \neq 0$. We compute the group of all such functionals:

$$\begin{aligned} H^2_{fl}(X_\infty, \mathbb{Z}/p\mathbb{Z})^\vee &= (\varinjlim H^2_{fl}(X_n, \mathbb{Z}/p\mathbb{Z}))^\vee \\ &= \varprojlim H^2_{fl}(X_n, \mathbb{Z}/p\mathbb{Z})^\vee \cong \varprojlim H^1_{fl}(X_n, \mu_p). \end{aligned}$$

The last isomorphism comes from the existence of a perfect *global duality pairing*, see [7]:

$$H^1_{fl}(X_n, \mu_p) \times H^2_{fl}(X_n, \mathbb{Z}/p\mathbb{Z}) \to \mathbb{Q}_p/\mathbb{Z}_p.$$

Notice that by Kummer theory

$$\varprojlim \mathcal{O}_n^\times/\mathcal{O}_n^{\times p} \hookrightarrow \varprojlim H^1_{fl}(X_n, \mu_p),$$

so we might expect to show $\delta b \neq 0$ by evaluating on it a functional coming from a norm-coherent sequence of units (mod p-th powers).

At the heart of this paper will thus be an explicit computation of the global duality pairing $H^2_{fl}(X_n, \mathbb{Z}/p\mathbb{Z}) \times H^1_{fl}(X_n, \mu_p) \to \mathbb{Q}_p/\mathbb{Z}_p$. To be precise, we will produce an explicit pairing formula which will allow us to deduce that $\mu(E)_p = 0$ in some cases. The mere existence of the formula will suffice for us; that it actually computes the canonically defined global duality pairing will not be spelled out.

3 Strategy of Proof

All module-theoretic notions used here ("torsion", "rank", *etc.*) will refer to $\mathbb{F}_p[[T]]$-modules unless explicitly stated otherwise. In particular, M_{div} will refer to the maximal $\mathbb{F}_p[[T]]$-divisible submodule of a $\mathbb{F}_p[[T]]$-module M.

Proposition 1 *$\mu(E)_p = 0$ if and only if there exists a $b \in H^1_{fl}(X_\infty, \mu)_{\mathrm{div}}$ such that $\delta b \neq 0$.*

Proof From (3) we extract the short exact sequence

$$0 \leftarrow H^1_{fl}(X_\infty, \mathbb{Z}/p\mathbb{Z})^\vee \leftarrow H^1_{fl}(X_\infty, \mathcal{E}[p])^\vee \leftarrow (\ker \delta)^\vee \leftarrow 0.$$

It suffices to show that the flanking $\mathbb{F}_p[[T]]$-modules $H^1_{fl}(X_\infty, \mathbb{Z}/p\mathbb{Z})^\vee$ and $(\ker \delta)^\vee$ both have rank 0. For the former, this is a straightforward consequence of the Ferrero–Washington theorem. The latter is equal to the cokernel of $\delta^\vee\colon H^2_{fl}(X_\infty, \mathbb{Z}/p\mathbb{Z})^\vee \to H^1_{fl}(X_\infty, \mu)^\vee$. Let F be the maximal free quotient of $H^1_{fl}(X_\infty, \mu)$. Since, up to finite kernel and cokernel, $H^1_{fl}(X_\infty, \mu)^\vee \cong H^1_{fl}(X_\infty, \mu_p)^\vee \cong (\mathcal{O}^\times_\infty/\mathcal{O}^{\times p}_\infty)^\vee$ (see Lemma 4), and the latter is easily seen to be of $\mathbb{F}_p[[T]]$-rank 1, we conclude that F is also of rank 1. To show that the cokernel of $\delta^\vee$ is $\mathbb{F}_p[[T]]$-torsion, it is therefore enough to show that the composed map

$$H^2_{fl}(X_\infty, \mathbb{Z}/p\mathbb{Z})^\vee \xrightarrow{\delta^\vee} H^1_{fl}(X_\infty, \mu)^\vee \to F$$

is non-zero. Dualizing, we need to show that the map

$$H^1_{fl}(X_\infty, \mu)_{div} \xrightarrow{\delta} H^2_{fl}(X_\infty, \mathbb{Z}/p\mathbb{Z})$$

is non-zero, as claimed. ■

So, we start with an $\mathbb{F}_p[[T]]$-divisible $b \in H^1_{fl}(X_\infty, \mu)$, and we want to show $\delta b \neq 0$. The class b will live on some finite level, say $b \in H^1_{fl}(X_n, \mu)$. Our task can be broken up into two:

1. Verify that $\delta b \neq 0$ in $H^2_{fl}(X_n, \mathbb{Z}/p\mathbb{Z})$.
2. Verify that δb remains non-zero under the restriction

$$H^2_{fl}(X_n, \mathbb{Z}/p\mathbb{Z}) \to H^2_{fl}(X_\infty, \mathbb{Z}/p\mathbb{Z}).$$

3.1 Finite-Level Computation

As we will be working over the single scheme $X_n = \operatorname{Spec} \mathcal{O}_n$, for the duration of this subsection we suppress the n from our notations. Thus $K = K_n,\ \mathcal{O} = \mathcal{O}_n,\ X = X_n$, *etc.*

As $\mathbb{Z}/p\mathbb{Z}_{/X}$ is a smooth group scheme, its flat cohomology is equal to its étale cohomology (denoted with an unadorned $H^*(X, \mathbb{Z}/p\mathbb{Z})$). The following proposition will give us something of a handle on the elements on $H^2(X, \mathbb{Z}/p\mathbb{Z})$:

Proposition 2 *The group $H^2(X, \mathbb{Z}/p\mathbb{Z})$ fits into the following long exact Gysin sequence*

$$(4)\quad 0 \to H^1(X, \mathbb{Z}/p\mathbb{Z}) \to \operatorname{Hom}(G_K, \mathbb{Z}/p\mathbb{Z}) \to \bigoplus_{v \nmid \infty} \operatorname{Hom}(U_v, \mathbb{Z}/p\mathbb{Z})$$

$$\xrightarrow{d_2} H^2(X, \mathbb{Z}/p\mathbb{Z}) \to H^2(K, \mathbb{Z}/p\mathbb{Z})$$

Here U_v denotes the units of the localization $\mathcal{O}_{K,v}$, and the sum is taken over all finite places of K. (The meaning of d_2 is explained in the proof.)

Proof Let $i\colon \operatorname{Spec} K \to X$ be the inclusion of the generic point. As étale sheaves, $\mathbb{Z}/p\mathbb{Z}_{/X} = i_*(\mathbb{Z}/p\mathbb{Z}_{/\operatorname{Spec} K})$ (note that this fails in the flat topology). Granting for the moment the identification $H^0(X, R^1 i_*\mathbb{Z}/p\mathbb{Z}) = \oplus_{v\nmid\infty} \operatorname{Hom}(U_v, \mathbb{Z}/p\mathbb{Z})$, the long exact sequence (4) becomes just the low-dimensional terms of the Grothendieck spectral sequence for the composition of functors i_* and $H^0(X, -)$:

$$E_2^{m,n} = H^m(X, R^n i_*\mathbb{Z}/p\mathbb{Z}) \Rightarrow H^{m+n}(K, \mathbb{Z}/p\mathbb{Z}),$$

and $d_2\colon E_2^{01} \to E_2^{20}$ the corresponding second-stage diagonal differential.

To prove $H^0(X, R^1 i_*\mathbb{Z}/p\mathbb{Z}) = \bigoplus_{v\nmid\infty} \operatorname{Hom}(U_v, \mathbb{Z}/p\mathbb{Z})$, we compute the stalks of $R^1 i_*\mathbb{Z}/p\mathbb{Z}$ at geometric points of X. At the geometric generic point $\bar{\eta} : \operatorname{Spec} \bar{K} \to X$, the stalk is $(R^1 i_*\mathbb{Z}/p\mathbb{Z})_{\bar{\eta}} = H^1(\bar{K}, \mathbb{Z}/p\mathbb{Z}) = 0$. At a geometric special point $\bar{v}\colon \operatorname{Spec} \bar{\mathbb{F}}_v \to X$ we get $(R^1 i_*\mathbb{Z}/p\mathbb{Z})_{\bar{v}} = \operatorname{Hom}(I_{\bar{v}/v}, \mathbb{Z}/p\mathbb{Z})$, which under the conjugation action of Frobenius Fr_v becomes an étale sheaf on $\operatorname{Spec} \mathbb{F}_v$. From these computations we conclude that $R^1 i_*\mathbb{Z}/p\mathbb{Z}$ is an étale skyscraper sheaf on the one-dimensional scheme X, and that therefore

$$R^1 i_*\mathbb{Z}/p\mathbb{Z} \cong \bigoplus_{v\nmid\infty} i_{v*} \operatorname{Hom}(I_{\bar{v}/v}, \mathbb{Z}/p\mathbb{Z}).$$

The desired identification used above follows from local class field theory:

$$\operatorname{Hom}(I_{\bar{v}/v}, \mathbb{Z}/p\mathbb{Z})^{\operatorname{Fr}_v = 1} \cong \operatorname{Hom}(U_v, \mathbb{Z}/p\mathbb{Z}),$$

for any choice of $\bar{v}|v$. ■

Say we are lucky enough to have $\delta b \in \ker(H^2(X, \mathbb{Z}/p\mathbb{Z}) \to H^2(K, \mathbb{Z}/p\mathbb{Z}))$. The technical core of this paper is the explicit computation of a lift of δb via d_2, the spectral sequence differential, to a collection of functions $(f_v\colon U_v \to \mathbb{Z}/p\mathbb{Z})$, almost all of which vanish. Having computed this lift, the following proposition will give us a sufficient condition for the lift to *not* be a restriction of a homomorphism $f\colon G_K \to \mathbb{Z}/p\mathbb{Z}$.

For any finite place v of K, we have the natural injection $\mathcal{O}_K^\times \hookrightarrow U_v$, $a \mapsto a_v$.

Proposition 3 *To show $\delta b \neq 0 \in H^2(X, \mathbb{Z}/p\mathbb{Z})$, it suffices to show that there is a* global *unit $a \in \mathcal{O}^\times$ such that*

$$\sum_{v\nmid\infty} f_v(a_v) \neq 0.$$

Remark Though we will not prove it, the sum on the left is nothing but the pairing $\langle a, b\rangle$ induced from the global duality pairing by the composition

$$\mathcal{O}^\times/\mathcal{O}^{\times p} \times H^1_{fl}(X, \mu) \to H^1_{fl}(X, \mu_p) \times H^1_{fl}(X, \mu) \xrightarrow{id\times\delta} H^1_{fl}(X, \mu_p) \times H^2(X, \mathbb{Z}/p\mathbb{Z}) \to \mathbb{Q}_p/\mathbb{Z}_p.$$

Proof To show $\delta b \neq 0$ it suffices, by the exact sequence (4), to show that the collection $(f_v \colon U_v \to \mathbb{Z}/p\mathbb{Z})$ is not the restriction of a global homomorphism $f \colon G_K \to \mathbb{Z}/p\mathbb{Z}$. The restriction is given simply by composing along the top row of the diagram

$$\begin{tikzcd} \prod_v U_v \arrow[r, hook] & \mathbb{A}_K^{\times f} \arrow[r, "\mathrm{rec}"] & G_{K^{ab}/K} \arrow[r, "f"] & \mathbb{Z}/p\mathbb{Z} \\ \mathcal{O}^\times \arrow[u] \arrow[r, hook] & K^\times \arrow[u] \arrow[ur] & & \end{tikzcd}$$

where rec is the Artin map of global class field theory. If $(f_v \colon U_v \to \mathbb{Z}/p\mathbb{Z})$ were to arise in this way, we would have that

$$\sum_{v \nmid \infty} f_v(a_v) = f \circ \mathrm{rec}\Big(\prod_{v \nmid \infty} a_v\Big) = f \circ \mathrm{rec}(a) = 0,$$

since $f \circ \mathrm{rec}\,|_{K^\times} = 0$ by global reciprocity (and the fact that $f \circ \mathrm{rec}$ is trivial on the Archimedean components of $\mathbb{A}_K^\times$, since p is odd). ∎

3.2 Moving up the Tower

Reinstate the n in the notation: $b \in H^1_{fl}(X_n, \mu)$ *etc.* Say we have shown that $0 \neq \delta b \in H^2(X_n, \mathbb{Z}/p\mathbb{Z})$ by finding, as above, a collection $(f_{n,v} : U_{n,v} \to \mathbb{Z}/p\mathbb{Z})$ lifting δb and a global unit $a_n \in \mathcal{O}_n^\times$ such that

$$\sum_{v \nmid \infty \text{ of } K_n} f_{n,v}(a_{n,v}) \neq 0.$$

Proposition 4 *Say $a_n = N_{K_{n+1}/K_n}(a_{n+1})$. Then*

$$0 \neq \mathrm{res}(\delta b) \in H^2(X_{n+1}, \mathbb{Z}/p\mathbb{Z}).$$

Proof Throughout the proof, w will denote a generic finite place of K_{n+1}, v the place of K_n below it, and $N_{w/v}$ the corresponding local norm. Let us compare the relevant parts of the long exact sequence (4) for X_n and X_{n+1}:

$$\begin{tikzcd} H^1(K_n, \mathbb{Z}/p\mathbb{Z}) \arrow[r] \arrow[d, "\mathrm{res}"'] & \bigoplus_v \mathrm{Hom}(U_{n,v}, \mathbb{Z}/p\mathbb{Z}) \arrow[r, "d_2"] \arrow[d, "\circ N_{w/v}"'] & H^2(X_n, \mathbb{Z}/p\mathbb{Z}) \arrow[d, "\mathrm{res}"'] \\ H^1(K_{n+1}, \mathbb{Z}/p\mathbb{Z}) \arrow[r] & \bigoplus_w \mathrm{Hom}(U_{n+1,w}, \mathbb{Z}/p\mathbb{Z}) \arrow[r, "d_2"] & H^2(X_{n+1}, \mathbb{Z}/p\mathbb{Z}) \end{tikzcd}$$

The middle vertical map sends $(f_{n,v} \colon U_{n,v} \to \mathbb{Z}/p\mathbb{Z})$ to $(f_{n+1,w} \colon U_{n+1,w} \to \mathbb{Z}/p\mathbb{Z})$ given by $f_{n+1,w} = f_{n,v} \circ N_{w/v}$.

The collection $(f_{n+1,w})$ is a lifting of $\operatorname{res}(\delta b) \in H^2(X_{n+1}, \mathbb{Z}/p\mathbb{Z})$. We have

$$\sum_{w \text{ of } K_{n+1}} f_{n+1,w}(a_{n+1,w}) = \sum_{v \text{ of } K_n} \sum_{w|v} f_{n,v}(N_{w/v}(a_{n+1,w})) = \sum_{v} f_{n,v}(a_{n,v}) \neq 0,$$

by assumption. Thus, essentially the same computation as on the n-th level shows that $\delta b \neq 0$ on the $(n+1)$-st level also. ■

For δb to remain non-zero all the way to $H^2(X_\infty, \mathbb{Z}/p\mathbb{Z})$, it will suffice that the unit a_n is the norm from $\mathcal{O}_k^\times$ for all $k \geq n$, in other words a universal norm in the cyclotomic tower (at least up to p-th powers). A good supply of such a_n's comes from cyclotomic units.

4 The Structure of $H^1_{fl}(X_\infty, \mu)$

Remember that μ is a quasi-finite flat group scheme over $\operatorname{Spec}\mathbb{Z}$, isomorphic to μ_p over $\operatorname{Spec}\mathbb{Z}[1/N]$ and to $\{1\}$ over $l|N$. On $\operatorname{Spec}\mathbb{Z}$, μ represents a flat sheaf whose value at an *irreducible* flat open $U \to \operatorname{Spec}\mathbb{Z}$ is given by

$$\mu(U) = \begin{cases} \mu_p(\mathcal{O}_U), & \text{if } \frac{1}{N} \in \Gamma(U, \mathcal{O}_U) \\ 1 & \text{if } \frac{1}{N} \notin \Gamma(U, \mathcal{O}_U). \end{cases}$$

Lemma 4 *Over X_∞, we have an exact sequence of $\mathbb{F}_p[[T]]$-modules*

$$0 \to \bigoplus_{v_\infty|N} \mu_p(\mathbb{F}_{v_\infty}) \to H^1_{fl}(X_\infty, \mu) \to H^1_{fl}(X_\infty, \mu_p) \to 0. \tag{5}$$

The sum in the first term ranges over the finitely many places $v_\infty|N$ of K_n.

Proof For every $n, 1 \leq n \leq \infty$, the "puncturing" of μ_p at places of X_n dividing N is captured in the exact sequence of flat sheaves over X_n:

$$0 \to \mu \to \mu_p \to \bigoplus_{v_n|N} i_{v_n *}\mu_p \to 0,$$

where $i_{v_n :}$: $\operatorname{Spec}\mathbb{F}_{v_n} \to X_n$.

Taking cohomology, we get a long exact sequence

$$\begin{aligned} 0 = \mu_p(\mathcal{O}_n) &\to \bigoplus_{v_n|N} \mu_p(\mathbb{F}_{v_n}) \to H^1_{fl}(X_n, \mu) \to H^1_{fl}(X_n, \mu_p) \\ &\to \bigoplus_{v_n|N} H^1_{fl}(X_n, i_{v_n *}\mu_p) \hookrightarrow \bigoplus_{v_n|N} H^1_{fl}(\mathbb{F}_{v_n}, \mu_p) = \bigoplus_{v_n|N} \mathbb{F}^\times_{v_n}/\mathbb{F}^{\times p}_{v_n}. \end{aligned} \tag{6}$$

The last inclusion comes from the Grothendieck spectral sequence for $i_{v_n *}$. After passing to the direct limit of these exact sequences, the first (non-zero) term in (6) stabilizes to the finite group $\bigoplus_{v_\infty | N} \mu_p(\mathbb{F}_{v_\infty})$, since there are only finitely many primes $v_\infty | N$ of K_∞. The last term in (6) vanishes in the limit, since for high n, all the elements of $\mathbb{F}_{v_n}^\times$ become p-th powers in $\mathbb{F}_{v_{n+1}}^\times$. ∎

In particular, we get that $H^1_{fl}(X_\infty, \mu)_{div} \twoheadrightarrow H^1_{fl}(X_\infty, \mu_p)_{div} \supseteq \mathcal{O}_\infty^\times / \mathcal{O}_\infty^{\times p}$, the inclusion coming from Kummer theory along with the easy fact that $\mathcal{O}_\infty^\times / \mathcal{O}_\infty^{\times p}$ is $\mathbb{F}_p[[T]]$-divisible. Our goal now is to find explicit Čech cocycles lifting the classes $b \in \mathcal{O}_\infty^\times / \mathcal{O}_\infty^{\times p}$ to $H^1_{fl}(X_\infty, \mu)$.

4.1 Illustration

Before we do this, let us do the lifting construction in a slightly different setting which will illustrate the main idea with a maximum of transparency. Take a field F containing μ_p, and a prime $v \nmid p$ of F. Note that $\mu_p \subset \mathbb{F}_v$. Let $Y = \operatorname{Spec} \mathcal{O}_F$, and let μ be the flat scheme over Y obtained from μ_p by puncturing only over v. As above, we have the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mu_p(\mathbb{F}_v) & \longrightarrow & H^1_{fl}(Y, \mu) & \longrightarrow & H^1_{fl}(Y, \mu_p) & \longrightarrow & \mathbb{F}_v^\times / \mathbb{F}_v^{\times p} \\ & & & & & & \uparrow & \nearrow & \\ & & & & & & \mathcal{O}_F^\times / \mathcal{O}_F^{\times p} & & \end{array}$$

The diagonal map is nothing but the reduction mod v. Take a $b \neq 1$ in $\mathcal{O}_F^\times / \mathcal{O}_F^{\times p}$ such that b is a p-th power mod v. We will lift the corresponding class $b \in H^1_{fl}(Y, \mu_p)$ to $H^1_{fl}(Y, \mu)$.

First of all, the map $\mathcal{O}_F^\times / \mathcal{O}_F^{\times p} \to H^1_{fl}(Y, \mu_p)$ is the coboundary map for the Kummer sequence of flat sheaves over Y, $0 \to \mu_p \to \mathbb{G}_m \xrightarrow{p} \mathbb{G}_m \to 0$. This coboundary is computed in the standard way: by abuse of notation start with $b \in \mathcal{O}_F^\times = \mathbb{G}_m(Y)$, take its "$p$-th root" as a flat 0-cochain y' of $\mathbb{G}_m$, and compute its Čech coboundary. Explicitly, fix once and for all a $b^{1/p}$ and let $L = F(b^{1/p})$, $G = \operatorname{Gal}(L/F)$. The cochain $(V', b^{1/p} \in \mathbb{G}_m(V'))$ on the flat open cover $V' = \operatorname{Spec} \mathcal{O}_L \xrightarrow{f} Y$ can then be taken as y'.

An easy scheme-theoretic computation gives the decomposition into irreducibles

$$V' \times_Y V' = \bigcup_{\sigma \in G} V'_\sigma,$$

where each V'_σ is a copy of V', and the p copies are all glued together at the primes ramified in L/F, all of which divide p. The two projections $p_1, p_2 \colon V' \times_Y V' \rightrightarrows V'$ are given as follows on any component V'_σ:

$$p_1 \colon V'_\sigma \cong V' \xrightarrow{id} V', \quad p_2 \colon V'_\sigma \cong V' \xrightarrow{\sigma} V'. \tag{7}$$

https://doi.org/10.4153/CJM-2005-032-9 Published online by Cambridge University Press

The Čech coboundary $\delta y' = p_2^* y'/p_1^* y'$ is a 1-cocycle for μ_p whose value on V'_σ is given by

$$(\delta y')_\sigma = (b^{1/p})^{\sigma-1}.$$

This is clearly *not* a cocycle for μ: for $\sigma \neq 1$, the component V'_σ has a point over v, yet supports a non-trivial root of unity, $(\delta y')_\sigma$.

We can, however, tweak y' to get a cocycle for μ. For this, we will refine V' to a Zariski open $V \subset V'$. Since $b \pmod{v} \in \mathbb{F}_v^{\times p}$, v splits completely in L/K. The fiber $f^{-1}(v)$ is a G-orbit consisting of p points $\{w_1, \dots, w_p\}$. Remove all but one, setting

$$V = V' \setminus \{w_2, \dots, w_p\}.$$

The picture of $V \hookrightarrow V'$ (for $p = 3$) is given in Figure 1 (the circles represent the removed points).

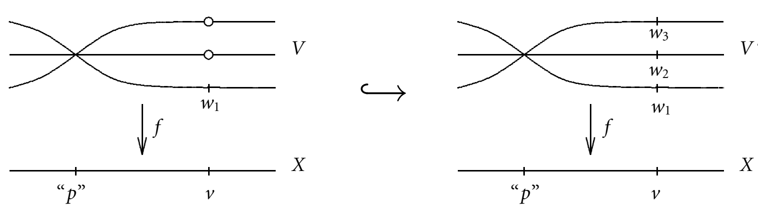

Figure 1

Lemma 5 *$V \times_Y V$ is a union of p irreducible components*

$$V \times_Y V = \bigcup_{\sigma \in G} W_\sigma,$$

where $W_\sigma \subset V'_\sigma$. $W_1 \cong V$, and $W_\sigma \cong V \setminus \{w_1\} \cong V' \setminus f^{-1}(v)$ for $\sigma \neq 1$.

Proof We have $V \times_Y V = p_1^{-1}(V) \cap p_2^{-1}(V) \subset V' \times_Y V'$. We obtain the claimed decomposition by setting $W_\sigma = (V \times_Y V) \cap V_\sigma$. Given the explicit description (7) of the projections, and identifying V'_σ with V', we find the identifications

$$\begin{array}{ccc} p_1^{-1}(V) \cap V'_\sigma & \subset & V'_\sigma \\ \| & & \| \\ V & \subset & V' \end{array} \quad \text{and} \quad \begin{array}{ccc} p_2^{-1}(V) \cap V'_\sigma & \subset & V'_\sigma \\ \| & & \| \\ \sigma^{-1}V & \subset & V' \end{array}$$

Intersecting the two yields the identification diagram

$$\begin{array}{cccc} W_\sigma & = (p_1^{-1}(V) \cap p_2^{-1}(V)) \cap V'_\sigma & \subset & V'_\sigma \\ & \| & & \| \\ & V \cap \sigma^{-1}V & \subset & V' \end{array}$$

For $\sigma \neq 1$, the picture is in Figure 2.

Since v splits in L/K, $w_1 \neq \sigma^{-1}w_1$, and we see that W_σ has no points over v. ∎

https://doi.org/10.4153/CJM-2005-032-9 Published online by Cambridge University Press

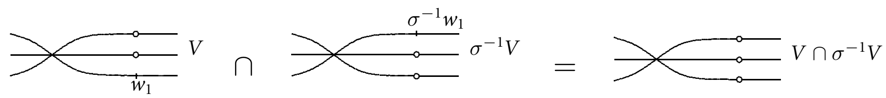

Figure 2

The cocycle δy, given on W_σ by $(\delta y)_\sigma = (b^{1/p})^{\sigma-1}$ is indeed a cocycle for μ. If $\sigma \neq 1$, $(\delta y)_\sigma$ is a non-trivial p-th root of 1, but that is in $\mu(W_\sigma)$ since the Lemma shows there are no points in W_σ above v. This procedure for making a cocycle for μ can clearly be performed simultaneously for several v's dividing N.

4.2 The General Computation

We will now repeat the same construction in our main setting, *i.e.*, over $K_n \not\supset \mu_p$. We start with the class $b \in \mathcal{O}_n^\times/\mathcal{O}_n^{\times p} \to \mathcal{O}_\infty^\times/\mathcal{O}_\infty^{\times p} \hookrightarrow H^1_{fl}(X_\infty, \mu_p)$, and we assume that b is a p-th power mod v for all $v|N$. This can always be achieved by increasing the level n. We will only work at level n, so we again suppress the index n.

The inclusion of rings

$$\mathcal{O} \hookrightarrow \mathcal{O}[y]/(y^p - b) = B,$$

gives us a flat open cover $U' \to X$, and the 0-cochain (U', y) is a "p-th root" of $b \in H^0(X, \mathbb{G}_m)$ whose Čech coboundary represents the class $b \in H^1_{fl}(X, \mu_p)$. Inspired by the above illustration, we will puncture U' to make a cocycle for μ. Let $v_1, \dots, v_r \in X$ be the primes dividing N. Since by assumption $b \equiv *^p \pmod{v_i}$, there is at least one $w_i|v_i$ in U' with $\mathbb{F}_{w_i} = \mathbb{F}_{v_i}$, with p choices if $\mu_p \subset \mathbb{F}_{v_i}$. We set

$$U = U' \setminus \{w|v_i : w \neq w_i\}.$$

Let $F = K(\mu_p)$, $Y = \operatorname{Spec} \mathcal{O}_F$, $V = U \times_X Y$. Since $\mathbb{F}_{w_i} = \mathbb{F}_{v_i}$, all the primes of V above w_i lie above distinct primes of Y, so $V \to Y$ is a cover of the sort we considered in the illustration. In particular, $V \times_Y V = (U \times_X U) \times_X Y = \cup W_\sigma$, and no $W_\sigma, \sigma \neq 1$ has a point above N. The same is thus true for the irreducible components of $U \times_X U$, so that the Čech coboundary of (U, y) is indeed a 1-cocycle for μ.

What if we had picked a different cover U? Specifically, when $\mu_p \subset \mathbb{F}_{v_i}$, we can pick any prime of B above v_i to serve as the w_i. Changing w_i corresponds precisely to changing our lift by an element of $\mu_p(\mathbb{F}_{v_i}) \subset \bigoplus_{v|N} i_{v*}\mu_p(\mathbb{F}_v) \hookrightarrow H^1_{fl}(X_n, \mu)$. Since the primes $w|v$ of B of degree 1 are in a one-to-one correspondence with the p-th roots $t_v \in \mathbb{F}_v$ of b mod v, we have proved the following Proposition, which establishes our standard explicit notation for elements of $H^1_{fl}(X_n, \mu)$:

Proposition 5 *Pick $b \in \mathcal{O}_n^\times/\mathcal{O}_n^{\times p}$, and assume that for all primes $v|N$ of K_n, $b \equiv t_v^p$* $\pmod{v}$ *for some $t_v \in \mathbb{F}_v$. We denote by $(b, \{t_v\}_{v|N})$ the cohomology class $\delta(U, y) \in H^1_{fl}(X_n, \mu)$ constructed above using this choice of t_v's. This notation gives a one-to-one*

https://doi.org/10.4153/CJM-2005-032-9 Published online by Cambridge University Press

correspondence between the choices $(t_v)_{v|N} \in \prod_{v|N} \mathbb{F}_v^\times/\mathbb{F}_v^{\times p}$ of roots of b mod all the places $v|N$ of K_n, and the lifts of $b \in \mathcal{O}_n^\times/\mathcal{O}_n^{\times p} \subset H^1_{fl}(X_n, \mu_p)$ to $H^1_{fl}(X_n, \mu)$.

4.3 Divisible Lifts

We know that $\mathcal{O}_\infty^\times/\mathcal{O}_\infty^{\times p} \subset H^1_{fl}(X_\infty, \mu_p)_{\mathrm{div}}$. In terms of the preceding description, which lifts are divisible?

Since $H^1_{fl}(X_\infty, \mu)/H^1_{fl}(X_\infty, \mu)_{\mathrm{div}}$ is dual to the torsion of the $\mathbb{F}_p[[T]]$-module $H^1_{fl}(X_\infty, \mu)^\vee$, there is an r such that

$$T^{p^r} H^1_{fl}(X_\infty, \mu) \subseteq H^1_{fl}(X_\infty, \mu)_{\mathrm{div}}.$$

We may as well assume r to be such that all the $v_r|N$ are inert in K_∞/K_r. T^{p^r} acts as $\rho - 1 := \gamma^{p^r} - 1$.

Proposition 6 *Pick $n \geq r$ large enough so that we can find a $b \in \mathcal{O}_n^\times/\mathcal{O}_n^{\times p}$, and a $u \in \mathcal{O}_n^\times/\mathcal{O}_n^{\times p}$ satisfying the following two conditions:*

- *$b = u^{\rho-1}$, and*
- *for every $v|N$ a place of K_n we can find an $s_v \in \mathbb{F}_v^\times$ such that $s_v^p \equiv u \pmod{v}$.*

Since ρ fixes all the v_r's, it will act on the residue field extension $\mathbb{F}_{v_n}/\mathbb{F}_{v_r}$, and we set $t_v = s_v^{\rho-1}$ (so that $b \equiv t_v^p \pmod{v}$). Then $(b, \{t_v\}_{v|N}) \in H^1_{fl}(X_\infty, \mu)_{\mathrm{div}}$.

Proof Since $T^{p^r}(u, \{s_v\}) = (u^{\rho-1}, \{s_v^{\rho-1}\}) = (b, \{t_v\})$, our choice of r guarantees that $(b, \{t_v\}) \in H^1_{fl}(X_\infty, \mu)_{\mathrm{div}}$. ■

5 The Fake Coboundary Map

Let $F\colon \mathcal{A} \to \mathcal{B}$ be a left exact functor between Abelian categories. Consider an exact sequence in $\mathcal{A}$, $0 \to A \to B \to C$. The last map need not be onto, so we do not in general get a coboundary between the derived functors $R^nF(C) \xrightarrow{\partial} R^{n+1}F(A)$. We will try to salvage as much of a coboundary map as possible in this slightly more general setting. So, choose the injective resolutions $0 \to A \to I_A^\cdot = (I_A^0 \to I_A^1 \to \cdots)$, and similarly $I_B^\cdot, I_C^\cdot$ fitting into the diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & I_A^\cdot & \longrightarrow & I_B^\cdot & \longrightarrow & I_C^\cdot \\ & & \uparrow & & \uparrow & & \uparrow \\ 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C \end{array}$$

https://doi.org/10.4153/CJM-2005-032-9 Published online by Cambridge University Press

The functor F induces a ladder

(8)
$$
\begin{array}{ccccccc}
 & & \vdots & & \vdots & & \vdots \\
 & & \uparrow & & \uparrow & & \uparrow \\
0 & \longrightarrow & F(I_A^{n+1}) & \longrightarrow & F(I_B^{n+1}) & \longrightarrow & F(I_C^{n+1}) \\
 & & \uparrow d & & \uparrow d & & \uparrow d \\
0 & \longrightarrow & F(I_A^{n}) & \longrightarrow & F(I_B^{n}) & \longrightarrow & F(I_C^{n}) \\
 & & \uparrow d & & \uparrow d & & \uparrow d \\
0 & \longrightarrow & F(I_A^{n-1}) & \longrightarrow & F(I_B^{n-1}) & \longrightarrow & F(I_C^{n-1}) \\
 & & \uparrow & & \uparrow & & \uparrow \\
 & & \vdots & & \vdots & & \vdots
\end{array}
$$

The standard "lift-and-differentiate" recipe for the coboundary fails already at the "lift" stage, since $F(I_B^n) \to F(I_C^n)$ is not necessarily onto. The recipe will still apply to the "liftable" cocycles:

Definition 1 Let $\tilde{F}(I_C^n) = \ker d \cap \operatorname{im}(F(I_B^n) \to F(I_C^n))$ be the group of liftable cocycles in $F(I_C^n)$. Given $x \in \tilde{F}(I_C^n)$, we can lift it to $\tilde{x} \in F(I_B^n)$, and then take $d\tilde{x} \in F(I_B^{n+1})$, which is the image of a $y \in F(I_A^{n+1})$, since x was closed. The cohomology class of $y \in R^{n+1}F(A)$, denoted ∂x, does not depend on the choice of lifting $\tilde{x}$, and gives us a well-defined "fake coboundary map"

$$\partial \colon \tilde{F}(I_C^n) \to R^{n+1}F(A).$$

The main point to appreciate here is that the fake coboundary *does not* necessarily descend to $R^nF(C)$, and so indeed depends on the injective resolutions chosen: even if a liftable $x \in F(I_C^n)$ is exact, $x = dy$, ∂x need not be 0. The usual Snake Lemma argument proving that ∂x is exact needs a lift of y, which need not exist.

6 A Spectral Sequence Lemma

Here is a little technical lemma, giving a sort of *dévissage* for general Grothendieck spectral sequences. Let $\mathcal{A} \xrightarrow{F} \mathcal{B} \xrightarrow{G} \mathcal{A}b$ be the setup for a Grothendieck spectral sequence: $\mathcal{A}, \mathcal{B}$ are Abelian categories, $\mathcal{A}b$ is the category of Abelian groups, F, G are covariant left-exact functors, and F takes injectives of $\mathcal{A}$ into G-acyclic objects of $\mathcal{B}$. Let $M \in \mathcal{A}$. Consider an injective resolution of M,

$$0 \to M \to I_M^0 \to I_M^1 \to \cdots,$$

https://doi.org/10.4153/CJM-2005-032-9 Published online by Cambridge University Press

apply F to it and find injective resolutions $0 \to F(M) \to J^{\cdot}_M, 0 \to F(I^q) \to J^{\cdot q}_M$ by $\mathcal{B}$-injectives fitting into a diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & F(I^1) & \longrightarrow & J^{01}_M & \longrightarrow & J^{11}_M & \longrightarrow & \cdots \\
 & & \uparrow & & d\uparrow & & \uparrow & & \\
0 & \longrightarrow & F(I^0) & \longrightarrow & J^{00}_M & \xrightarrow{\delta} & J^{10}_M & \longrightarrow & \cdots \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
0 & \longrightarrow & F(M) & \longrightarrow & J^{0}_M & \longrightarrow & J^{1}_M & \longrightarrow & \cdots \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

Then $E^{pq}_{0M} = G\big(J^{pq}_M\big)$ is a double complex with anti-commuting differentials d and δ, which yields a spectral sequence with E_2-term $E^{pq}_{2M} = (R^pF \circ R^qG)(M)$. The sequence converges:

$$(R^pF \circ R^qG)(M) \Rightarrow R^{p+q}(G \circ F)(M).$$

As for the E_1-term, we have in particular $E^{p0}_{1M} = \ker d \colon E^{p0}_{0M} \to E^{p1}_{0M}$, which is none other than $G(J^p_M) = \ker d \colon G(J^{00}_M) \to G(J^{01}_M)$.

Take an exact sequence in $\mathcal{A}$, $0 \to A \to B \to C \to 0$. The goal is to prove a lemma relating the above spectral sequence of C to that of A: suitable coboundary maps are asserted to commute with diagonal spectral sequence differentials d_1 and d_2. First, find compatible $\mathcal{A}$-injective resolutions of A, B and C:

$$\begin{array}{ccccccccc}
0 \to & I^{\cdot}_A & \to & I^{\cdot}_B & \to & I^{\cdot}_C & \to 0 \\
 & \uparrow & & \uparrow & & \uparrow & \\
0 \to & A & \to & B & \to & C & \to 0
\end{array}$$

Since I^q_A is injective, we get an exact sequence $0 \to F(I^q_A) \to F(I^q_B) \to F(I^q_C) \to 0$ for every q, and then choose the double complexes J^{pq}_A, *etc.* to fit in the three-dimensional ladder whose typical slice is:

$$\begin{array}{ccccccc}
0 \to & J^{\cdot q}_A & \to & J^{\cdot q}_B & \to & J^{\cdot q}_C & \to 0 \\
 & \uparrow & & \uparrow & & \uparrow & \\
0 \to & F(I^q_A) & \to & F(I^q_B) & \to & F(I^q_C) & \to 0
\end{array}$$

The complex $G(J^{\cdot}_C)$ computes the derived functors $R^{\cdot}G$ on $F(C)$. Let $\tilde{E}^1_C = \ker \delta \cap \operatorname{im}(G(J^1_B) \to G(J^1_C))$ be the group of liftable cochains in $G(J^1_C) = E^{10}_{1C}$, (so $\tilde{E}^1_C = \tilde{G}(J^1_C)$, in the notation of Section 5). Set $\tilde{E}^0_C = \delta^{-1}\tilde{E}^1_C \subseteq E^{00}_{1C}$. We are now ready to state:

Proposition 7 *There exist coboundary maps $\partial_v \colon E^{00}_{1C} \to E^{01}_{1A}$ and $\partial_h \colon \tilde{E}^1_C \to E^{20}_{2A}$ such* *that for any $a \in \tilde{E}^0_C$, $\partial_v a$ lands inside $E^{01}_{2A} \subseteq E^{01}_{1A}$, and the following diagram commutes:*

$$\begin{tikzcd} E^{01}_{2A} \arrow[drr, "d_2"] & & \\ \tilde{E}^0_C \arrow[u, "\partial_v"] \arrow[r, "d_1"'] & \tilde{E}^1_C \arrow[r, "\partial_h"'] & E^{20}_{2A} \end{tikzcd}$$

Here $d_1 = \delta$ is the spectral sequence differential on E_{1C} and d_2 its analog on E_{2A}.

Proof We spell out the definition of the coboundary maps ∂_v, ∂_h, leaving the proof of the commutativity to the reader.

The "vertical" coboundary ∂_v: We define $\partial_v \colon E^{00}_{1C} = G(J^0_C) \to E^{01}_{1A}$ as the connecting homomorphism arising from

$$E_0 : \quad \begin{tikzcd} 0 \arrow[r] & G(J^{01}_A) \arrow[r] & G(J^{01}_B) \arrow[r] & G(J^{01}_C) \arrow[r] & 0 \\ 0 \arrow[r] & G(J^{00}_A) \arrow[r] \arrow[u, "d"] & G(J^{00}_B) \arrow[r] \arrow[u, "d"] & G(J^{00}_C) \arrow[r] \arrow[u, "d"] & 0 \end{tikzcd}$$

Restricted to $G(F(C)) \hookrightarrow G(J^0_C)$, this map is nothing but $G(F(C)) \xrightarrow{G(\partial)} G(R^1F(A)) = E^{01}_{2A}$ induced from the classic connecting homomorphism of the long exact sequence of the derived functors of F.

The "horizontal" coboundary ∂_h: The connecting homomorphism in question should in principle be a map $E^{10}_{1C} \to E^{20}_{2A}$, but this turns out to be too much to ask for. Indeed, consider the corresponding piece of our 3D spectral sequence ladder at the stage E_0:

$$(9) \qquad E_0 : \quad \begin{tikzcd} 0 \arrow[r] & G(J^{20}_A) \arrow[r] & G(J^{20}_B) \arrow[r] & G(J^{20}_C) \arrow[r] & 0 \\ 0 \arrow[r] & G(J^{10}_A) \arrow[r] \arrow[u, "\delta"] & G(J^{10}_B) \arrow[r] \arrow[u, "\delta"] & G(J^{10}_C) \arrow[r] \arrow[u, "\delta"] & 0 \end{tikzcd}$$

To pass to the E_1 stage we take the kernel of d since we are on the bottom row of E_0. Note that d is "perpendicular" to the differential δ in (9), which accounts for the (possible) failure of right exactness of the ensuing ladder:

$$(10) \qquad E_1 : \quad \begin{tikzcd} 0 \arrow[r] & G(J^2_A) \arrow[r] & G(J^2_B) \arrow[r] & G(J^2_C) \\ 0 \arrow[r] & G(J^1_A) \arrow[r] \arrow[u] & G(J^1_B) \arrow[r] \arrow[u] & G(J^1_C) \arrow[u] \end{tikzcd}$$

This failure precludes the definition of a coboundary map on the entire $G(J_C^1) = E_{1C}^{10}$. Still, we recognize the diagram (10) as being part of the ladder (8) associated to the exact sequence $0 \to F(A) \to F(B) \to F(C)$ in $\mathcal{B}$. Set

$$\partial_h \colon \tilde{E}_C^1 \to R^1G(F(A)) = E_{2A}^{20}$$

to be the fake coboundary map defined as in Section 5.

The proof of the Proposition now becomes a simple but tedious diagram chase. ■

Remarks

(1) This proposition will allow us to replace a computation of d_2 with a computation of d_1, which is much simpler: notice, for example, that the $\tilde{E}$'s are defined solely in reference to resolutions of $F(B)$ and $F(C)$, and make no mention of the rest of the spectral sequence machinery.

(2) One might expect that $\partial_h d_1$ is always 0, since it looks like a connecting homomorphism for δ evaluated on an δ-exact cochain. But this is not quite right: even if $b = \delta a$, the usual Snake lemma argument showing that $\partial_h b$ is a coboundary requires a to be liftable to $G(J_B^0)$, which does not necessarily happen. If it does, then $\partial_h b$ is indeed 0.

7 Lifting Across d_2

We will now use our spectral sequence lemma to give a general template for lifting across d_2. We keep the notation of the preceding sections. Start with exact sequences $0 \to X \to Y \to Z$ in $\mathcal{B}$ and $0 \to A \to B \to C \to 0$ in $\mathcal{A}$ living in a diagram

(11)
$$\begin{array}{ccccccc} 0 & \longrightarrow & X & \longrightarrow & Y & \longrightarrow & Z \\ & & \downarrow{\scriptstyle\alpha} & & \downarrow{\scriptstyle\alpha} & & \downarrow{\scriptstyle\alpha} \\ 0 & \longrightarrow & F(A) & \longrightarrow & F(B) & \longrightarrow & F(C) \end{array}$$

Pick compatible injective resolutions over this ladder required to set up the spectral sequences from Section 6, $0 \to X \to J_X^{\cdot}, 0 \to F(A) \to J_A^{\cdot}$, *etc.* As in Section 5, form the groups of liftable cocycles $\tilde{G}(J_Z^1), \tilde{G}(J_C^1) = \tilde{E}_C^1$ which are the domains for fake coboundary maps relative to our choice of injective resolutions. They fit into the commutative diagram:

(12)
$$\begin{array}{ccc} \tilde{G}(J_Z^1) & \xrightarrow{\partial} & [R^2G](X) \\ \downarrow{\scriptstyle\alpha} & & \downarrow{\scriptstyle\alpha} \\ \tilde{E}_C^1 = \tilde{G}(J_C^1) & \xrightarrow{\partial_h} & [R^2G](F(A)) \end{array}$$

This set-up will help us deal with the following basic

https://doi.org/10.4153/CJM-2005-032-9 Published online by Cambridge University Press

Question Given $z \in \tilde{G}(J_Z^1)$, is $\partial z \neq 0 \in [R^2G](X)$?

To answer affirmatively, it will suffice to show that $\alpha(\partial z)$ is non-zero in $[R^2G](F(A))$. This would follow if we could lift $\alpha(\partial z)$ across d_2 to an element of $G([R^1F](A))$, and show that this lift does not come from $[R^1(G \circ F)](A)$ in the long exact sequence

$$0 \to [R^1G](F(A)) \to [R^1(G \circ F)](A) \to G([R^1F](A)) \xrightarrow{d_2} [R^2G](F(A)),$$

coming from the spectral sequence for $G \circ F$. On this level of abstraction, it is not at all clear that this is a useful strategy. We have a concrete example in mind, though: the Grothendieck spectral sequence of Proposition 2 computing $H^2(X, \mathbb{Z}/p\mathbb{Z})$. Here, $G([R^1F](A))$ $(= \bigoplus_{v\nmid\infty} \operatorname{Hom}(U_v, \mathbb{Z}/p\mathbb{Z}))$ is a much more concrete object than $[R^2G](F(A))$ $(= H^2(X, \mathbb{Z}/p\mathbb{Z}))$, so the computation will indeed go through. All we have to do is find a d_2-lift of $\alpha(\partial z)$.

Note that our question makes no reference to the sequence $0 \to A \to B \to C \to 0$, which should indeed be thought of as auxiliary and chosen with a concrete $z \in \tilde{G}(J_Z^1)$ in mind. Specifically, we have

Proposition 8 *Assume the class $[z]$ represented by a liftable cocycle $z \in \tilde{G}(J_Z^1)$ is in* $\ker([R^1G](Z) \xrightarrow{\alpha} [R^1G](F(C))$. *Then we can explicitly find a lift of $\alpha(\partial z)$ across d_2.*

Proof Since the complex

$$G(J_C^0) \xrightarrow{\delta} G(J_C^1) \xrightarrow{\delta} G(J_C^2) \xrightarrow{\delta} \cdots$$

computes $[R^{\cdot}G](F(C))$, we can find $y \in G(J_C^0)$ with $d_1 y = \delta y = \alpha z$. Since $z \in \tilde{G}(J_Z^1)$, $\alpha z \in \tilde{G}(J_C^1) = \tilde{E}_C^1$ and $y \in \tilde{E}_C^0$ (z liftable $\Rightarrow$ αz liftable). We can therefore apply our spectral sequence Lemma 7 to conclude that $\partial_v y$ is our lifting of $\alpha(\partial z)$:

$$\alpha(\partial z) = \partial_h(\alpha z) = \partial_h(d_1 y) = d_2(\partial_v y). \qquad \blacksquare$$

8 The Meat of the Argument

In this section we use the machinery developed so far to prove that, under certain assumptions, the coboundary map $H^1_{fl}(X_n, \mu) \xrightarrow{\delta} H^2_{fl}(X_n, \mathbb{Z}/p\mathbb{Z})$ is non-zero.

8.1 Preliminaries

The p-torsion of our curve $E_{/\mathbb{Q}}$ lies in a *non-split* exact sequence of $G_{\mathbb{Q}}$-modules

(13) $$0 \to \mathbb{Z}/p\mathbb{Z} \to E[p] \to \mu_p \to 0.$$

Fix once and for all a basis $\langle T_0, T_1 \rangle$ of $E[p](\bar{K})$ such that $T_0 \in E[p](\mathbb{Q})$. Relative to this basis, the action of $\sigma \in G_{\mathbb{Q}}$ on $E[p]$ is given by the matrix

(14) $$\begin{pmatrix} 1 & c(\sigma) \\ 0 & \omega(\sigma) \end{pmatrix}.$$

Here $\omega^{-1}c\colon G_{\mathbb{Q}} \to \mathbb{Z}/p\mathbb{Z}$ is a 1-cocycle in $H^1(\mathbb{Q}, \mathbb{Z}/p\mathbb{Z}(-1)) \cong \operatorname{Ext}^1_{G_{\mathbb{Q}}}(\mu_p, \mathbb{Z}/p\mathbb{Z})$ whose class corresponds to the extension $E[p]$.

https://doi.org/10.4153/CJM-2005-032-9 Published online by Cambridge University Press

8.2 The Main Theorem

The following theorem provides the key ingredient for the strategy outlined in Section 3.

Theorem 1 *Assume that there is a level n in the cyclotomic $\mathbb{Z}_p$-tower, and a prime $v|l|N$ of K_n for which the following condition holds:*

$(*)$ *There exists a global unit $a \in \mathcal{O}_n^\times$ which is not a p-th power mod v.*

(This forces $\mu_p \subseteq \mathbb{F}_l^\times \subseteq \mathbb{F}_v^\times$.) Then the coboundary map associated with (2),

$$H^1_{fl}(X_n, \mu) \xrightarrow{\delta} H^2(X_n, \mathbb{Z}/p\mathbb{Z})$$

is non-zero.

Proof We will be working entirely at the finite level n, so we again suppress it from the notation. We start with a class $b \in H^1_{fl}(X, \mu)$. Recall our strategy for proving $\delta b \neq 0$ from Section 3: we lift δb across $d_2\colon \bigoplus_{v\nmid\infty} \mathrm{Hom}(U_v, \mathbb{Z}/p\mathbb{Z}) \to H^2(X, \mathbb{Z}/p\mathbb{Z})$ to a collection of homomorphisms $(f_v\colon U_v \to \mathbb{Z}/p\mathbb{Z})$, and then find a global unit a such that $\sum_{v\nmid\infty} f_v(a_v) \neq 0$.

Remark We will compute on the étale site. This might seem strange, since we are lifting across d_2 the image of the coboundary in *flat* cohomology,

$$H^1_{fl}(X, \mu) \xrightarrow{\delta} H^2_{fl}(X, \mathbb{Z}/p\mathbb{Z}).$$

The étale cohomology does not "see" most of the classes $(a, \{t_v\}_{v|N}) \in H^1_{fl}(X, \mu)$ since the representing cocycle is usually ramified over p. This is why the class we will work with will have $a = 1$. Still, the étale site is comfortable to work with, chiefly because $i_*E[p] = \mathcal{E}[p]$ as étale sheaves, and because the Gysin sequence (4) naturally lives on it. It is possible, if more involved, to lift a general $\delta(b, \{t_v\}_{v|N})$, but even this is done by "smoothing" the cocycle at p and doing an étale computation. In any case, $0 \to \mathbb{Z}/p\mathbb{Z} \to \mathcal{E}[p] \to \mu \to 0$ remains exact when viewed as a sequence of étale sheaves.

The Lifting Set-up

So, let us do a concrete application of Section 7. Consider the functors

$$\mathcal{S}h((\mathrm{Spec}\, K)_{\acute{e}t}) \xrightarrow{i_*} \mathcal{S}h(X_{\acute{e}t}) \xrightarrow{\Gamma(\,\cdot\,)=\Gamma(X,\,\cdot\,)} \mathcal{A}b$$

from G_K-modules to étale sheaves over X to Abelian groups. We have a ladder

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{Z}/p\mathbb{Z} & \longrightarrow & \mathcal{E}[p] & \longrightarrow & \mu & \longrightarrow & 0 \\ & & \| & & \| & & \downarrow & & \\ 0 & \longrightarrow & i_*\mathbb{Z}/p\mathbb{Z} & \longrightarrow & i_*E[p] & \longrightarrow & i_*\mu_p & & \end{array}$$

https://doi.org/10.4153/CJM-2005-032-9 Published online by Cambridge University Press

which we recognize as an instance of the diagram (11) from Section 7. Choose the panoply of compatible injective resolutions $J^{\cdot}_{\mathbb{Z}/p\mathbb{Z}}$, $J^{\cdot}_{i_*\mu_p}$, *etc.* as in that section. We are ultimately interested in computing the map $H^1_{fl}(X,\mu) \xrightarrow{\delta} H^2(X,\mathbb{Z}/p\mathbb{Z})$ which appears on the right edge of the diagram:

$$\begin{tikzcd}
 & & H^1_{fl}(X,\mu) \arrow[d] \\
\tilde{\Gamma}(J^1_\mu) \arrow[r] \arrow[d, "\alpha"'] & H^1(X,\mu) \arrow[r, "\delta"] \arrow[ur] & H^2(X,\mathbb{Z}/p\mathbb{Z}) \arrow[d, equal] \\
\tilde{E}^1_{i_*\mu_p} = \tilde{\Gamma}(J^1_{i_*\mu_p}) \arrow[rr, "\partial_h"'] & & H^2(X,\mathbb{Z}/p\mathbb{Z})
\end{tikzcd}$$

The commutative square in this diagram is precisely diagram (12) from Section 7. To apply Proposition 8 we will need to find a liftable cocycle $b \in \tilde{\Gamma}(J^1_\mu)$ whose class $[b]$ is in $\ker(H^1(X,\mu) \to H^1(X,i_*\mu_p))$. Liftability of b will be automatic, since the map of *étale* sheaves $\mathcal{E}[p] \to \mu$ is onto.

Finding the Right b

Since $\mu_{/X} \to i_*(\mu_{p/K})$ factors as $\mu_{/X} \to \mu_{p/X} \to i_*(\mu_{p/K})$, it will suffice to consider classes in $\ker(H^1(X,\mu) \to H^1(X,\mu_p))$. To get at this kernel, consider the short exact sequence of étale sheaves over X,

$$0 \to \mu \to \mu_p \to \bigoplus_{v|N} i_{v*}\mu_p \to 0 \tag{15}$$

analogous to that of Lemma 4, and the corresponding piece of the long exact cohomology sequence with connecting homomorphism D:

$$0 \to \bigoplus_{w|N} \mu_p(\mathbb{F}_w) \xrightarrow{D} H^1(X,\mu) \to H^1(X,\mu_p).$$

By assumption $(*)$, there is a $v|N$ with $\mu_p(\mathbb{F}_v) \neq 1$. Fix once and for all a prime $\bar{v}|v$ of $\bar{K}$. The image of the basis element T_1 under $E[p] \to \mu_p$ gives a non-trivial $\zeta \in \mu_p(\bar{K})$. Define $\zeta_v \in \mu_p(\mathbb{F}_v) \subset \bigoplus_{w|N} \mu_p(\mathbb{F}_w)$ by $\zeta \equiv \zeta_v \pmod{\bar{v}}$. We obtain the desired class simply by setting $[b] = D(\zeta_v)$. As $[b] \in \ker(H^1(X,\mu) \to H^1(X,\mu_p))$, αb is a coboundary of a 0-cochain for $i_*\mu_p$, for any cocycle b representing $[b]$. Our spectral sequence lemma works on the level of resolutions, not cohomology, so we need to find this cochain explicitly.

The Čech Cochain

First we represent $\zeta_v \in H^0(X, \bigoplus_{w|N} i_{w*}\mu_p)$ by a Čech cocycle. To be more precise, we will write down a 0-cochain for μ_p lifting ζ_v, as this is the intermediate step in computing $[b] = D(\zeta_v)$.

Set $K(U_0) = L = K(\zeta)$, $K(U_1) = K$, and $v' = \bar{v}|_{K(U_0)}$. The $K(U_i)$'s are the function fields of the two components of the étale cover $U = U_0 \coprod U_1 \to X$ given by:

$$U_0 = \operatorname{Spec} \mathcal{O}_{K(U_0)}[1/pN] \cup \{v'\}$$
$$U_1 = \operatorname{Spec} \mathcal{O}_K \setminus \{v\}.$$

For the picture, see Figure 3.

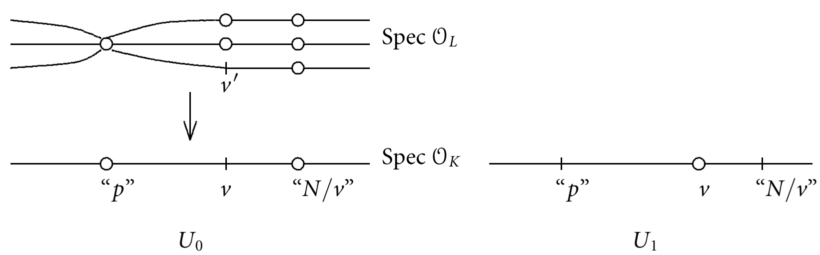

Figure 3

The Čech cochain $y \in \check{C}^0(U, \mu_p)$ defined on U_0 by $y_0 = \zeta \in \mu(U_0) = \mu_p(U_0)$ and on U_1 by $y_1 = 1 \in \mu(U_1)$ lifts $\zeta_v \in H^0(X, \bigoplus_{w|N} i_{w*}\mu_p)$ as promised. Therefore $\delta y = b$ is a cocycle representing our class $[b] \in \ker(H^1(X, \mu) \to H^1(X, i_*\mu_p))$.

Let αy stand for y thought of as a Čech 0-cochain for $i_*\mu_p$. At least in degrees 0 and 1, the complex of Čech sheaves $\check{\mathcal{C}}^{\cdot}(U, i_*\mu_p)$ maps into the resolution $0 \to i_*\mu_p \to J^{\cdot}_{i_*\mu_p}$. By abuse of notation, we still denote by αy the corresponding element of the $\Gamma(J^0_{i_*\mu_p})$ term of the complex

$$0 \to \Gamma(i_*\mu_p) \to \Gamma(J^0_{i_*\mu_p}) \xrightarrow{\delta} \Gamma(J^1_{i_*\mu_p}) \xrightarrow{\delta} \Gamma(J^2_{i_*\mu_p}) \to \cdots$$

which computes $H^*(X, i_*\mu_p)$. We have $\delta(\alpha y) = \alpha b \in \tilde{E}^1_{i_*\mu_p}$, the group of liftable cocycles, because b is automatically liftable. By definition, $\alpha y \in \tilde{E}^0_{i_*\mu_p}$.

Now the comes the crucial step. We apply the spectral sequence Lemma 7:

$$d_2\partial_v(\alpha y) = \partial_h d_1(\alpha y) = \partial_h(\alpha b) = \alpha(\delta[b]) \cong \delta[b] \in H^2(X, \mathbb{Z}/p\mathbb{Z}). \tag{16}$$

We see that $\partial_v(\alpha y)$ is the desired d_2-lift of $\delta[b]$. Before representing it explicitly, we recall Remark (2) at the end of Section 6. Indeed, when the extension (13) is non-split, $\partial_h d_1(\alpha y)$ is not necessarily zero. As in the Remark, the 0-cochain $\alpha y = \{(U_0, \zeta), (U_1, 1)\}$ for $i_*\mu_p$ cannot be lifted to a 0-cochain for $i_*E[p]$, as is apparent from the geometry of y. Indeed, say $U' \to U_0$ were an *étale* open cover such that $\zeta \in i_*\mu_p(U') = \mu_p(K(U'))$ lifts to $E[p](K(U'))$. Then all of $E[p]$ must be rational over $K(U')$. Since the extension (13) is non-split, $K(U')/K$ must ramify at every prime above N. But U_0, and therefore U', has a point over $v|N$, hence the supposedly étale cover $U' \to U_0$ ramifies over v'.

https://doi.org/10.4153/CJM-2005-032-9 Published online by Cambridge University Press

8.2.1 Finally, a d_2-Lift

To lift $\delta[b]$, we compute $\partial_v(\alpha y) \in H^0(X, R^1 i_* \mathbb{Z}/p\mathbb{Z})$ explicitly. Let $f_i = \partial_i y_i, i = 1, 2$, where $\partial_i \colon \mu_p(K(U_i)) \to \operatorname{Hom}(G_{K(U_i)}, \mathbb{Z}/p\mathbb{Z})$ is the coboundary map associated to (13) viewed as a sequence of $G_{K(U_i)}$-modules. The homomorphisms $f_i \colon G_{K(U_i)} \to \mathbb{Z}/p\mathbb{Z}$ are easy to compute, given the Galois module structure (14) of $E[p]$:

$$f_0 = c \colon G_{K(U_0)} \to \mathbb{Z}/p\mathbb{Z}, \quad f_1 = 0 \colon G_{K(U_1)} \to \mathbb{Z}/p\mathbb{Z}.$$

(The 1-cocycle c for $\mathbb{Z}/p\mathbb{Z}(-1)$ becomes a homomorphism when restricted to $G_{K(U_0)}$.) The collection $f := \{(U_0, f_0), (U_1, f_1)\}$ gives a 0-cochain for the presheaf

$$U \mapsto H^1(K(U), \mathbb{Z}/p\mathbb{Z}) = \operatorname{Hom}(G_{K(U)}, \mathbb{Z}/p\mathbb{Z}).$$

This presheaf sheafifies to $R^1 i_* \mathbb{Z}/p\mathbb{Z}$, and f yields a global section which a moment's reflection will convince you is nothing other than

$$\partial_v(\alpha y) \in E_{2(\mathbb{Z}/p\mathbb{Z})}^{01} = H^0(X, R^1 i_* \mathbb{Z}/p\mathbb{Z}).$$

To translate this description of $\partial_v(\alpha y)$ from $H^0(X, R^1 i_* \mathbb{Z}/p\mathbb{Z})$ to

$$\bigoplus_{v \nmid \infty} \operatorname{Hom}(U_v, \mathbb{Z}/p\mathbb{Z}),$$

we simply take a $w \in X$, pick an open U_0 or U_1 covering it, and restrict the corresponding f_i to the inertia group of some $\bar{w}|w$ over $K(U_i)$. In other words, if $w \neq v$, it is covered by U_1, and the w-component of f is 0. An exercise for the reader: what if $w \nmid pN$, so that it is covered by U_0 also? The v-component is c restricted to $I_{\bar{v}/v}$, which is non-zero precisely because we assumed that (13) is non-split. It is Frobenius-invariant, and thus descends to a map $f_v \colon U_v \to \mathbb{Z}/p\mathbb{Z}$ since v splits completely in $K(U_0)$.

To finish off the proof of Theorem 1, we invoke the unit $a \in \mathcal{O}_n^\times$. Since by Assumption $(*)$ a is not a p-th power mod v, $f_v(a_v) \neq 0$, and

$$\sum_{w \nmid \infty} f_w(a_w) = f_v(a_v) \neq 0,$$

so the collection $(f_w \colon U_w \to \mathbb{Z}/p\mathbb{Z})$ is not the restriction of a global homomorphism $f \colon G_K \to \mathbb{Z}/p\mathbb{Z}$. ■

The particular shape of f_v is contingent on our choice of $\zeta_v \equiv \zeta \pmod{\bar{v}}$. Had we chosen a different root of unity, its lift would change by a constant multiple, but in any case we have the following more precise theorem:

https://doi.org/10.4153/CJM-2005-032-9 Published online by Cambridge University Press

Theorem 2 *With notations of this section, assume there is a prime $v|N$ of K with $|\mathbb{F}_v| \equiv 1 \pmod{p}$ (no assumption is made on global units mod v). Pick a $\zeta_v \in \mu_p(\mathbb{F}_v)$ non-trivial, and let $b \in H^1_{fl}(X, \mu)$ be its image under*

$$\mu_p(\mathbb{F}_v) \subset H^0(X, \bigoplus_{w|N} i_{w*}\mu_p) \overset{D}{\hookrightarrow} H^1_{fl}(X, \mu).$$

Then $\delta b \in H^2(X, \mathbb{Z}/p\mathbb{Z})$ lifts across $\bigoplus_{v\nmid\infty} \mathrm{Hom}(U_v, \mathbb{Z}/p\mathbb{Z}) \xrightarrow{d_2} H^2(X, \mathbb{Z}/p\mathbb{Z})$ to a collection of homomorphisms

$$(f_w \colon U_w \to \mathbb{Z}/p\mathbb{Z})$$

with $f_w = 0$ if $w \neq v$, and $f_v \neq 0$.

9 Examples

Finally, we produce some examples to show that the above theory not only has content, but also yields new curves for which we can prove $\mu(E)_p = 0$. In fact, as soon as we get one new example, we trivially get infinitely many: any curve E' with $E'[p] \cong E[p]$ also satisfies $\mu(E')_p = 0$, as the argument depended only on the structure of p-torsion. For $p = 3$ or 5 we can in fact do better and produce infinitely many examples with pairwise non-isomorphic p-torsion.

Before stating the general theorems, we will illustrate the strategy on a concrete example when $p = 3$.

9.1 1990D1

Take $p = 3$, and consider the curve 1990D1 from Cremona's tables:

$$E_1 : y^2 + xy = x^3 - 6390x - 215900.$$

E_1 is good ordinary at 3, $E_1(\mathbb{Q})_{\mathrm{tors}}$ has order 3, and the corresponding exact sequence

$$0 \to \mathbb{Z}/3\mathbb{Z} \to E_1[3] \to \mu_3 \to 0$$

does not split, since we read from the tables that there is only one other curve in the isogeny class of E_1. The conductor factors as $1990 = 2 \cdot 5 \cdot 199$, and the corresponding reduction types and Tamagawa numbers are as follows: at $2 - I_{27}, c_2 = 27$; at $5 - I_3, c_5 = 3$; at $199 - I_1, c_{199} = 1$. Since $E[p]$ ramifies at $v|N$ if and only if $p \nmid c_v$, $\mathcal{E}[3]$ fits into the exact sequence

$$0 \to \mathbb{Z}/3\mathbb{Z} \to \mathcal{E}[3] \to \mu \to 0,$$

where μ is μ_3 punctured above 199.

The following formula for the p-adic valuation of $f_E^{\mathrm{alg}}(0)$ when E is good ordinary at p and $\mathrm{Sel}_{p^\infty}(E_{/\mathbb{Q}})$ is finite has been obtained by Perrin-Riou in the CM case, and by Schneider in general (see [3], p. 35):

$$\nu_p(f_E(0)) = \nu_p(\mathrm{Tam}_E\,|\tilde{E}(\mathbb{F}_p)|^2|\,\mathrm{Sel}_{p^\infty}(E_{/\mathbb{Q}})|/|E(\mathbb{Q})|^2), \tag{17}$$

where Tam_E is the product of the Tamagawa numbers and $\tilde{E}$ is the reduction of E at p. In the case at hand, we read off from the tables that $\text{Ш}_{E_1}(\mathbb{Q})[3^\infty] = 0$, rk $E_1(\mathbb{Q}) = 0$, so $\mathrm{Sel}_{3^\infty}(E_{1/\mathbb{Q}}) = 0$. Formula (17) gives $f(E_1) = 27 \cdot 3 \cdot 1 \cdot 9 \cdot 1/9 = 81$ up to units, which tells us nothing more than $\mu(E_1)_3 \le 4$. We can show that, in fact, $\mu(E_1)_3 = 0$.

Since $9 \parallel 199^2 - 1$, 199 splits completely in K_1 and the three primes above it are inert thereafter. Over X_∞ we thus have

$$0 \to \mu_3(\mathbb{F}_{199})^3 \to H^1_{fl}(X_\infty, \mu) \to H^1_{fl}(X_\infty, \mu_p) \to 0.$$

The primes above 199 in $K_1 = \mathbb{Q}(\alpha)$ correspond to the roots mod 199 of $x^3 - 3x + 1 = 0$, the minimal polynomial of

$$\alpha = \zeta_9^{-1}\frac{1-\zeta_9^4}{1-\zeta_9^2}.$$

Those roots, $6, 34, 159 \pmod{199}$ may seem perfectly interchangeable, but in fact they are not: $159 \equiv 69^3 \pmod{199}$, whereas $6, 34 \notin \mathbb{F}_{199}^{\times 3}$. Fix α and name the three primes $\nu_i|199$ of K_1 by stipulating that

$$\alpha \equiv 159 \pmod{\nu_0},\ \alpha \equiv 6 \pmod{\nu_1},\ \alpha \equiv 34 \pmod{\nu_2}.$$

Then α fits into a norm-coherent sequence $\{\alpha_n\}, \alpha_1 = \alpha, \alpha_n \in \mathcal{O}_n^\times$. Let $\nu_{i,n}$ be the unique prime of K_n above ν_i. We claim that α_n is a cube mod $\nu_{0,n}$ and a non-cube mod $\nu_{1,n}, \nu_{2,n}$. Indeed, $\nu_{i,n}$ is inert over ν_i, so we have a commutative diagram whose vertical arrows are induced by the norm map $N_{n/1}\colon K_n \to K_1$:

$$\begin{tikzcd}
\mathcal{O}_n^\times \arrow[r] \arrow[d, "N_{n/1}"'] & \mathbb{F}_{\nu_{i,n}}^\times \arrow[r] \arrow[d, "N"'] & \mathbb{F}_{\nu_{i,n}}^\times/\mathbb{F}_{\nu_{i,n}}^{\times 3} \arrow[d, "N"'] \\
\mathcal{O}_1^\times \arrow[r] & \mathbb{F}_{\nu_i}^\times \arrow[r] & \mathbb{F}_{\nu_i}^\times/\mathbb{F}_{\nu_i}^{\times 3}
\end{tikzcd}$$

The last map is an isomorphism, being a surjection of two groups of order 3. Therefore, α_n is a cube mod $\nu_{i,n}$ if and only if $N_{n/1}\alpha_n = \alpha$ is a cube mod ν_i.

We now construct a divisible element in $\ker(H^1_{fl}(X_\infty, \mu) \to H^1_{fl}(X_\infty, \mu_p))$. Fix an $r \ge 1$ big enough so that $T^{p^r} H^1_{fl}(X_\infty, \mu) \subseteq H^1_{fl}(X_\infty, \mu)_{\mathrm{div}}$, as in Section 4. Let $\rho = \gamma^{p^r}$, so that $T^{p^r} \in \mathbb{F}_p[[T]]$ acts as $\rho - 1$. For $i = 1$ or 2, α_r mod $\nu_{i,r}$ has no cube root in $\mathbb{F}_{\nu_{i,r}}$, but acquires one in $\mathbb{F}_{\nu_{i,r+1}}$; call them s_1, s_2. Pick s_0 to be a cube root of α_r mod $\nu_{0,r}$ already in $\mathbb{F}_{\nu_{0,r}}$ (say $69 \in \mathbb{F}_{199} \subset \mathbb{F}_{\nu_{0,r}}$). In $\mathcal{O}_{r+1}^\times$, α_r becomes a cube mod all three $\nu_{i,r+1}$, so we can lift it to a class $(\alpha_r, \{s_0, s_1, s_2\}) \in H^1_{fl}(X_{r+1}, \mu) \to H^1_{fl}(X_\infty, \mu)$. As $\nu_{i,r+1}$ is inert over $\nu_{i,r}$, ρ acts on $\mathbb{F}_{\nu_{i,r+1}}$ and we compute

$$\begin{aligned} T^{p^r}(\alpha_r, \{s_0, s_1, s_2\}) &= (\alpha_r, \{s_0, s_1, s_2\})^{\rho-1} = (\alpha_r^{\rho-1}, \{s_0^{\rho-1}, s_1^{\rho-1}, s_2^{\rho-1}\}) \\ &= (1, \{1, \zeta_1, \zeta_2\}), \end{aligned}$$

https://doi.org/10.4153/CJM-2005-032-9 Published online by Cambridge University Press

where by our choice of the s_i's, $\zeta_1, \zeta_2 \neq 1 \in \mu_3(\mathbb{F}_{199})$. By Proposition 6, $b = (1, \{1, \zeta_1, \zeta_2\}) \in \ker(H^1_{fl}(X_\infty, \mu) \to H^1_{fl}(X_\infty, \mu_p))$ is divisible.

Notice that the class b lives in $H^1_{fl}(X_1, \mu)$; passing to X_{r+1} was necessary only to divide it by T^{p^r}. We will now show that $\delta b \in H^2_{fl}(X_1, \mathbb{Z}/p\mathbb{Z})$ has non-zero image by lifting it to $(f_w : U_w \to \mathbb{Z}/p\mathbb{Z})_{w \nmid \infty}$ and showing that

$$\sum_{w \nmid \infty} f_w(u) \neq 0$$

for a unit u in a norm-coherent sequence. By the argument of Section 3, this suffices to show that $\delta b \neq 0 \in H^2_{fl}(X_\infty, \mathbb{Z}/p\mathbb{Z})$.

Since $b = D\zeta_1 + D\zeta_2$ in the notation of Theorem 2, b is "supported" only at v_1 and v_2, and thus lifts to a collection $(f_w \colon U_w \to \mathbb{Z}/p\mathbb{Z})_{w \nmid \infty}$ with only f_{v_1}, f_{v_2} non-zero.

Select u to be the Galois conjugate of α satisfying the following congruences (obtained by cyclically permuting the congruences for α):

$$u \equiv 34 \pmod{v_0}, \quad u \equiv 159 \pmod{v_1}, \quad u \equiv 6 \pmod{v_2}.$$

We see that u is now a cube mod v_1 and a non-cube mod v_2. Thus, by Hensel's lemma, $u \in U^3_{v_1}$, $u \notin U^3_{v_2}$. Since $U_w/U^3_w \cong \mathbb{Z}/p\mathbb{Z}$ for $w \nmid 3$, we see that $f_{v_1}(u) = 0$, $f_{v_2}(u) \neq 0$, so finally

$$\sum_{w \nmid \infty} f_w(u) = f_{v_1}(u) + f_{v_2}(u) = f_{v_2}(u) \neq 0.$$

So, we are done: we have an element $b \in H^1_{fl}(X_\infty, \mu)_{\mathrm{div}}$ with $\delta b \neq 0$, which, as explained in Section 3, implies $\mu(E_1)_3 = 0$. The key to the evaluation was that we choose the class b and a unit u so that the sum giving the pairing of b and u reduces to a single summand. This avoids potentially hard-to-control cancellations.

9.2 3314B1

The same argument, *mutatis mutandis*, applies to Cremona's curve 3314B1 given by the equation

$$E_2 : y^2 + xy = x^3 + 58x - 22684,$$

with 1657 replacing 199. Unlike E_1, E_2 has rank 1: Cremona computes that $(104, 1002)$ is a point of infinite order! Since $f_E(0) = 0$, it carries no information about μ. In a sense the success of our method is not surprising: both the λ and the μ invariants contribute to $f_E(0)$, while our approach zeroes in on μ only (while losing much useful information on λ).

9.3 A Generalization

Let us extract a proof template from the preceding two examples. For a fixed odd prime p, any number field F and its integral ideal $\mathcal{N}$, we define the *support* at $\mathcal{N}$ of a global unit $x \in \mathcal{O}_F^\times$ by

$$\mathrm{Supp}^F_{\mathcal{N}}(x) = \left\{ v | \mathcal{N} : x \text{ not a } p\text{-th power in } \mathbb{F}_v^\times \right\}.$$

https://doi.org/10.4153/CJM-2005-032-9 Published online by Cambridge University Press

Note that if $v \in \mathrm{Supp}^F_{\mathcal{N}}(x)$ for some $x \in \mathcal{O}_F^\times$, then $\mu_p \subset \mathbb{F}_v$. Moreover, the rational prime l below v is not inert in $F/\mathbb{Q}$: if it were, the norm from F to $\mathbb{Q}$ would induce the vertical maps in the diagram

$$\begin{tikzcd} \mathcal{O}_F^\times \arrow[r] \arrow[d] & \mathbb{F}_v^\times/\mathbb{F}_v^{\times p} \arrow[d, "\cong"'] \\ \{\pm 1\} = \mathbb{Z}^\times \arrow[r] & \mathbb{F}_l^\times/\mathbb{F}_l^{\times p} \end{tikzcd}$$

which would force the reduction mod v of any unit in $\mathcal{O}_F$ to be a p-th power. When $F = K_n$, these two necessary conditions simply translate into

$$v \in \mathrm{Supp}^{K_n}_{\mathcal{N}}(x) \text{ for some } x \in \mathcal{O}_n^\times \;\Rightarrow\; p^2 | l-1. \tag{18}$$

This notion of support will help us capture the general argument implicit in the above example:

Theorem 3 *Assume there is a level K_n in the $\mathbb{Z}_p$-tower satisfying the following conditions:*

(a) *All primes $v|N$ are inert in K_∞/K_n.*
(b) *$T^{p^n} H^1_{fl}(X_\infty, \mu) \subset H^1_{fl}(X_\infty, \mu)_{div}$.*
(c) *There exist units $\alpha, u \in \mathcal{O}_n^\times$ such that both are universal norms for the $\mathbb{Z}_p$-tower K_∞/K_n, and such that $\mathrm{Supp}^{K_n}_N(\alpha) \cap \mathrm{Supp}^{K_n}_N(u) = \{v_0\}$, a singleton.*

Then, given our assumptions on E, we can conclude that $\mu(E)_p = 0$.

Proof The proof essentially follows the pattern of the example. As above, we choose an $s_v \in \bar{\mathbb{F}}_v$ for all $v|N$ such that $s_v^p \equiv \alpha \pmod{v}$. T^{p^n} acts on $H^1_{fl}(X_\infty, \mu)$ as $\gamma^{p^n} - 1 = \rho - 1$ and fixes all $v|N$, so we can compute

$$\begin{aligned} T^{p^r}(\alpha, \{s_v\}_{v|N}) &= (\alpha, \{s_v\}_{v|N})^{\rho-1} = (\alpha^{\rho-1}, \{s_v^{\rho-1}\}_{v|N}) \\ &= (1, \{\zeta_v\}_{v|N}) =: b \in H^1_{fl}(X_\infty, \mu)_{\mathrm{div}}, \end{aligned}$$

where $\zeta_v \neq 1$ precisely when $s_v \notin \mathbb{F}_v$, *i.e.*, when $v \in \mathrm{Supp}^{K_n}_N(\alpha)$. Theorem 2 will then lift the divisible class $b = (1, \{\zeta_v\}_{v|N})$ to a collection of functions $(f_w \colon U_w \to \mathbb{Z}/p\mathbb{Z})$, w ranging over all primes of K_n, such that $f_w \neq 0$ precisely when $w \in \mathrm{Supp}^{K_n}_N(\alpha)$.

The terms in the sum $\sum_{w\nmid\infty} f_w(u_w)$ are non-zero precisely when $f_w \neq 0$ *and* u is not a p-th power mod w, *i.e.*, for $w \in \mathrm{Supp}^{K_n}_N(\alpha) \cap \mathrm{Supp}^{K_n}_N(u) = \{v_0\}$. So the above sum really has only one term, and no cancellation is possible:

$$\sum_{w\nmid\infty} f_w(u) = f_{v_0}(u_v) \neq 0.$$

We conclude $\delta \neq 0$ on $H^1_{fl}(X_\infty, \mu)_{\mathrm{div}}$, as desired. ■

https://doi.org/10.4153/CJM-2005-032-9 Published online by Cambridge University Press

For every $l|N$ define the exponent m_l by $p^{m_l+1} \parallel l-1$. The prime l splits completely in K_{m_l} and is inert in K_∞/K_{m_l}.

Here is a situation where the conditions of Theorem 3 hold:

Theorem 4 *Suppose that there is exactly one prime $l|N$ satisfying $m_l \geq 2$. For this l, also assume the following:*

for at least one prime λ of K_{m_l-1} above l, π_{m_l-1} is not *a p-th power mod λ.*

Then the conditions of Theorem 3 *are satisfied. (Here π_{m_l-1} is the generator of the prime above p in K_{m_l-1} chosen in Section* 1.)

Proof Set $m = m_l$. First we choose n so that $n \geq m$ and $T^{p^n} H^1_{fl}(X_\infty, \mu) \subset H^1_{fl}(X_\infty, \mu)_{\mathrm{div}}$. This n will satisfy condition (b) of Theorem 3. By the definition of m, all primes dividing l are inert in K_∞/K_m, so *a fortiori* in K_∞/K_n, thus satisfying condition (a). Most of our work, then, will focus on producing the units $\alpha, u \in \mathcal{O}_n^\times$ satisfying condition c). In fact, we will start by producing suitable units $\alpha', u' \in \mathcal{O}_m^\times$, and the lifting to $\mathcal{O}_n$ will be a formality we leave for the end.

We have that $\mathrm{Supp}_N^{K_m}(x) = \mathrm{Supp}_l^{K_m}(x)$ for any $x \in \mathcal{O}_m^\times$, since by assumption l is the only prime dividing N which satisfies the necessary condition (18). To study the behavior of units modulo the primes above l, it is natural to introduce the following definitions.

Set $G = G_{K_m/\mathbb{Q}} = \langle\gamma\rangle$, $R = \mathbb{F}_p[G]$, and let $\mathcal{A} \subset K_m$ be the ring of elements integral at all $\lambda|l$, so that $\pi_m \in \mathcal{A}$. Consider the R-module $V = (\prod_{\lambda|l} \mathbb{F}_\lambda^\times/\mathbb{F}_\lambda^{\times p})^0$ of vectors whose components have product 1 under the natural identification $\mathbb{F}_\lambda^\times/\mathbb{F}_\lambda^{\times p} \cong \mathbb{F}_l^\times/\mathbb{F}_l^{\times p}$. Then V is the target for the (G-equivariant) reduction map

$$\mathrm{red}\colon \mathcal{A}^\times/\mathcal{A}^{\times p} \to V,$$
$$a \mapsto (a \bmod \lambda)_{\lambda|l}.$$

We will study the R-module theory of this map to show that the image of red is large enough to contain two vectors $r, s \in V$ with a *single* place of common support (*i.e.*, a place where both have an entry $\neq 1$). Lifting them to $\mathcal{O}_m^\times$, and then to $\mathcal{O}_n^\times$, will produce our desired units α and u.

First, some basic structure theory of R: $R \cong \mathbb{F}_p[T]/T^{p^m}$ under the identification $T \leftrightarrow \gamma - 1$, and all its ideals are powers of the augmentation ideal $I = \ker(R \to \mathbb{Z}/p\mathbb{Z})$, forming the chain $I \supset I^2 \supset \cdots \supset I^{p^m} = 0$. For any subgroup $G_k = \langle\gamma^{p^k}\rangle \subseteq G$, we will be interested in the ideal

$$I^{p^k} = \langle\gamma^{p^k} - 1\rangle = \Big\{ \sum a_\sigma \sigma \;\Big|\; \sum_{\tau \in G_k} a_{\rho\tau} = 0,\ \forall \rho \in G \Big\}.$$

Since l splits completely in $K_m/\mathbb{Q}$ and is inert thereafter, $V \cong I$ as R-modules (this is the main advantage of working over K_m). Call $V_k \subset V$ the submodule corresponding to $I^{p^k} \subset I$:

$$V_k = \{(x_\lambda) \in \prod_{\lambda|l} \mathbb{F}_\lambda^\times/\mathbb{F}_\lambda^{\times p} | \prod_{\tau \in G_k} x_{\tau\lambda} = 1,\ \forall \lambda|l\}$$

https://doi.org/10.4153/CJM-2005-032-9 Published online by Cambridge University Press

In particular, $\mathrm{red}(\pi_m) \in V_k \Leftrightarrow N_{K_m/K_k}(\pi_m) = \pi_k$ is a p-th power mod every λ. Our assumption on π_{m-1} now simply reads $\mathrm{red}(\pi_m) \notin V_{m-1}$.

The group of cyclotomic units modulo p-th powers, denoted $C \subset \mathcal{A}^\times/\mathcal{A}^{\times p}$, is isomorphic to $I\pi_m$. We claim that

$$\mathrm{red}(C) \supseteq V_{m-1}.$$

Since $V \cong I$, and since the R-submodules of I form a chain, it is enough to show that the reverse inclusion does not hold. Suppose $V_{m-1} \supsetneq \mathrm{red}(C) = I\pi_m$. Then we would have $V_{m-1} \supseteq R\ \mathrm{red}(\pi_m)$, contradicting our assumption that $\mathrm{red}(\pi_m) \notin V_{m-1}$.

Since $\mathrm{red}(C) \supseteq V_{m-1}$, all we have to do is find two elements $r, s \in V_{m-1}$ whose supports have precisely one $\lambda | l$ in common. This is easy: Since $p \geq 3$, we can find three distinct elements $\alpha_1, \alpha_2, \alpha_3 \in G_{m-1}$. Fix a place $\lambda_0 | l$, and let $u \in \mathbb{F}_l^\times/\mathbb{F}_l^{\times p}$ be a generator. We define $r, s \in V_{m-1}$ by specifying their components:

$$\begin{array}{rcccc} & \alpha_1\lambda_0 & \alpha_2\lambda_0 & \alpha_3\lambda_0 & \\ & \downarrow & \downarrow & \downarrow & \\ r = (& u & u^{-1} & 1 & 1\ldots1) \\ s = (& 1 & u & u^{-1} & 1\ldots1). \end{array}$$

We lift r and s to α' and u' in $C \subset \mathcal{O}_m^\times/\mathcal{O}_m^{\times p}$. Cyclotomic units being universal norms, we can choose $\alpha, u \in \mathcal{O}_n^\times$ whose norms from K_n to K_m are α' and u', respectively. Since all primes above l in K_m remain inert in K_m, there are one-to-one correspondences $\mathrm{Supp}_l^{K_n}(\alpha) \cong \mathrm{Supp}_l^{K_m}(\alpha')$, $\mathrm{Supp}_l^{K_n}(u) \cong \mathrm{Supp}_l^{K_m}(u')$ and we conclude

$$\mathrm{Supp}_l^{K_n}(\alpha) \cap \mathrm{Supp}_l^{K_n}(u) \cong \mathrm{Supp}_l^{K_m}(\alpha') \cap \mathrm{Supp}_l^{K_m}(u') = \{\alpha_2\lambda_0\},$$

a singleton as required. ■

Remark The simpler condition "p not a p-th power mod l" implies that π_{m-1} in not a p-th power mod λ, for some $\lambda | l$.

When $p = 3$ or 5, we now have the tools to prove $\mu(E)_p = 0$ for infinitely many curves E satisfying our running hypotheses on $E[p]$, as in Conjecture 2. Our examples are essentially different in that no two curves we will produce have isomorphic p-torsion. We will find our curves in the Kubert families (see [5]) parametrizing curves with a point of order p.

$p = 3$: Consider the family

$$E_t : y^2 + ty = x^3 + x^2 + tx$$

whose discriminant and j-invariant are given by

$$\Delta_t = -t^3(27t - 8), \quad j_t = \frac{(3t-1)^3}{t^3(27t-8)}.$$

The point $P = (0, 0)$ is of order 3 on any E_t.

Choose $t \in \mathbb{Z}$ such that $l = 27t - 8$ is a prime number, and such that 3 is not a cube mod l. There are infinitely many such t by the Čebotarev Theorem applied to the extension $K = \mathbb{Q}(\zeta_{27}, \sqrt[3]{3})$ and $\sigma \in G_{K/\mathbb{Q}}$ satisfying $\sigma|_{\mathbb{Q}(\zeta_{27})} = -8 \in \mathbb{Z}/27\mathbb{Z}^\times$ and not fixing $\sqrt[3]{3}$.

Since $v_l(\Delta_t) = 1$, the equation for E_t is minimal at l, and l is a prime of bad reduction. If the reduction at l is additive, the point of order 3 forces it to be of type IV or IV^*, and μ has a puncture at l in either case. If the reduction is multiplicative, the numerator cannot cancel the l in the denominator (since $j(E_t)$ would then be integral at l, and the reduction would be potentially good), thus $c_l = -v_l(j_t) = 1$.

Any other prime p of bad reduction divides t. Since t^3 and $(3t-1)^3$ are relatively prime *in* $\mathbb{Z}[x]$, we conclude that $3|v_p(j_t) \leq 0$. Thus p is a prime of multiplicative reduction: if it were additive, it would again have to be of type IV or IV^*, in which case we would have $j(E_t) \equiv 0 \pmod{p}$, contradiction. Thus reduction is multiplicative, and $3|c_p = -v_p(j(E_t))$.

We conclude that the quasi-finite flat group scheme μ associated to E_t has precisely one puncture, at l, *i.e.*, that its p-torsion conductor is $N = l$. Since $9 \parallel l - 1$ and 3 is not a cube mod l, l satisfies all the conditions of Theorem 4, which guarantees $\mu(E_t)_3 = 0$. The infinitely many E_t's we have thus produced have pairwise non-isomorphic 3-torsion, since the punctures occur at different primes l.

$p = 5$: Consider the family

$$E_{s,t} : y^2 + (s-t)xy - s^2ty = x^3 - stx^2$$

whose members have the point $(0, 0)$ of order 5, and whose discriminant and j-invariant are given by

$$\Delta_{s,t} = -s^5t^5(s^2 + 11st - t^2), \quad j_{s,t} = \frac{(s^4 + 12s^3t + 14s^2t^2 - 12st^3 + t^4)^3}{s^5t^5(s^2 + 11st - t^2)}.$$

We now choose $s, t \in \mathbb{Z}$ so that $l = s^2 + 11st - t^2$ is a prime, $25|l - 1$, and such that 5 is not a 5th power mod l as follows. Consider the extension $L = Q(\zeta_{25}, \sqrt[5]{5})$, and choose a rational prime l which splits completely in $\mathbb{Q}(\zeta_{25})$, but not in L. This clearly forces the last two conditions on l. As for finding $s, t \in \mathbb{Z}$ with $l = s^2 + 11st - t^2$, this is possible for any $l \equiv \pm 1 \pmod{5}$, since the strict class number of the order of $\mathbb{Q}(\sqrt{5})$ of discriminant 125 is 1.

Having chosen our s and t, we check that μ, the quasi-finite flat quotient of $\mathcal{E}_{s,t}[5]$, has a single puncture precisely at l. As $E_{s,t}$ has a point of order 5, all primes of bad reduction are necessarily multiplicative. Since $v_l(\Delta_{s,t}) = 1$, l is a prime of (stable) bad reduction. Therefore the l in the denominator of $j_{s,t}$ cannot cancel, and $c_l = v_l(j_{s,t}) = 1$. Any other bad prime p divides s or t, say s. If p were to divide the numerator in $j_{s,t}$, we would have have $p|t$ also, so $p|l$, a contradiction. Thus $5|c_p = -v_p(j_{s,t})$, and μ has no puncture at p. Theorem 4 applies again and allows us to conclude that $\mu(E_{s,t})_5 = 0$. Moreover, if for a (s', t') chosen analogously we have $l' \neq l$, $E_{s,t}[5] \ncong E_{s',t'}[5]$, and we get an infinite supply of fundamentally distinct examples of curves with μ-invariant zero.

For example, $s = 6, t = 1$ will satisfy all our conditions. The corresponding curve

$$E_{6,1} : y^2 + 5xy - 36y = x^3 - 6x^2$$

has conductor 606, and Tamagawa numbers $c_2 = c_3 = 5, c_{101} = 1$.

A similar argument with $p = 7$ is in principle possible, but runs into interesting difficulties, analytic in nature, concerning the representation of primes by cubic forms. For now, here are three curves with a rational point of order 7 which satisfy the conditions of Theorem 4 and thus have $\mu(E)_7 = 0$. The examples were chosen to have a relatively small puncture prime l, which is the last prime in the factorization of the (elliptic curve) conductor:

$$y^2 - 319xy - 49096y = x^3 - 12274x^2, N_E = 950266 = 2 \cdot 17 \cdot 19 \cdot 1471,$$

$$y^2 - 589xy - 419796y = x^3 - 46644x^2, N_E = 20510 = 2 \cdot 3 \cdot 13 \cdot 23 \cdot 2594,$$

$$y^2 - 155xy + 1872y = x^3 + 1872x^2, N_E = 20622 = 2 \cdot 3 \cdot 13 \cdot 2939.$$

A final note: The argument above works only with the quasi-finite flat group scheme $\mathcal{E}[p]$, so it is tempting to consider a slightly more general situation. Fix a field F, and consider a $\mathbb{Z}_p$ extension F_∞/F. Take a quasi-finite flat group scheme $\mathcal{G}_{/\mathcal{O}_F}$ living in a short exact sequence

$$0 \to \mathbb{Z}/p\mathbb{Z} \to \mathcal{G} \to \mu \to 0, \tag{19}$$

with μ again a punctured over an ideal $\mathcal{N}$, all of whose prime factors are assumed finitely split in F_∞. As in Section 4, we can find a $\mathcal{K} \subseteq H^1_{fl}(\operatorname{Spec} \mathcal{O}_{F_\infty}, \mu)$ which is an extension of $\mathcal{O}^\times_{F_\infty}/\mathcal{O}^{\times p}_{F_\infty}$ by a finite group. As in the case of elliptic curves, the long exact sequence differential δ associated to (19) induces a pairing:

$$\varprojlim \mathcal{O}^\times_{F_n}/\mathcal{O}^{\times p}_{F_n} \times \mathcal{K} \to \varprojlim H^1_{fl}(\operatorname{Spec} \mathcal{O}_{F_n}, \mu_p) \times H^1_{fl}(\operatorname{Spec} \mathcal{O}_{F_\infty}, \mu) \overset{id \times \delta}{\to}$$
$$\to \varprojlim H^1_{fl}(\operatorname{Spec} \mathcal{O}_{F_n}, \mu_p) \times H^2(\operatorname{Spec} \mathcal{O}_{F_\infty}, \mathbb{Z}/p\mathbb{Z}) \to \mathbb{Z}/p\mathbb{Z},$$

where the last arrow is the limit of the canonical global duality pairing. Here is a natural question to consider: is this pairing always non-zero when the pullback of (19) to the generic point is non-split?

Acknowledgments I would like to thank my thesis adviser, Prof. Barry Mazur, for help and encouragement in pursuing this work.

References

[1] J. E. Cremona, *Algorithms for Modular Elliptic Curves.* Second edition. Cambridge University Press, Cambridge, 1997.

[2] M. J. Drinen, *Finite submodules and Iwasawa μ-invariants.* J. Number Theory **93**(2002), 1–22.

[3] R. Greenberg, *Iwasawa theory for elliptic curves.* In: Arithmetic Theory of Elliptic Curves, Lecture Notes in Math. 1716, Springer, Berlin, 1999, pp. 51–144.

[4] R. Greenberg and V. Vatsal, *On the Iwasawa invariants of elliptic curves.* Invent. Math. **142**(2000), 17–63.
[5] D. S. Kubert, *Universal bounds on the torsion of elliptic curves*. Proc. London Math. Soc. (3) **33**(1976), 193–237.
[6] B. Mazur, *Rational points of abelian varieties with values in towers of number fields.* Invent. Math. **18**(1972), 183–266.
[7] J. S. Milne, *Étale Cohomology*. Princeton Mathematical Series 33, Princeton University Press, Princeton, NJ, 1980.
[8] B. Perrin-Riou, *Variation de la fonction L p-adique par isogénie.* In: Algebraic Number Theory, Adv. Stud. Pure Math. 17, Academic Press, Boston, MA, 1989, pp. 347–358.
[9] K. Rubin, *Euler systems and modular elliptic curves.* In: Galois Representations in Arithmetic Algebraic Geometry, (A. Scholl and R. Taylor, eds.), London Math. Soc. Lecture Note Ser. 254, Cambridge University Press, Cambridge, 1998, pp. 351–367.
[10] P. Schneider, *The μ invariant of isogenies.* J. Indian Math. Soc. (N.S.) **52**(1988), 159–170.
[11] V. Vatsal, *Special values of anticyclotomic L-functions.* Duke Math. J. **116**(2003), 219–261.
[12] ———, *Multiplicative-type subgroups of $J_0(N)$ and applications to elliptic curves*, to appear in J. Inst. Math. Jussieu.

Department of Mathematics
McGill University
Montreal, QC
H3A 2T5
e-mail: mak@math.mcgill.ca

https://doi.org/10.4153/CJM-2005-032-9 Published online by Cambridge University Press